Designing Human-Centered Collective Intelligence

Ivor Addo
Marquette University

DESIGNING HUMAN-CENTERED COLLECTIVE INTELLIGENCE

by

Ivor D. Addo

A Dissertation submitted to the Faculty of the Graduate School,

Marquette University, in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

Milwaukee, WI, USA

August 2016

ABSTRACT

DESIGNING HUMAN-CENTERED COLLECTIVE INTELLIGENCE

Ivor D. Addo

Marquette University, 2016

Human-Centered Collective Intelligence (HCCI) is an emergent research area that seeks to bring together major research areas like machine learning, statistical modeling, information retrieval, market research, and software engineering to address challenges pertaining to deriving intelligent insights and solutions through the collaboration of several intelligent sensors, devices and data sources. An archetypal contextual CI scenario might be concerned with deriving affect-driven intelligence through multimodal emotion detection sources in a bid to determine the likability of one movie trailer over another. On the other hand, the key tenets to designing robust and evolutionary software and infrastructure architecture models to address cross-cutting quality concerns is of keen interest in the "Cloud" age of today. Some of the key quality concerns of interest in CI scenarios span the gamut of security and privacy, scalability, performance, fault-tolerance, and reliability.

I present recent advances in CI system design with a focus on highlighting optimal solutions for the aforementioned cross-cutting concerns. I also describe a number of design challenges and a framework that I have determined to be critical to designing CI systems. With inspiration from machine learning, computational advertising, ubiquitous computing, and sociable robotics, this literature incorporates theories and concepts from various viewpoints to empower the collective intelligence engine, ZOEI, to discover affective state and emotional intent across multiple mediums. The discerned affective state is used in recommender systems among others to support content personalization. I dive into the design of optimal architectures that allow humans and intelligent systems to work collectively to solve complex problems. I present an evaluation of various studies that leverage the ZOEI framework to design collective intelligence.

ACKNOWLEDGEMENTS

Ivor D. Addo

In no particular order, I would like to thank my deceased mother, my father, my wife, my children, and my siblings for inspiring me and remaining supportive of my academic journey. I cannot underscore my utmost appreciation for my faculty, doctoral committee, and my doctoral committee director for staying supportive throughout my studies at Marquette University. Many thanks to Dr. S. Iqbal Ahamed (my dissertation chair), Dr. Praveen Madiraju, Dr. Thomas Kaczmarek, Dr. Rong Ge, and Dr. William Chu (my dissertation committee members). I would also like to thank the Graduate School and all Marquette University administration members who have supported me throughout my academic journey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

A. Overview

Companies like Google, Match.com, Netflix, and more have been successful at using various computational models to aggregate data from several sources in a bid to better understand end-user needs [1]. To a large extent, these insights often drive targeted advertising and content personalization. Invariably, there are multitudes of use cases for implementing Collective Intelligence (CI) especially in the ever growing "Internet of Things" (IoT) phenomenon. Some of the relevant application areas of CI include Affective Computing solutions, Ubiquitous Computing applications, Social Media Intelligence systems, Human-Robot Interaction (HRI) systems and more.

The definition of Collective Intelligence (CI) forms a foundation for the hypothesis of this study. Singh and Gupta [10] define Collective Intelligence as the capability of a series of unsophisticated agents to collaboratively solve significant and complex problems that would otherwise remain unsolved by a single agent. Segaran [1] describes CI as the combination of behavior, preferences, or notions of clusters of people to create innovative insights. To enable collective intelligence, a number of things have to fall in place including: continuous user interaction with the solution, suitable models to amass the learnings of the system and the ability to draw from the aggregated knowledge to recommend relevant and personalized content to users [10]. I argue that beyond the technology solutions at play, the privacy of the end users involved is a major concern in this type of CI approach to HCCI solution design.

The synergistic application of knowledge gleaned pervasively from multiple integrated sensors in our everyday lives in an effort to collaboratively assist humans in their quest to attain a specific goal is quite promising and suitable for solving complex problems that require an adaptive and personalized approach. Even so, if this machine-to-machine (M2M) knowledge sharing approach is capable of identifying groups of people and the differences in their persona that influence their propensity for behavior change, it makes it more interesting to build effectually personalized solutions. In a sample CI application, I mined data pertaining to a child's progress towards physical activity and healthy diet choices from various sources, discovered patterns in the data collected for multiple participants using clustering ML algorithms and successively made relevant personalized suggestions for behavior change by leaning on a predictive model based on ML classification [11].

The emergent prevalence of childhood obesity remains one of the most significant healthcare challenges facing the United States today. On the other hand, breakthroughs in Human-Robot Interaction (HRI) research and the diminishing cost of personal robots and virtual agents along with the ever-increasing use of smart personal devices, suggests that there is room for harnessing the power of ubiquitous intelligent systems that can work in partnership to solve some of our most difficult challenges in the very near future. Electronic Health and Wellness needs of this nature paves the way for implementing collective intelligence approaches aimed at employing machine learning algorithms that work in concert to facilitate the personalization of autonomous Health Coaches with a focus on implementing interventions through HRI and other adaptive Ubiquitous Computing (UbiComp) solutions.

In this work, I describe Collective Intelligence as an amalgamation of several multimodal input signals stemming from various humans, sensors and computing devices in an effort to derive insights to support personalization.

B. Background: Privacy in Collective Intelligence

As cloud services, mobile gadgets and other ubiquitous technologies are employed for supporting healthcare monitoring scenarios, the security, privacy and trust concerns surrounding the acceptance of these technologies continue to remain a key barrier to mainstream adoption. In recent times, pervasive healthcare monitoring solutions are known to employ multiple sensors and gadgets for collecting user behavior data in, say, a smart home environment. Data collected in these environments are typically transferred through a web service interface to cloud-based data storage. In most instances, some form of collective intelligence technique is used to draw insights from the raw data to help improve the participant's quality of life. Nonetheless, this trend in cloud-assisted ubiquitous health monitoring systems is expected to continue to grow [2].

Even then, Privacy continues to materialize as a major disincentive to the adoption of pervasive health monitoring solutions [6]. Viewed in the light of the inherent concerns with solutions that draw from the Internet, Cloud Computing, Ubiquitous Computing, mHealth, and Computational Advertising, the problem becomes even more alarming for end-users of the solution. Intuitively, one would expect that a low disposition of privacy in a particular system will result in a low level of trust in the associated solution. A recent study [3], suggests that privacy and trust have a symbiotic relationship in a way that allows the dearth of privacy to be compensated by a surfeit of trust and vice versa. Naturally, lack of security in a given system is, more likely than not, perceived to be synonymous with lack of privacy, even though it is not necessarily true. Subliminally, there are strong dependencies of trust on privacy and security.

Surprisingly, there is little evidence that an online user's privacy concerns translate into privacy-enhancing behaviors in his or her online activities [3]. In most cases, the average consumer of emerging technologies does not have the time or ability to read and comprehend the legal fine print of a privacy policy for a given technological solution. Yet, consumers seek some level of privacy in their disclosure of personal information in these settings. There is, currently, no known widely-accepted standard for certifying the level of privacy protection available in a given technology solution or for monitoring a solution provider's ongoing privacy reputation.

Technology solution providers are often looking to use personal information disclosed by a target user for good intentions. However, in some instances, a solution provider might be willing to concede to the privacy of the end-users in return for monetary gains, conformance to government legislation, and more. In the advent of Application Programming Interfaces (APIs), several solution providers (particularly, Social Networking sites like Twitter, Facebook, LinkedIn and Google) expose an API for consuming user data that may otherwise be perceived by the owner of the data to be private. These solution providers have no standard way of protecting the end-user's private data from getting into the hands of ill-intent API consumers who may or may not protect the user's privacy once the data crosses the boundaries of the solution provider's system. To earn the trust of consumers, their privacy must be protected not only within the system where the personal information is collected or disclosed, but also in ancillary systems that are subsequently capable of accessing the private user data.

In the face of recent attempts at establishing security and privacy frameworks to support trust management in CI systems, a comprehensive model that fosters trust among the target users of these emerging technologies is yet to achieve mainstream adoption [4]. A number of previous studies have proposed privacy and security frameworks for protecting data in specific domains ranging from mobile health monitoring [5], self-improving smart spaces [6], location privacy in mobile computing [7], privacy protection in web services [8], privacy enhancement in platform-as-a-service cloud computing scenarios [9], and more. I challenge the trend by proposing a holistic view to the problem with a focus on protecting the security and privacy of end-user data while fostering trust in new and old technology solutions that are willing to subscribe to these standards.

C.Background: Emotional Intelligence in CI

As intelligent systems become increasingly context-aware and socially expressive, there is a growing need to establish a believable and trustworthy framework for detecting human emotion and influencing the selection of relevant content, ads, or automated dialog response messages. The basic premise of computational advertising problems is predicated on the ability for a system to select the most suitable content or advertisement for a given user profile based on a particular context. Context, in this sense, might refer to web sponsored search results, banner advertisements (ads), news articles, video content, and more. Traditional television (TV) ad campaigns seldom offer quantifiable evidence-based metrics to justify a hard measure for return on investment (ROI). In most instances, TV ads cannot be personalized. What if, the smart TV in your living room can recommend shows or personalize video content based on your affective mood? By virtue of the system's ability to detect human faces in support of human identification, mood-based personalized TV ads are expected to support ad revenue traceability and ROI attribution. This study seeks to describe the state-of-the-art design of an affective computing framework that can be leveraged for personalizing traditional content including TV ads.

D. Background: ZOEI, A Human-Centered CI Framework

To implement a robust framework for designing human-centered collective intelligence (HCCI) solutions, I recount the need for several reference architectures that can guide human-centered architecture scenarios. The reference models stress the use of emotional intelligence, privacy and security in designing human-centered solutions. I designed a set of reference architectures models and frameworks aimed at addressing major design principles related to CI scenarios. The proposed framework model for building HCCI systems is referred to in this literature as ZOEI – an acronym for a Zestful Outlook on Emotional Intelligence systems.

The class of problems that the ZOEI framework (illustrated in Figure 1) is best suited for includes scenarios where multiple deployed smart agents, sensors and devices leverage a centralized knowledge store in a cloud-hosted service environment to share intelligence in support of personalized human-machine interaction patterns in a smart environment. These scenarios might involve leveraging external data sources including online social media networks to mine individual and aggregate user behavior data in support of the promise of collective intelligence. A *feedback loop* is established between the multimodal cognitive module and the personalized interaction module to reinforce and collaboratively filter the detected cognition (e.g. emotion) in an effort to further minimize prediction errors. In this study, I focus on *affect* as a cognitive feature in the interaction pattern, however, other modalities and cognition features can be used interchangeably in the reference model.

Of note, some of the components in the proposed framework are optional based on the exact human-centered IoT application scenario under investigation. To facilitate “believability” in the human-machine interaction patterns, some form of psychological interaction pattern is recommended. The therapeutic behavior change technique employed in the sample Childhood Obesity CI system is drawn from *motivational interviewing* (MI) theory [23]. MI presents an effectual strategy for stimulating a participant’s readiness for health-related behavior change by personalizing the persuasive system’s approach to the human subject’s level of readiness based on a behavior alteration continuum [89].

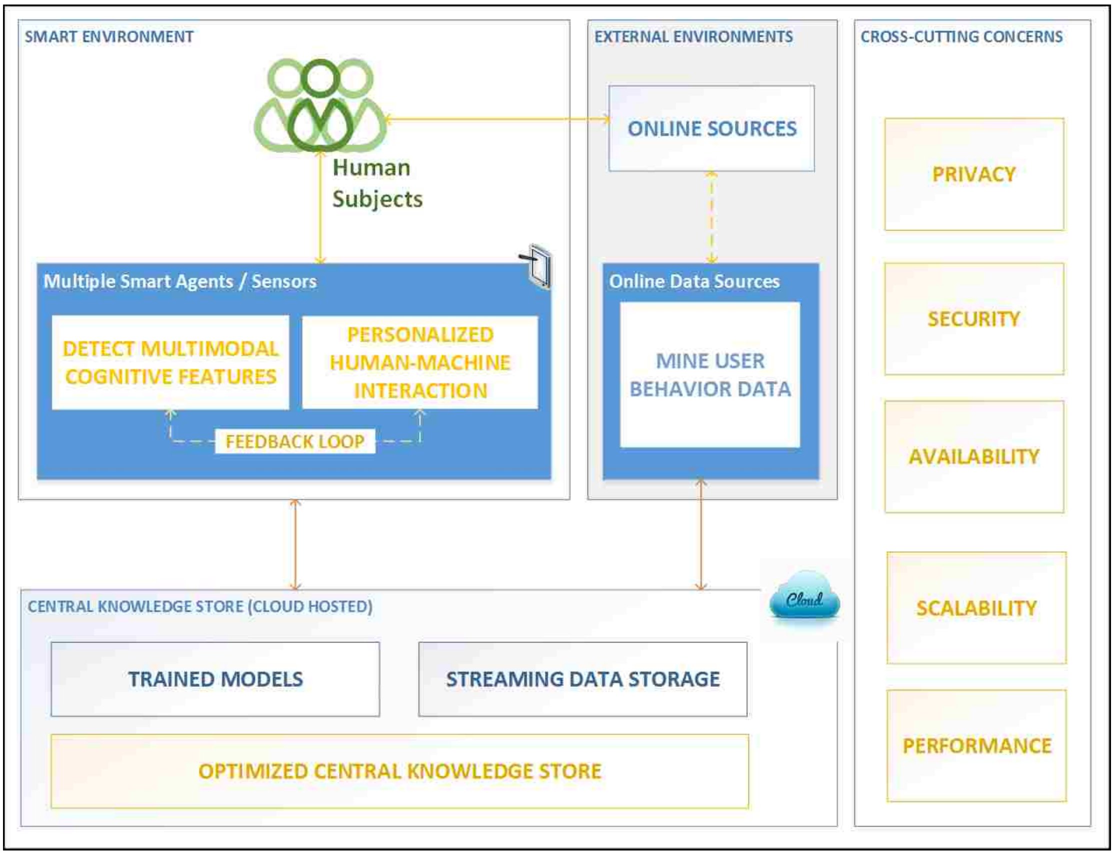


Fig. 1. The ZOEI framework for human-centered CI solutions – conceptual reference model

E. Statement of the Problem

To implement a robust framework for designing collective intelligence solutions, there is a need for researchers and practitioners to draw on reference architectures that offer best practices and optimal solutions to designing human-centered architecture solutions.

F. Purpose of Study

With the advent of cloud computing services, there are a plethora of options for designing collectively intelligent systems. However, there is very minimal literature surrounding human-centric architecture models and best practices. Establishing some guidance around design patterns for building human-centered architectures and collectively intelligent systems will help inspire new experiments and guide the design and optimization of future models.

G. Research Questions and Specific Aims

This study seeks to understand some of the principal components of human-centered architectures geared towards collective intelligence. In addition, I delve into the relationships between the individual components in the framework through the *proposed aims* identified below. Figure 2 illustrates the framework for this study, in the light of the proposed framework illustrated in Figure 1.

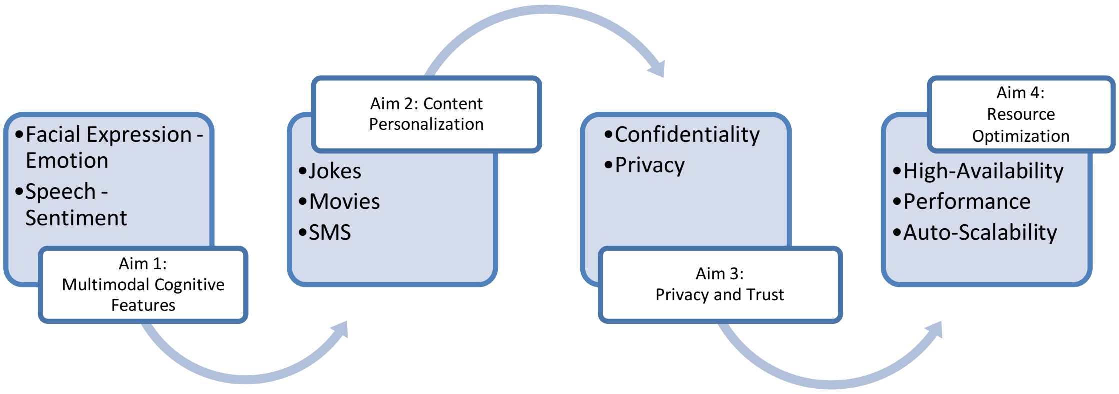


Fig. 2. The framework for the research study

The research study seeks to bring clarity to some of the major concerns in CI architecture design by addressing the following outstanding research questions:

1) Aim 1: Investigate Multimodal Cognitive Features

Research Question: **Investigate how to incorporate Cognitive Features in CI solutions.**

Though there are bound to be several *Multimodal Cognitive Features* involved with a typical CI system design, this study will focus specifically on investigating how to implement multimodal emotional intelligence through *sentiment analysis modeling in natural language dialogue, facial recognition,* and *affect detection through facial expression analysis* as Aim 1.

2) Aim 2: Investigate Content Personalization

Research Question: **Determine how to design effective Content Personalization solutions in CI systems.**

In most CI solutions, there is often the need to customize or personalize end-user content (e.g. jokes, movies, persuasive dialogue, Short Message Service - SMS text, etc.) based on end-user behavior. In this study I will focus on investigating a framework for designing content recommendations based on insights derived from the multimodal cognitive features along with external data sources including social media intelligence (SMI) sources. Psychological theories like motivational interviewing, etc. can be used to deliver effective human-machine interactions.

3) Aim 3: Investigate Security and Privacy concerns

Research Question: **Investigate how to design CI systems that exhibit ethical choices, security, and privacy preservation for end-user data.**

Considering the fact that various data collection features in a CI system are focused on collecting end-user behavior data (particularly in IoT solutions), it is important to consider the privacy preservation needs of the end user. In this study I consider the detection and preservation of privacy and confidentiality as an impetus to establishing trust and driving further end user adoption of such HCCI systems.

4) Aim 4: Cloud Resource Reliability

Research Question: **Investigate how to design CI solutions that exhibit optimal Cloud Resource Reliability.**

While multiple architectural quality attributes contribute to building highly accessible and operational reference solutions, this study will focus on investigating best practices for optimizing cloud-based CI solution architectures to support high-availability, automatic scalability, and high performance.

H. Significance of the Study

In the wake of an era where cloud-enabled Internet of Things (IoT) applications seek to derive intelligence from multiple data sources, this study offers a guide for designing human centered architecture models that utilize optimal technology resources without compromising the needs of the human components in collectively intelligent solutions.

By offering novel reference architectures and computational models for designing cloud-enabled collective intelligence applications, I expect to provide an architectural model for designing, analyzing, and evaluating multiple approaches to implementing evolutionary software and infrastructure frameworks in support of application scenarios across Human-Robot Interaction (HRI), IoT, Ubiquitous Computing (UbiComp), Social Media Intelligence (SMI), and Affective applications.

I. Summary

I expect collective intelligence to become pervasive in the coming years. As several researchers and practitioners race to take advantage of this new phenomenon, I expect this study to help govern and inform all participating stakeholders in CI solutions through my findings. I expect the literature to impact future work on optimizing and maximizing the promise of CI in real world applications.

II. LITERATURE REVIEW

A. Overview

In this chapter, I present insights and background information for modeling privacy, confidentiality, security and affect-driven systems in collective intelligence applications. I surveyed several topics including various frameworks for addressing key quality attributes in a useful CI architecture model. I identified privacy, confidentiality, dialogue management systems, cloud reliability and performance, as well as affect-driven solutions to be major concerns in typical CI applications. The ensuing literature reviews the state of the art studies in these key areas.

B. Modeling Affect Detection in CI

While I employed IoT concepts in a unique way for this study, previous research studies have employed Collective Intelligence strategies to enhance HRI through a combination of ubiquitous sensors and communication robots [26]. I take inspiration from some of the affective HRI systems that often take the form of human-like and animal-like embodiment. I contrast some of the differences between the proposed approach and that of other prominent affective HRI dialog systems in Table I.

TABLE I. THE PROPOSED STRATEGY COMPARED TO OTHER APPROACHES

Characteristics	**Kismet [24]**	**Robovie [27]**	**Mental Commit Robots [28]**	**ZOEI**
Applies CI or IoT	No	No	Yes	Yes
Describes AI learning method	No	No	No	Yes
Emotion Generation	Yes	Yes	Yes	Yes
Describes user segmentation and content selection approach	No	No	No	Yes
Emotion Detection	Yes	No	No	Yes
Uses a Cloud-based Service	No	No	No	Yes

Wada et al. [28] applied robot-assisted activity to stimulate affection in an elderly care facility by using artificial emotional animal-like robots that take the form of a dog, cat and a seal robot. Some of the previous HRI studies have explored the use of various communication techniques for assistive robots in a shopping mall [27]. In addition, Breazeal [24] has performed multiple HRI studies using the animal-like robot named Kismet. Robovie, of the ATR Intelligent Robotics laboratories, demonstrates affective dialog patterns in entertainment scenarios [27]. Honda's ASIMO robot is also known to exhibit affective HRI dialog patterns.

While there are a number of studies regarding affective communication robots I believe that the proposed strategy describes an alternative methodology to addressing the ongoing challenges of building affective dialog systems while presenting a unique case study for entertainment applications of affective HRI dialog.

C.Modeling Content Personalization

In building a holistic CI system that is capable of inspiring behavior change among diverse participants, it is often important for the intelligent system to feature adaptive messages or content that is personalized for the human subjects involved based on the context of the situation. Similar to the approach that is used in the market research field to understand the needs of a specific market segment, the use of unsupervised machine learning algorithms is proposed for clustering the human-to-human interaction data captured in smart environments as well as the human-to-machine interactions recorded through smart dialog systems. The k-Means clustering algorithm will be adopted for identifying similarities in profiles that go beyond the basic demographic data clusters [23].

D. Motivational Interviewing in CI dialogue systems

While several HRI-based interventions are focused on fighting Autism among children [43], childhood obesity [23], and other socially assistive solutions [86], I am not aware of any particular approach that leverages the collective intelligence strategy described in this research work to solve a health-related issue through Motivational Interviewing (MI).

Robot-mediated therapy is commonly used along with other therapeutic approaches to address stroke, spinal cord injury, and Multiple Sclerosis (MS) issues [42]. Lisette, Visser and Rishe [89] have made some significant inroads into applying MI to behavior change interventions. However, their research work was limited to applying MI in Embodied Conversational Agents (ECA) [45]. Needless to mention, there are also several traditional strategies for child and adolescent obesity interventions today [44] that do not involve HRI and UbiComp-inspired approaches to solving the problem.

TABLE II. THE PROPOSED STRATEGY COMPARED TO OTHER APPROACHES

CHARACTERISTICS	**MI in ECA [45]**	**Other HRI interventions [43]**	**ZOEI**
Features Collective Intelligence	No	No	Yes
Use of Physiotherapy	Yes - MI	No	Yes - MI
Utilizes Emotion Detection	No	No	Yes
Use of Interactive gameplay	No	Yes	Yes
Implements user segmentation via data mining	No	No	Yes
Incorporates M2M networks collaboratively	No	No	Yes

While, several of the related works have focused on describing rich approaches to behavior intervention, very minimal work has been done towards enabling a holistic solution that embodies various effective solutions to CI-influenced healthcare intervention issues. Table II contrasts the differences in related works and that of the proposed solution. I believe that the proposed strategy described in the study will go a long way to impact future work in eHealth and well-being interventions through collectively intelligent and highly personalized techniques.

E. Modeling Privacy Preservation in CI

In the wake of an imminent infusion of robot companions and other autonomous agents in our everyday lives, one of the most critical barriers that might remain a strong inhibitor to the adoption of the "robot in every home" phenomenon is rooted in our basic right as humans to protect our privacy. Questions like "Will I trust a robot to respect my privacy?", "How will the humanoid robot access my privacy preferences?", and many more plague the thoughts of potential early adopters [40].

I acknowledge the questions posed by the need to implement privacy-awareness in an HRI interaction as a set of challenging problems. What are some techniques for performing real-time filtering of spoken language? What are some techniques for filtering out previously acquired knowledge based on the HRI context? How can privacy-awareness be implemented in a way that makes the proposition of having an always-on humanoid robot or intelligent system welcome in our homes? These and many ancillary question capture my curiosity for embarking on the design of a privacy framework for HRI-based privacy preservation.

Lee et al. [12] argued that anthropomorphized robots can be used to manipulate end-users into disclosing more private information than they will otherwise be willing to share. Invariably, it is hard for end-users to detect when a robot is recording information about them [12]. Pallapa et al. [13] shared a scheme for improving the granularity of end-user privacy in context-aware ubiquitous systems. Jiang [14] postulated that establishing a trusted privacy runtime does not necessitate collocating the privacy tags with the data objects. Schreck [15] shared several ideas for privacy preservation in user modeling. Some of the key data points of interest from a security and privacy perspective can be categorized as user demographic data, usage behavior or usage data, and environmental (contextual) data. Shreck [15] shared some ideas for user modeling with privacy and security in mind. Privacy preservation problems and resulting techniques can be categorized as being related to [16]*: Identity protection, Anonymity, and Access control*. Some of the data types involved can be labeled as: *Demographic user data*, *Observable usage data*, and *Environmental data* (including the context).

A significant number of previous studies on privacy have focused on user data anonymity, though in an HRI dialogue scenario the focus is on observable usage data and contextual data to drive personalization [17, 18]. While several privacy frameworks and protocols have been proposed for ubiquitous computing devices in the past, I believe that I have a unique approach to filtering out CI-related dialogue data from both the front-end and the back-end in a way that has not been attempted previously. I draw inspiration from the privacy scheme presented by Pallapa et al. [13]. In Table III, I contrast some of the differences between the proposed framework and that of other prominent privacy systems.

Traditional online advertising scenarios are often susceptible to privacy violations of end users. Leon et al. posit that an end-user's privacy preferences are not only determined by the sensitivity of the information that is gathered by online advertisers [59]. In their quantitative analysis, the researchers found the following factors to be quite important to an end-user's privacy preferences in behavioral advertising scenarios: scope of data collection and use, the relevance of the data collected to advertising, and the expected benefits of divulging a specific type of data [58, 59].

TABLE III. THE PROPOSED STRATEGY COMPARED TO OTHER APPROACHES

Characteristics	Shreck [15]	Pallapa [13]	SBAC [16]	Lee [12]	ZOEI
Tailored to CI	No	No	No	Yes	Yes
Presents a framework or scheme	No	Yes	Yes	No	Yes
Access Control	No	No	Yes	No	Yes
Applies Machine Learning	No	No	No	No	Yes
Considers dialogue systems	No	No	No	Yes	Yes
Context-awareness	No	Yes	No	Yes	Yes
Cloud-based Service considerations	No	No	No	No	Yes

F. Modeling Confidentiality in CI

Intelligent conversational systems can be used to motivate behavior change among people who are interested in behavior change towards curbing obesity [20], risky behavior change among Post-Traumatic Stress Disorder (PTSD) patients, smoking cessation, and more. There are other applications of conversational robots in elderly care monitoring scenarios [25]. My primary motivation is to enable autonomous systems with an ability to implicitly detect confidentiality in CI dialogue systems.

In most human-to-human communications, there is often a need to evaluate both verbal and non-verbal communication signals to truly understand the situation at hand. Verbal communication often involves the use of spoken words while non-verbal communication involves visual cues including facial expressions, body movement, proximity, body language, and more [23, 24]. Generally, when a human stands further away from another human (i.e. proximity) it indicates their level of comfort with the other party. In other scenarios, a human might say something positive through spoken word, while simultaneously exhibiting contradicting signals through non-verbal cues. A combination of verbal and non-verbal signals can be used by intelligent systems to discern confidentiality in dialogue systems.

Imagine a simple dialogue exchange between a teenage girl (*Amy*) and her friend (*Chloe*) at a college party, *Amy* whispers to *Chloe* the spoken word “I’m pregnant” (as illustrated in Figure 3 – left image). Even though, *Amy* did not explicitly indicate to

Chloe that her pregnancy should be kept confidential, the combination of the "*whisper*" (i.e. low pitch sound and close proximity to *Chloe* during the exchange), content of the verbal communication (i.e. "*pregnant*"), and the context of the scenario (i.e. at a crowded party scene) can be enough grounds for suggesting confidentiality. Arguably, if Chloe's next utterance in response to the news is a loud pitched celebratory response (e.g. "Wow, congratulations!") it might damage *Amy*'s trust and comfort with sharing future confidential dialogue with *Chloe*. This is the type of implicit confidentiality that this research seeks to enable companion robots with. The ability to detect and preserve confidentiality through their day-to-day interactions with humans is critical.

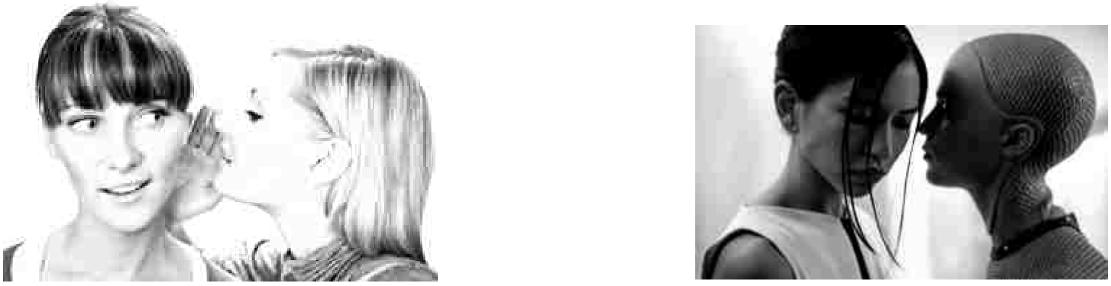


Fig. 3. On the left, I illustrate an exhibition of non-verbal cues in a human-to-human conversation regarding a confidential subject (involving whispering). On the right, I illustrate a sample conversation gesture between a futuristic Android robot and a human in an HRI dialogue as the robot shares spoken word regarding a confidential subject.

A common design practice in dialogue systems involves implementing a dialogue manager (DM) [20, 21] to generate, consume, and coordinate both verbal and non-verbal dialogue interactions between the human subjects and the intelligent systems involved. In the traditional dialogue system, there is often an Automatic Speech Recognition (ASR) module and a Text-to-Speech (TTS) module involved with consuming verbal content and exuding speech capabilities in the intelligent system, respectively [22]. That notwithstanding, non-verbal cues including gestures and facial expression can be identified using the camera inputs on the dialogue system. In investigating an approach to modeling confidentiality in HRI dialogue, I implemented the solution using the NAO T14 humanoid robot platform.

G. Cloud Reliability in CI Applications

To elaborate the potential impact of this aspect of human-centered CI systems, consider a number of socially assistive smart agents (for example, Apple's Siri software agent) and/or autonomous networked humanoid robots that share a centralized knowledge store hosted "in the cloud" for a collective intelligence scenario. Assuming the intelligent agents involved are fully operationalized and widely deployed across multiple locations, the reliability of this centralized intelligence data store becomes elevated to a high-importance design principle because the cloud resources involved would be expected to remain always-on to support intelligence sharing across multiple agents simultaneously.

As the adoption rate of *Cloud Computing* continues to grow among various application archetypes, there is a growing concern for identifying reliable automatic failover solutions between various cloud providers in an attempt to minimize the effect of recent cloud provider outages [54] among diverse always-on and mission-critical applications in healthcare, e-Commerce and other relevant CI ancillary settings. Automatic failover between cloud providers, among others, stands out as a solution for course-plotting application reliability requirements in support of high-availability, disaster recovery and high-performance scenarios.

While a few reference architectures exist for improving high-availability and disaster recovery within cloud implementations, with a focus on the Infrastructure-as-a-Service model, I am not aware of any literature that examines the challenges and characteristics involved with implementing a cross-cloud high-availability solution for Platform-as-a-Service (PaaS) scenarios. Both Erl et al. [29] and McKeown et al. [32] presented some interesting scenarios for implementing high-availability solutions within a given cloud provider. Additionally, McKeown et al. touched on the fact that exploring alternative clouds as a potential solution for improving HA and DR scenarios, in which the cloud provider is experiencing service disruption, seems feasible.

The authors posit that "the use of Virtual Machines [VMs] might be easier in these cases than cloud-specific PaaS designs" [32]. While the seemingly complex problem was attractive, as a research problem, I also realize that there are real-world scenarios where the use of an IaaS-based VM solution will not work well for mission-critical solutions that require a PaaS-based solution. There has been minimal discussion on how to implement a hybrid solution of this sort, some of the challenges and potential solutions in that space. Table IV explores some of the differences and similarities between this work and that of other relevant studies.

TABLE IV. COMPARISON WITH OTHER APPROACHES

CHARACTERISTICS	**McKeown et. al. [32]**	**Erl et. al. [29]**	**ZOEI**
Presents Cloud availability characteristics	Yes	No	Yes
Presents Failover algorithm	No	Yes	Yes
Discusses HA and DR solutions	Yes	Yes	Yes
Supports PaaS scenarios	No	No	Yes
Discusses DDNS	No	No	Yes

H. Summary

In summary, there are numerous studies that aim to address some of the key components in the proposed, ZOEI, framework. However, there are very few studies that expose a more holistic framework for supporting the key quality attributes and concerns in CI applications.

III. RESEARCH DESIGN AND METHODS

A. Overview

The ensuing paragraphs seek to present the research design and methodology for the 4 proposed aims:

- Aim 1: Investigating Multimodal Cognitive Features
- Aim 2: Investigating Content Personalization
- Aim 3: Investigating Security, Privacy Preservation and Ethics
- Aim 4: Investigating Cloud Resource Optimization

B. Aim 1: Designing Multimodal Cognitive Intelligence

As illustrated in the research study framework (in Figure 2), *Aim 1* will explore the infusion of cognitive intelligence features in a CI system by exploring what goes into designing persuasive CI systems that incorporate multimodal affect detection analysis through *facial expression analysis* and *sentiment analysis* in conversational HRI systems.

1) Scenario Analysis

In exploring the role of affect detection (as a sample cognitive feature in a CI system), I draw on the design of the following architectural designs for 3 main CI scenarios including:

- ***Scenario 1***: HRI dialogue sentiment analysis in a childhood obesity humanoid health coach system scenario [23] as well as
- ***Scenario 2***: Affect detection in a joke telling humanoid robot for elderly care companionship robot scenarios [38]
- ***Scenario 3***: Deriving Twitter.com sentiment analysis in SMI applications [48]

2) Architectural Design

The following literature illustrates the solution architecture for some of the CI solutions under consideration in this study.

Scenario 1: The following illustration depicts the logical view of a Collective Intelligence system designed to help curb childhood obesity through a humanoid health coach by using a combination of HRI and UbiComp interactions as described in *Scenario 1* above.

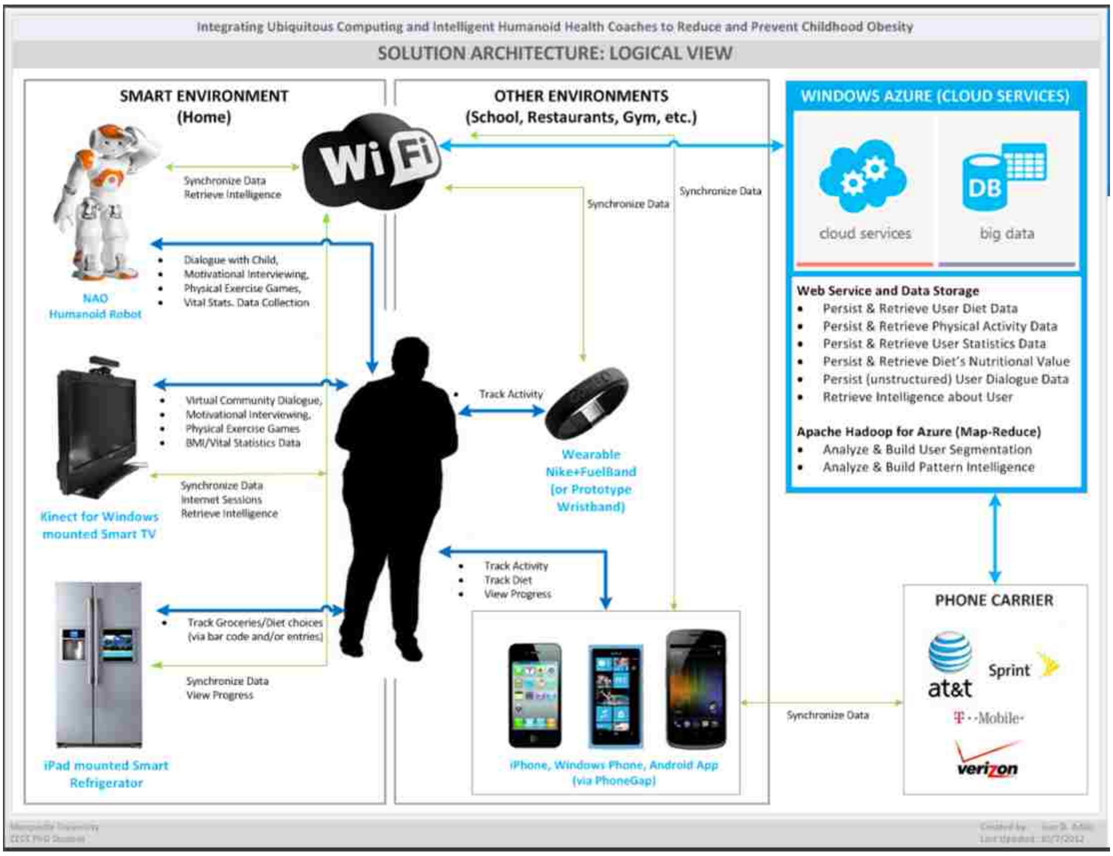

Integrating Ubiquitous Computing and Intelligent Humanoid Health Coaches to Reduce and Prevent Childhood Obesity
SOLUTION ARCHITECTURE: LOGICAL VIEW
SMART ENVIRONMENT (Home)
OTHER ENVIRONMENTS (School, Restaurants, Gym, etc.)
WINDOWS AZURE (CLOUD SERVICES)
Wi Fi
Synchronize Data
Retrieve Intelligence
Synchronize Data
Synchronize Data
NAO Humanoid Robot
Dialogue with Child,
Motivational Interviewing,
Physical Exercise Games,
Vital Stats. Data Collection
cloud services
DB
big data
Web Service and Data Storage
Persist & Retrieve User Diet Data
Persist & Retrieve Physical Activity Data
Persist & Retrieve User Statistics Data
Persist & Retrieve Diet's Nutritional Value
Persist (unstructured) User Dialogue Data
Retrieve Intelligence about User
Apache Hadoop for Azure (Map-Reduce)
Analyze & Build User Segmentation
Analyze & Build Pattern Intelligence
Virtual Community Dialogue,
Motivational Interviewing,
Physical Exercise Games
BMI/Vital Statistics Data
Track Activity
Wearable Nike+FuelBand (or Prototype Wristband)
Synchronize Data
Internet Sessions
Retrieve Intelligence
Kinect for Windows mounted Smart TV
Track Activity
Track Diet
View Progress
PHONE CARRIER
at&t
Sprint
T··Mobile·
verizon
Track Groceries/Diet choices (via bar code and/or entries)
Synchronize Data
View Progress
Synchronize Data
iPad mounted Smart Refrigerator
iPhone, Windows Phone, Android App (via PhoneGap)

Fig. 4. Solution Architecture for a Childhood obesity CI solution [23]

Scenario 2: The architecture of Scenario 2 is represented in Figure 5 below. In this scenario, the sentiment of the human's reactionary speech in the HRI dialogue to jokes uttered by the humanoid robot is assessed through the same predictive model established for Scenario 1. The training corpus is enhanced with common words and associated sentiment labels in the scenario at hand to ensure relevance to the dialogue under investigation. In this scenario, both the sentiment in spoken dialog and the facial expression of the audience is equally important in determining how the audience perceives the content.

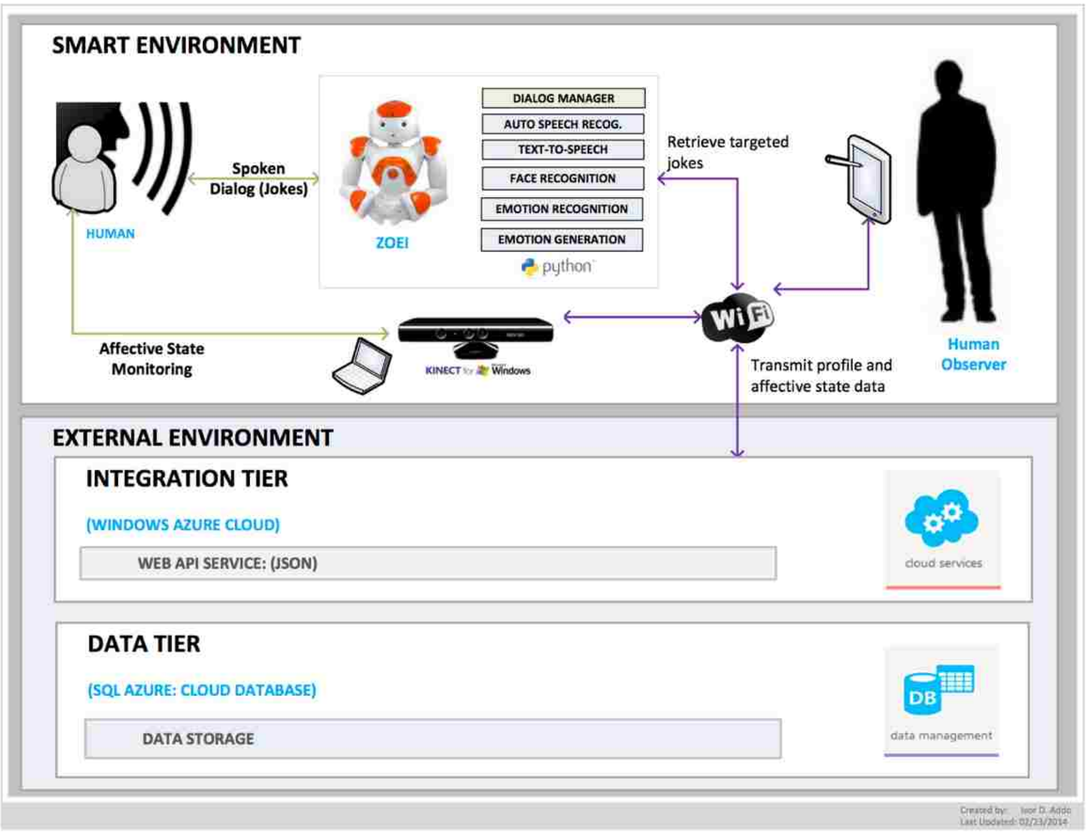


Fig. 5. Solution Architecture for a Joke-Telling Companion Robot [38]

Scenario 3: In Scenario 3, Twitter.com tweets are analyzed for positive, neutral and negative sentiments. It is assumed that, depending on the use case, social media influence can be used as a multimodal signal to support the personalization or recommendation of targeted content in Aim 2.

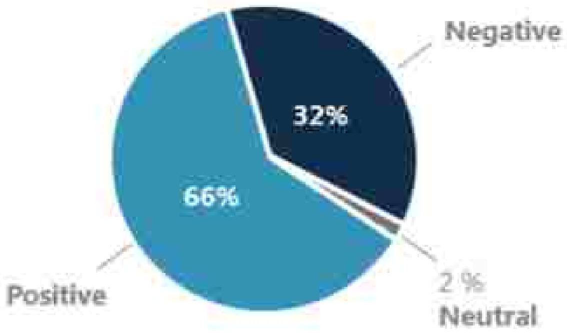


Fig. 6. Sample aggregate sentiment analysis of Twitter data extract [48]

3) Research Challenges

The following challenges are evident in implementing multimodal affect detection in the aforementioned scenarios:

- **Challenge 1:** Sentiment detection in the HRI dialogue while using the Automatic Speech Recognition (ASR) feature of the humanoid robot.
- **Challenge 2:** In addition, *Emotion Recognition through Facial Expression* (ERFE) analysis is a challenging problem.

4) Data Collection

For the sentiment analysis experiments pertaining to these scenarios, a binary classification model was built using the popular Sentiment140 sentiment dataset [55]. A corpus of about 160,000 pre-labeled "tweet messages" from the dataset are loaded to a Microsoft Azure Cloud Blob Storage location. The Azure Machine Learning platform is used to build a binary classification model. In different scenarios, the training corpus is augmented with relevant labeled data to improve the predictive model.

5) Methods

The dataset is tokenized and cleansed by converting all the data values to lowercase, and replacing punctuation, special characters and digits with a space character. The

Feature Hashing [93] technique is applied to the tweet messages with a *hashing bitsize* of 17 with two *n-grams*. As depicted in Figure 7, the data is then divided into two independent parts: *Training Data* and *Test Data*. Using, the *Holdout* method, sometimes known as *Test Sample Estimation*, I partition the available data D_N into two mutually exclusive subsets, the Training set D_{TR} and the holdout or Test set D_{TS}.

An 80% split percentage value for D_{TR} is used (i.e. D_{TS} = 0.2). The Chi-Squared scoring method is utilized in the feature selection stage of the data modeling exercise to filter the top 20,000 most important features (input variables) in the data set. Upon selecting the best algorithm for the task, the model is published as a predictive web service and consumed by the NAO T14 Humanoid for determining the sentiment of spoken natural language by the human counterpart in the scenario.

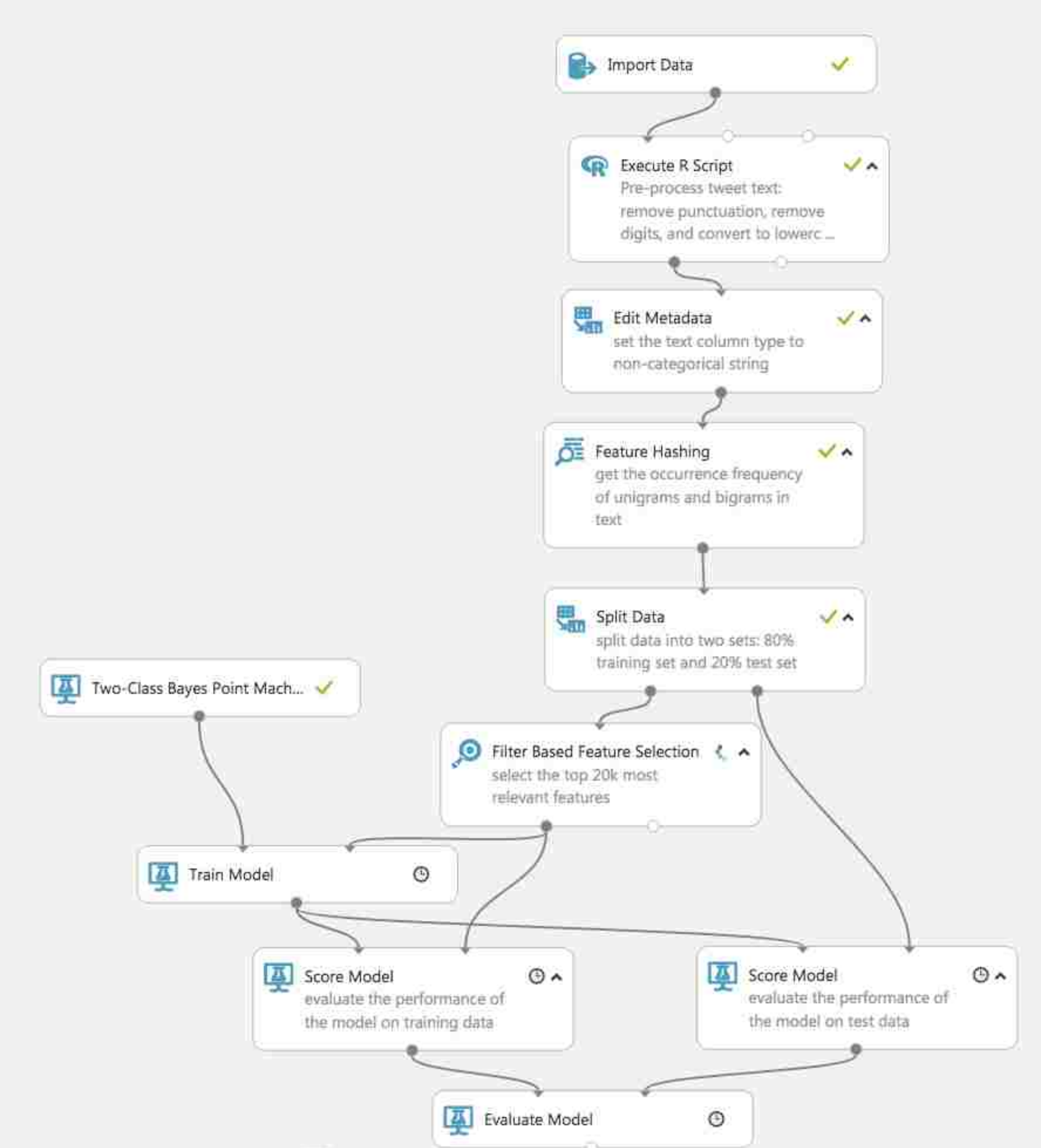

Import Data
Execute R Script
Pre-process tweet text: remove punctuation, remove digits, and convert to lowerc ...
Edit Metadata
set the text column type to non-categorical string
Feature Hashing
get the occurrence frequency of unigrams and bigrams in text
Split Data
split data into two sets: 80% training set and 20% test set
Two-Class Bayes Point Mach...
Filter Based Feature Selection
select the top 20k most relevant features
Train Model
Score Model
evaluate the performance of the model on training data
Score Model
evaluate the performance of the model on test data
Evaluate Model

Fig. 7. The machine learning process flow for sentiment analysis

For implementing facial expression analysis to support multimodal affect detection in Scenario 2, the OpenCV library for Image Classification is used in the Azure Machine Learning platform (Azure ML) along with a module for importing sample image data for classification. The results are then scored and evaluated using a custom R programming script. The machine learning process flow is illustrated in Figure 8 below.

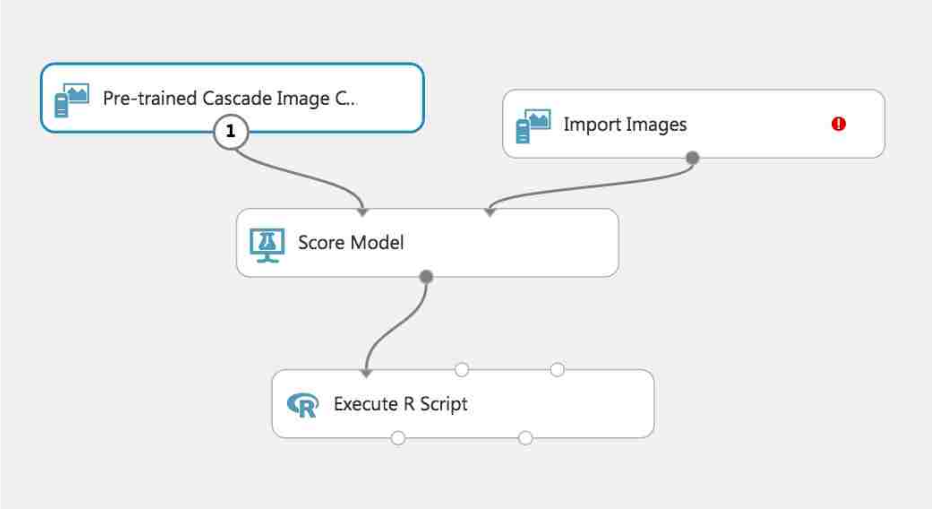


Fig. 8. The machine learning process flow for frontal face expression analysis

6) Algorithms

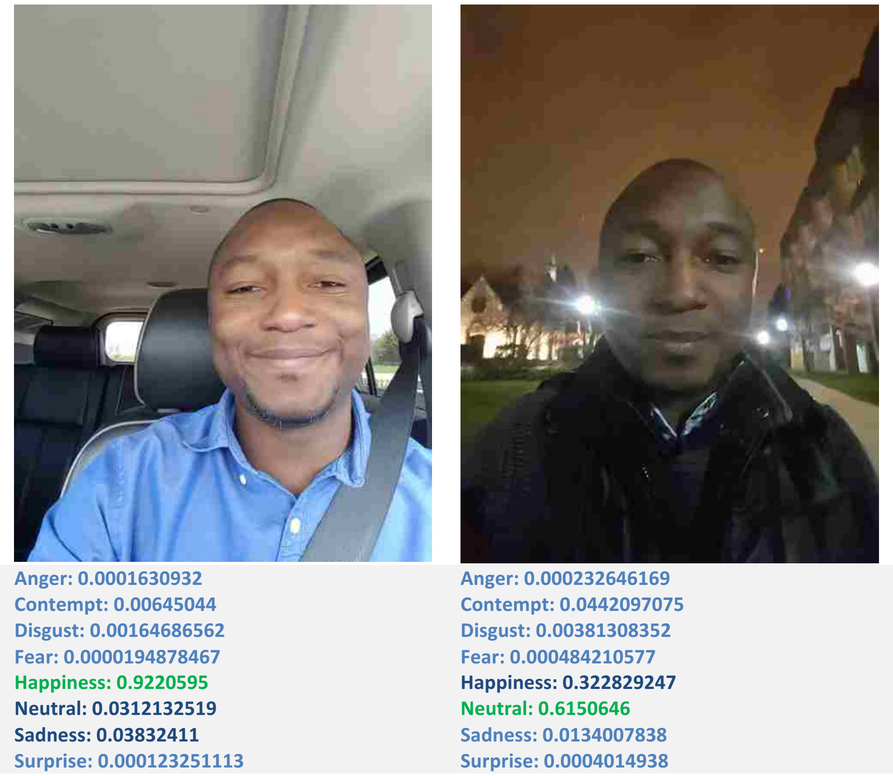
Three popular machine learning binary classification methods are employed to train the sentiment analysis model. I then score and evaluate the model to determine the most accurate algorithm for this type of cognitive intelligence task in the cloud. The supervised learning algorithms under investigation include:

- Bayes Point Machine [90]
- Support Vector Machine (SVM) [91]
- Neural Networks [92]

For the facial expression analysis problem, the Haar cascade [99] face detection algorithm (from the OpenCV frontal face detection library) is used to implement a robust and fast implementation of the face detection problem. The SVM algorithm was used to support emotion classification.

7) Limitations

The face detection and analysis approach used in this experiment is sensitive to light conditions and not applicable to side face detection. The best results are achieved with frontal face images. As depicted in Figure 9, the list of emotions under investigation in the facial expression analysis implementation are limited to: *Anger, Contempt, Disgust, Fear, Happiness, Neutral, Sadness,* and *Surprise*. Each face is assigned an emotional state based on the emotional state with the highest score calculated by the predictive classification model.



```
Anger: 0.0001630932
Contempt: 0.00645044
Disgust: 0.00164686562
Fear: 0.0000194878467
Happiness: 0.9220595
Neutral: 0.0312132519
Sadness: 0.03832411
Surprise: 0.000123251113
```

```
Anger: 0.000232646169
Contempt: 0.0442097075
Disgust: 0.00381308352
Fear: 0.000484210577
Happiness: 0.322829247
Neutral: 0.6150646
Sadness: 0.0134007838
Surprise: 0.0004014938
```

Fig. 9. Sample Results of the Facial Expression Analysis Model

In the *Sentiment Analysis* challenge, each dialogue sentence is evaluated to determine if it exhibits a *positive*, *negative*, or *neutral* sentiment.

C. Aim 2: Designing Content Personalization

As illustrated in the research study framework (in Figure 2), *Aim 2* will focus on the implementation of content personalization as a consumer of the cognitive features in the CI system.

1) Scenario Analysis

In investigating the key characteristics of an effective CI solution that relies on cognitive services, the following scenarios were investigated.

- ***Scenario 1***: Affect detection in a joke telling humanoid robot for elderly care companionship robot scenarios [38]
- ***Scenario 2***: Selecting motivational messages in persuasive dialogue scenarios aimed at curbing childhood obesity [23]

From a computational advertising perspective, online advertising (ad) systems often use "ad" relevancy and document content relevance information to target or rank ads with respect to a given document with content [38]. In the case of online ads, the general goal is to maximize ad revenue by serving up the most relevant ad that is likely to trigger a desired conversion action (which in the case of Ecommerce, often represents a purchase action).

In a similar fashion, I approach the problem of selecting the most relevant personalized content (e.g. jokes, movies, SMS messages) – representing an ad – by analyzing the relevance score of the various constituents of the personalized content based on attributes of the participating audience's demographic profile as well as other characteristics of the target content including its learned affective signal score when it was delivered to a similar audience. For example, a joke that is relevant to elderly people might not be relevant to middle-aged people. Hence, the need for content targeting.

2) Architectural Design

The system prototype affords human-robot interactions between the robot and one human, at a time. A logical view of the solution architecture is illustrated in Figure 5.

3) Research Challenges

Some of the key challenges associated with Aim 2 include:

- **Challenge 1*:*** The implementation of a computational model for content personalization through a recommender system
- **Challenge 2:** The implementation of a reinforcement learning model based on affective state.

4) Data Collection

In this case study experiment, I invited 14 people with varying demographic backgrounds to interact with the ZOEI humanoid robot in a joke telling HRI session. The age classifications explored for profile segmentation include: elderly people, middle-aged, and young adults. ZOEI's joke database was loaded with short jokes that were gleaned from various sources.

5) Methods

The jokes, in this scenario, were pre-classified as either "funny" or "very funny" jokes. Non-verbal actions were tagged to the various jokes to be interpreted and performed by ZOEI during the joke telling session. In this study, the humanoid robot interacts with the cloud data storage system through a web service hosted in a Cloud environment to retrieve pre-classified funny jokes to be uttered and acted out. Each joke has a non-verbal classification that allows the humanoid to deliver the joke with expressive gestures in an effort to exhibit believable behaviors. At the end of each joke, the humanoid robot prompts the human to confirm how funny the joke was and also indicate if he or she is interested in hearing additional jokes or funny tales. This approach supports the *feedback loop* implemented in the proposed framework to reinforce the derived emotion detected in this scenario. The human response in this scenario supports knowledge about the content (that is, the jokes) and also reinforces the previously detected emotion.

The dialogue system makes use of Automatic Speech Recognition (ASR), face and emotion recognition features. In addition, the Text-To-Speech (TTS) capabilities are used in combination with gesture interactions to convey human-like behaviors through a combination of verbal and non-verbal communications techniques. A web-based survey is used to collect additional affective state data during the HRI session by the human observer. Prior to the interaction session, anonymized participant demographic information is collected to help guide the content targeting features for selecting targeted jokes.

In the implementation of reinforcement learning for driving action (joke) selection, I employ the "∈-greedy" policy [56] which seeks to always pick a joke that has previously been confirmed as having the highest value of reward ("very funny") while considering the profile segment that the current user belongs to. Using some small probability ∈, the CI system will pick a random joke occasionally to explore alternative jokes that may or may not have been previously tested for the current user's profile segment.

6) Algorithms

The use of an unsupervised machine learning algorithm (specifically the k-Means Clustering algorithm) is proposed for identifying profile similarities and clustering demographic data that appears to be consistent with the affective signals collected for similar jokes.

Reinforcement learning is a machine learning technique that has been used with success in solving innumerable scientific puzzles including robotic navigation problems [56, 57]. It is quite akin to biological learning [56]. It falls in the middle ground between scenarios where an algorithm is trained on data that contains the correct answers to a problem (supervised learning) and scenarios where similarities in the data need to be explored for clustering (unsupervised learning) [56]. Reinforcement learning can be slow in its quest to exploit and explore various options in order to arrive at the best solution. This is not necessarily a concern, considering the fact that human standup comedians spend several years of trial-and-error runs to refine their comic performances and effectively target their jokes and funny tales appropriately to the right audience.

To help the system self-improve on selecting the best funny tales that have been known to work in the past based on the current context of it's audience, I employ the reinforcement learning technique which uses a search algorithm over a *state space* of possible inputs and outputs to maximize a *reward*. In this case study, the state space is a list of pre-classified funny jokes that need to be tested and ranked through trial-and-error. The pre-classified jokes are stored in a database that is accessible to the CI system through a cloud-hosted web service. The reward to be maximized in this case study is the current affective state of the human audience. The humanoid seeks to influence the human to obtain a very strong positive affective state score that will be indicative of how funny the robot's performance was.

In reinforcement learning, the learner (the humanoid, in this case) seeks to map *States* (attributes of the current audience member) to *Actions* (pre-classified jokes in the database) in an effort to maximize a numerical *Reward* (the affective state of the current audience). In the reinforcement learning cycle for this case study is illustrated in Figure 9 below, the learning *agent* (the humanoid) performs *action* (joke) a_t in state s_t and receives reward r_{t+1} from the intelligent environment, ending up in state s_t .

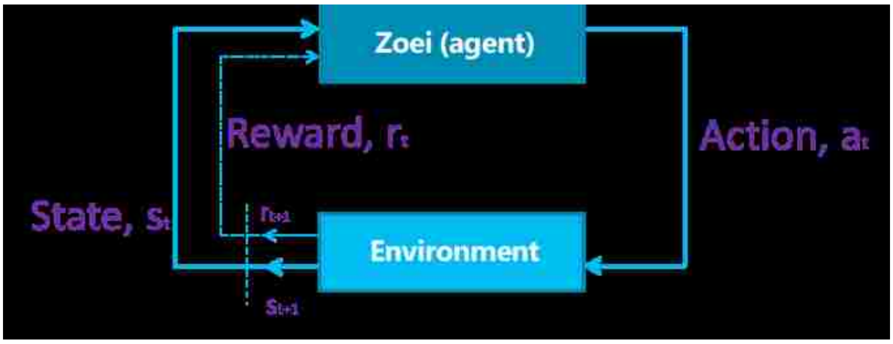


Fig. 10. The reinforcement learning cycle

7) Limitations

The humanoid robot is only capable of interacting with one person at a time.

D. Aim 3: Designing Security and Privacy Preservation

This aim is focused on exploring the best approach to implementing privacy preservation in Internet of Things (IoT) applications as well as the unique challenges inherent in implementing privacy-preservation in affect-driven personalization systems.

1) Scenario Analysis

Affective systems are capable of amassing highly personal, intimate and sensitive data regarding our everyday lives over long periods of time. Beyond the discovery of an end user's affective data (or bits), humans can be easily identified through image search capabilities. In some cases, these models can be susceptible to later reference for lawsuits, insurance claim issues, and prospective employee background checks [62].

While a person's emotional state might be useful for personalizing future funny jokes to entertain the individual (in the joke telling humanoid scenario), he or she is not likely to want to share that affective state information with third-party telemarketers who might find a person in a "good" mood, a prime candidate for receiving the best deals for today [62]. Yet, based on Leon et al.'s findings [59], if the advertising or deal of the day is specifically relevant to the user's mood, it might trigger a different type of welcoming response. Ultimately, end-users are going to be interested in having the ability to control who can access their affective bits.

Two use cases that I considered in an effort to validate the implementation of the reference model for confidentiality, include the following:

- ***Scenario 1***: humanoid robot as an interaction partner in an elderly care scenario
- ***Scenario 2***: humanoid robot as a health coach in a childhood obesity scenario.

In both scenarios, the human parties would expect to use the robot as a socially assistive partner with human-like social capabilities in lieu of treating it as a meager tool. In such interaction scenarios, the robot is expected to be able to exhibit communication skills by using natural language, emotion, and maintain social relationships over a period of time. In many persuasive health interventions, humanoid robots and other intelligent systems are capable of carrying out meaningful conversations with human subjects in an effort to influence humans towards behavioral or attitudinal change. In human-to-human conversations, the listening party often has the ability to discern whether or not certain aspects of the conversation should be kept confidential. Consequently, in conversational service robot scenarios (including elderly care use cases), it is assumed that humans will eventually expect humanized machines to be capable of preserving the privacy and confidentiality of human-robot dialogues [58].

2) Architectural Designs

I propose the use of a novel security, privacy and trust framework known as SPTP [47] as illustrated in Figure 11.

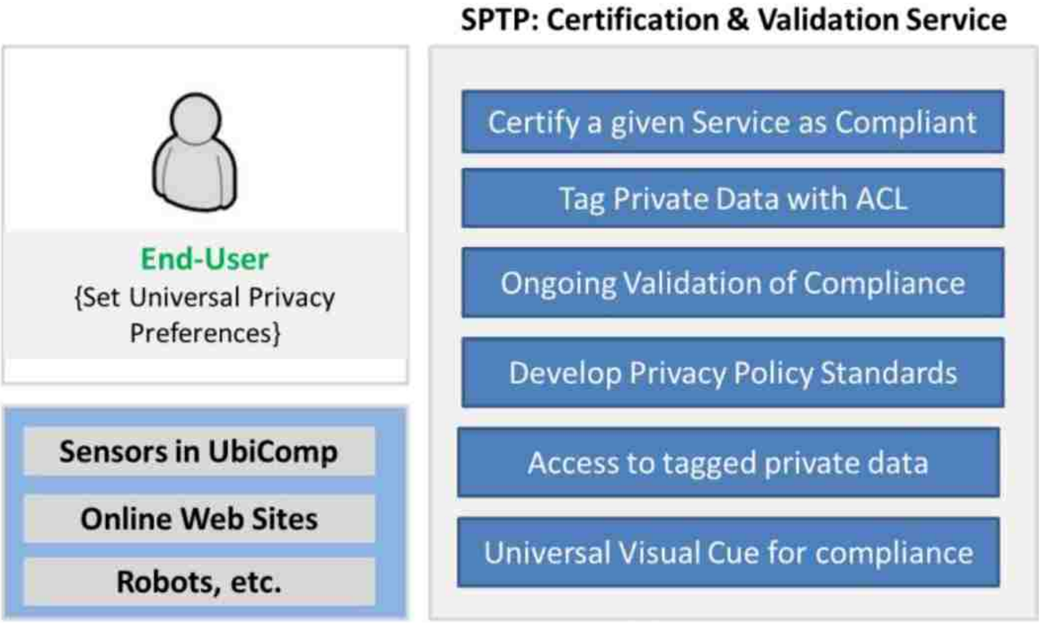

SPTP: Certification & Validation Service
End-User
{Set Universal Privacy Preferences}
Sensors in UbiComp
Online Web Sites
Robots, etc.
Certify a given Service as Compliant
Tag Private Data with ACL
Ongoing Validation of Compliance
Develop Privacy Policy Standards
Access to tagged private data
Universal Visual Cue for compliance

Fig. 11. Reference model for the SPTP protocol [47]

In addition, I propose the use of a conceptual reference model for preserving privacy in the IoT applications [46] – illustrated in Figure 12. Figure 12 offers an alternate approach to implementing privacy preservation in affect-driven systems. Security issues in integrating mobile agents and devices with services can be categorized as [65]: Confidentiality, Authentication, Authorization, Integrity, Nonrepudiation, Privacy, and Availability. I propose a reference model for detecting both implicit and explicit *confidentiality* in HRI dialogue systems as depicted in Figure 14 below.

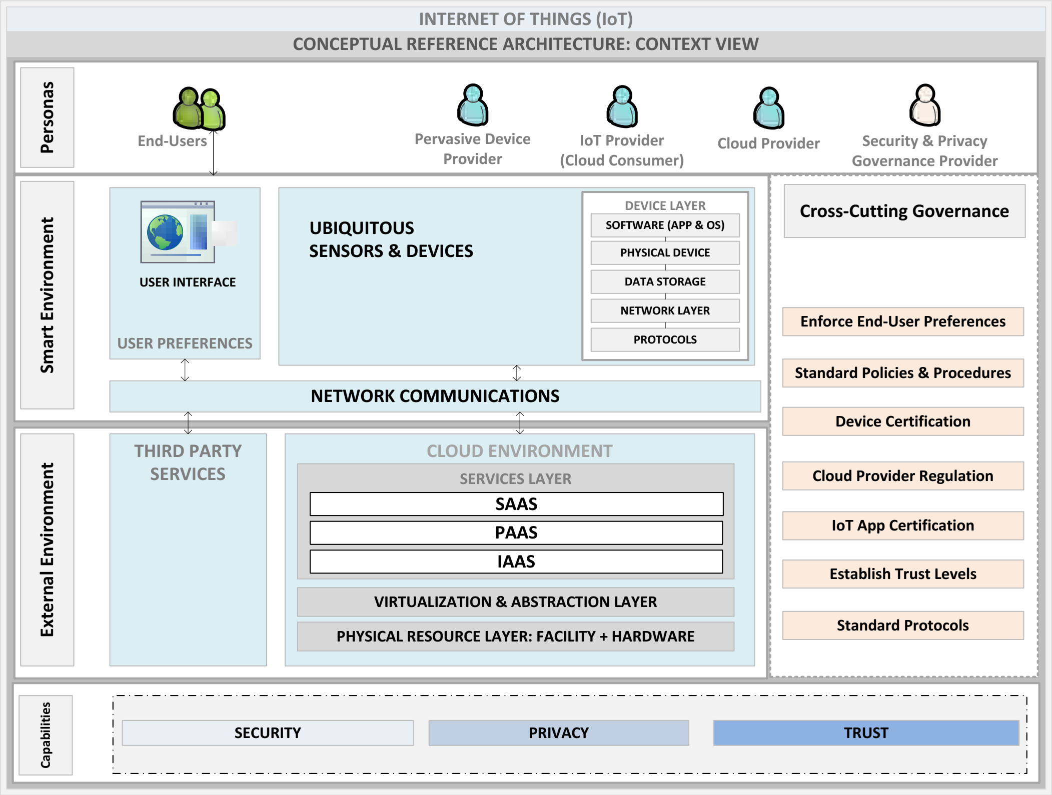


Fig. 12. Conceptual reference architecture for IoT Apps [46]

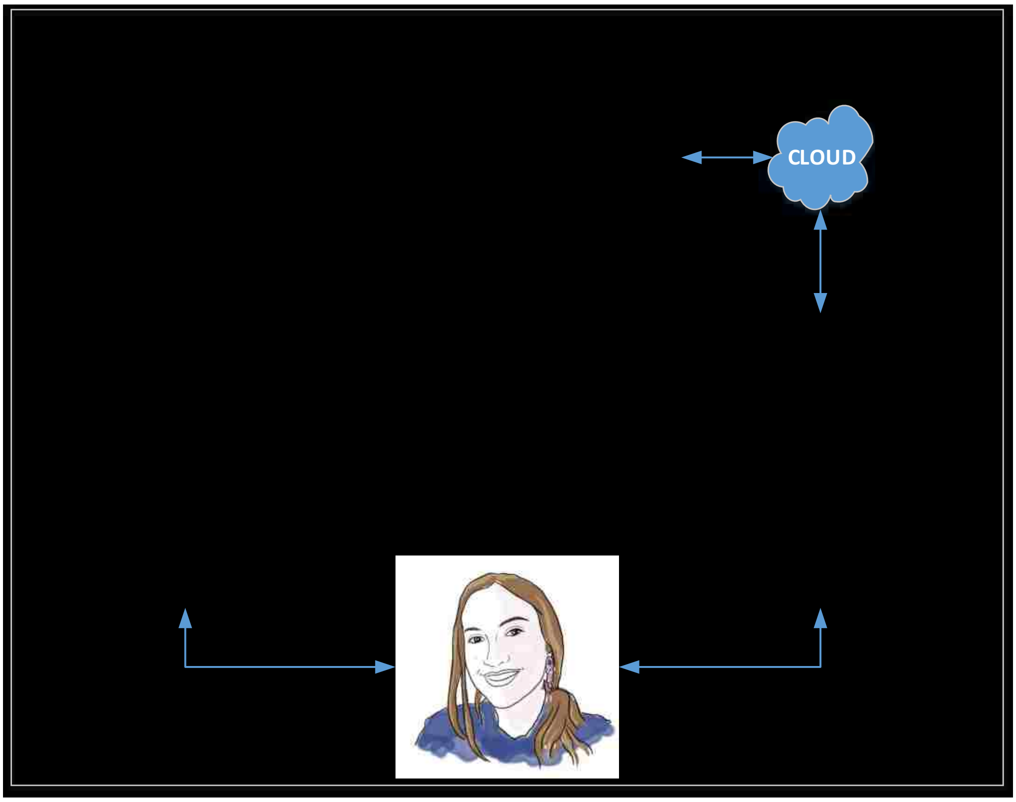


Fig. 13. Logical View: ADPL Privacy Preservation Reference Model [58]

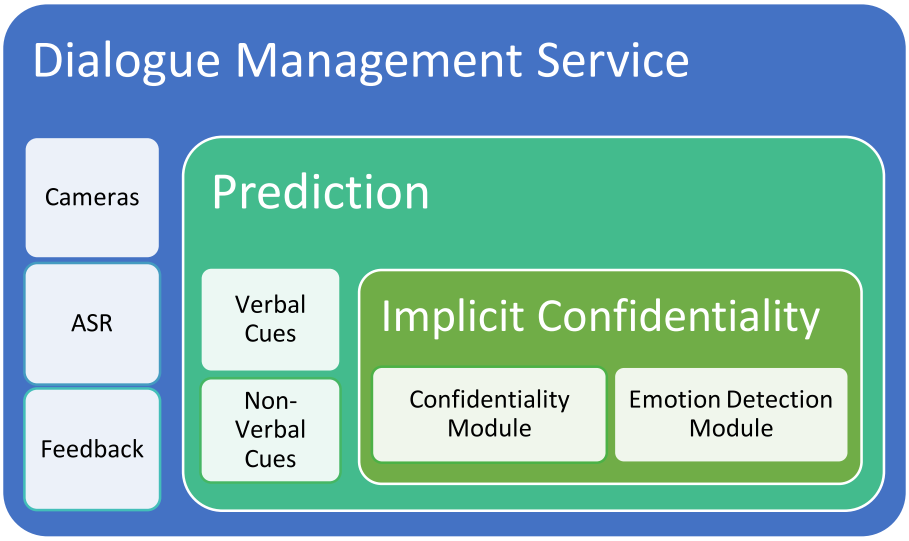


Fig. 14. Reference Model for Dialogue Management Systems [58]

3) Research Challenges

Some of the challenges inherent in this problem include:

- **Challenge 1:** Privacy preservation in IoT applications. Foner [63] contends that privacy protection in networked agents is a challenging research problem.
- **Challenge 2**: Investigate privacy preservation in affect-driven personalization scenarios
- **Challenge 3:** Detecting implicit and explicit confidential information in conversational agents

4) Data Collection

To test the hypothesis that the reference architecture is feasible for most modern IoT implementations, I reviewed the implementation of security and privacy solutions aimed at achieving trust in the two scenarios (among others) and compared the inherent layers in the scenario to that of the proposed conceptual reference architecture.

In addition, I built a prototype of the case study described in this paper and shared the way in which various security and privacy concerns are addressed in the solution with a few Information Technology (IT) practitioners. I collected feedback from these end-users through a survey to gauge their comfort level with the implementation of security and privacy solutions at various layers of the conceptual model.

5) Methods

Of the 18 distributed end-user surveys, I received 14 usable responses with questions centered on evaluating the importance of the various facets in the reference architecture and how it affects their overall level of trust in the IoT system:

- Trust in the underlying Cloud data storage system
- Trust in the ubiquitous devices and user interface
- Trust in the vendor services involved in the IoT App
- Need for a third-party regulating body

Participants (end users) were asked to indicate their rating with a scale of 1 through 3 (where 3 means the characteristic is *Important*, 2 represents *Indifferent*, and 1 denotes *Not Important*).

In addition, I will qualitatively evaluate various IoT and HRI systems that have been implemented in the past to determine their goodness of fit or relevance to the proposed privacy framework. For the confidentiality model, I plan on quantitatively evaluating the performance of the various classification algorithms involved.

It is important to quantify the performance of the selected classifiers in a bid to measure and improve their accuracy. The available data set will be split between the Training Set and the Test Set using the 80:20 split ratio. The classifier will be trained using the 80% set and evaluated with the remaining 20% of the data set. The classifier accuracy will be measured as a percentage score of the test data points that are correctly classified by the classifier. I propose the use of ROC curves for comparing the various models. I expect a greater area under the curve (AUC) to indicate a more accurate model. The Gini-statistic can also be computed from the ROC curves.

I also propose the use of the K-fold cross-validation estimator as opposed to the hold-out approach as a technique for minimizing potential prediction errors in scenarios where the dataset under evaluation is limited in size and likely to be sensitive to the data partitioning approach. With this approach, I will divide the training set into *k* (=10) folds and use the *k*th fold for testing each of the planned *k* experiments. This will help minimize variance-related issues pertaining to an unfortunate data split.

6) Algorithms

Multiple classification algorithms including the following can be evaluated to dynamically select the best algorithm or model for a given set of input features: Support Vector Machines (SVM), Boosted Decision Tree, Regression Trees, Random Forests, Neural Networks, and Nearest Neighbors.

7) Limitations

There are other aspects of trust and ethical issues that are not covered in this study.

E. Aim 4: Cloud Resource Optimization

In this Aim, I seek to investigate some best practices for ensuring high-availability, scalability, disaster recovery, and high performance. Over the past couple of years, we have witnessed several cloud outages across multiple high-profile cloud providers who are otherwise considered to be widely reliable in terms of cloud service uptime [54]. Unfortunately, when a cloud provider experiences an outage it can have a major financial and functional impact on mission-critical applications hosted on the provider's infrastructure. Collective intelligence systems can be integrated into mission critical healthcare systems which require maximum uptime and high performance, hence the imminent need to delve into this facet.

1) Scenario Analysis

To help investigate this facet of the proposed framework for human-centered collective intelligence systems, I evaluated the implementation of this proposed framework component in an mHealth persuasive systems for supporting behavior change in a Smoking Cessation intervention [49, 50]. The text-message-based motivational system was deployed "live" with a centralized cloud backend hosted in the Microsoft Azure cloud and kept operational for over a three-year period without a reliability incident.

In addition, I implemented a prototype solution for delivering web-based personalized movie recommendations and video streaming content. While this was not a mission critical application, the web site was deployed to both the Google App Engine and the Windows Azure PaaS platform to validate the proposed framework. An SLA Monitoring Agent was also deployed to both clouds, taking into account the reference architecture described earlier. The active cloud was defined as the Windows Azure cloud whereas Google's App Engine represented (Cloud B) the passive cloud platform.

The Movie Recommendation Application (App) features static image content which is stored on the cloud storage service and other Software-as-a-Service solutions as well as Facebook [107]. Other data elements served on the web site are dynamic in nature and can be supplied to the end-user through a database call invoked by the web application based on the user's interaction with the application.

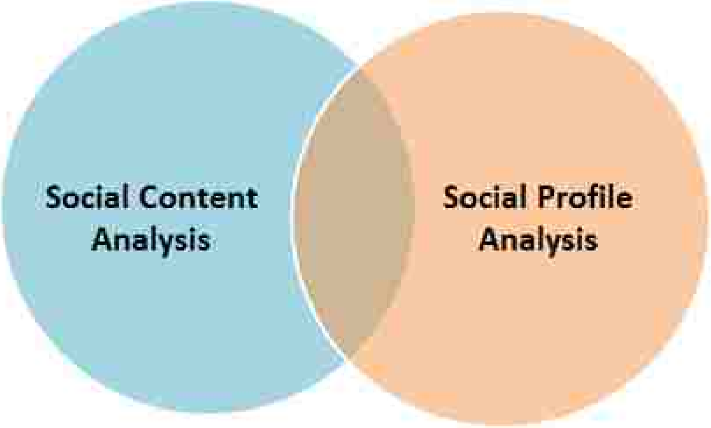


Fig. 15. SMI Problem Classifications [48]

With the two types of SMI classifications presented in Figure 15 in mind, I embarked on the implementation of two case studies that cover the spectrum of SMI analysis. From a Social Profile Analysis standpoint, I examined what goes into building a movie recommendations cloud service that pulls social insights from the movie preferences of a given user's Facebook friends as a form of input signal for ranking personalized movie recommendations. This solution was deployed as a web application service hosted on the Microsoft Azure cloud platform. In addition to this case study, I implemented a sentiment analysis solution for evaluating Social Media Content, that is, Twitter messages (or tweets) by utilizing the Amazon AWS cloud platform for Elastic MapReduce (EMR) including Hadoop.

2) Architectural Design

In creating a generalized reference architecture for improving high availability in cloud-provider-down conditions, I offer a cross-cloud hybrid Platform-as-a-Service (PaaS) solution illustrated in Figure 16. On the other hand, Figure 17 depicts a reference model for selecting various cloud resource options for a given SMI analytics task.

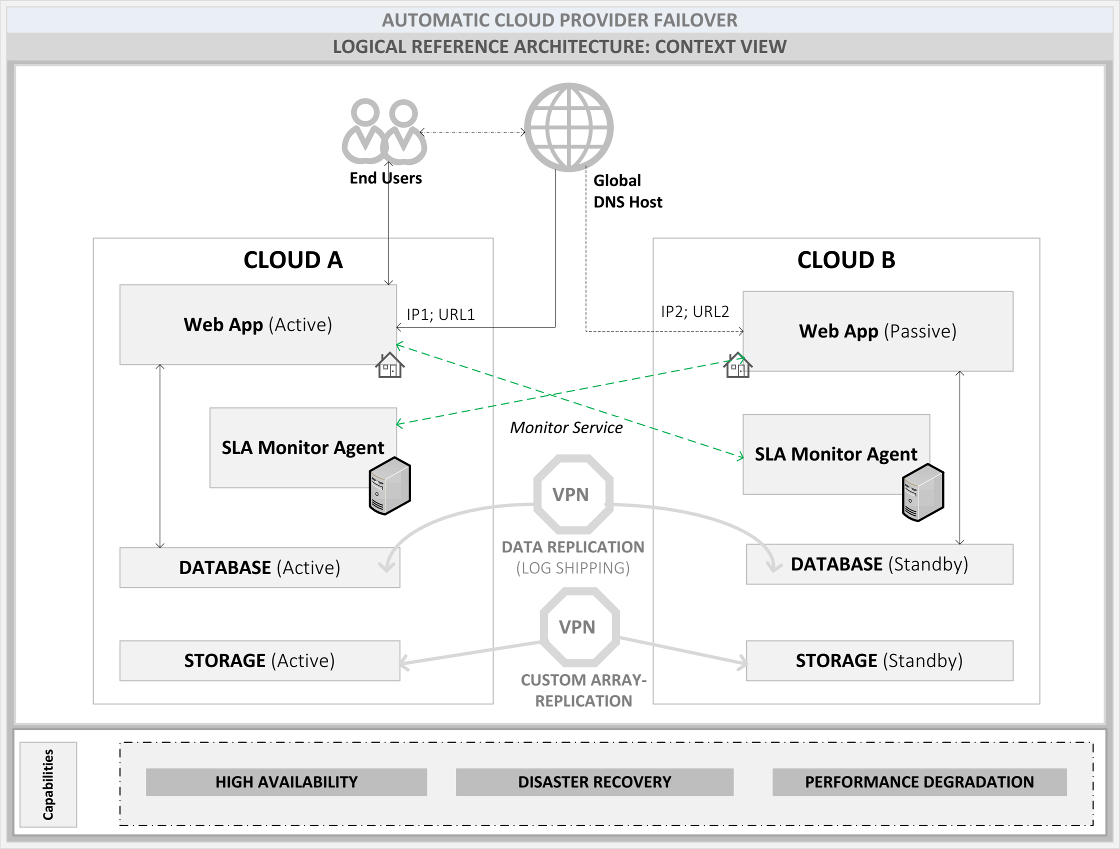


Fig. 16. Reference Model for Cross Cloud Failover [58]

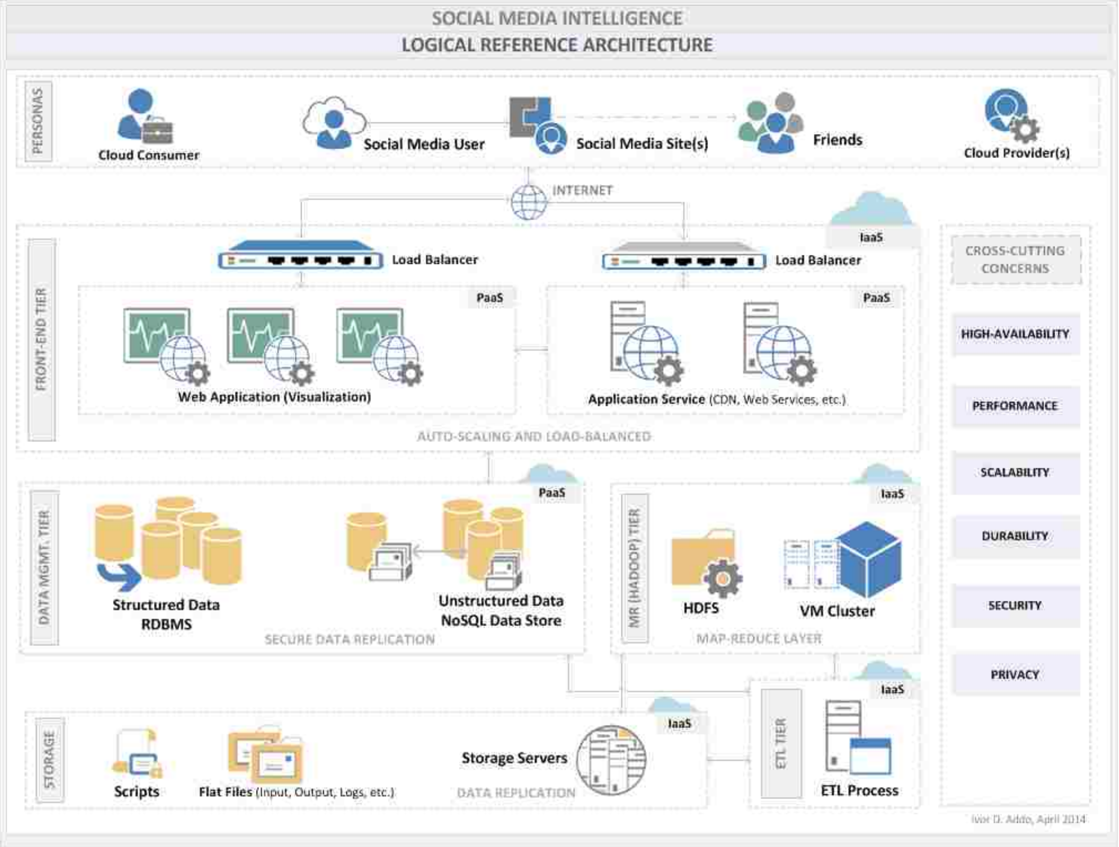


Fig. 17. Logical View: Reference Architecture for SMI Solutions [48]

3) Research Challenges

Some of the prevalent challenges in implementing cost-effective cloud solutions that support automatic scaling and require the least infrastructure management overhead include:

- **Challenge 1:** Portability and fault-tolerance PaaS cloud design
- **Challenge 2:** Selecting the most effective cloud resources within a given cloud provider's portfolio to support collective intelligence

4) Data Collection

I executed a simulation for automatic cloud failover to investigate the viability of using the proposed approach for *Challenge 1*. I collected a few metrics during the experiment to confirm feasibility. For challenge

5) Methods

To test the hypothesis that the proposed reference architecture associated with *Challenge 1* is feasible for most mission-critical PaaS hosted applications, I created a prototypical web application as described in the case study. The executed simulations include:

- Cloud service outages, and
- Severe performance degradation introduced in the target application

For Challenge 2, I also designed a reference architecture by surveying various SMI projects through qualitative analysis and addressing common cross-cutting concerns in using cloud resources for collectively intelligent data mining tasks.

6) Algorithms

I implemented a custom *fault recovery algorithm* that is inspired by that of Saha and Mukhopadhyay's proposed approach [70]. The two *status* conditions under which a failover will occur include situations where performance degradation in a given Cloud

Provider is detected by the SLA Monitoring Agent or the active Cloud Provider is down.

Inputs:

- n: number of cloud providers (for example, n=2)
- k: critical application dependent cloud services
- r: retry interval in milliseconds (for example, r=500)
- s: number of retries
- p: performance degradation threshold (milliseconds)

```
Logic for a given active cloud $i$, $0 <= i <= n - 1$

if $CLOUD\_FAILOVER_i$ = FALSE; // the active cloud
  for all cloud services $k$ executing in cloud $i$

      perform a $STATUS_k$ check;
      set $STATUS\_TIME_k$ to elapse time
      if $STATUS\_TIME_k > p$
        or $STATUS\_TIME_k$ == TIMEOUT
          set $FAULT\_FLAG_k$ = TRUE; // save the fault on k
          for $j = 1$ to $s$
              perform a $STATUS_k$ check;

              if $STATUS\_TIME_k > p$
                or $STATUS\_TIME_k$== TIMEOUT;
                   if $j == s$ // retry complete
                      set $CLOUD\_FAILOVER_i$ = TRUE;
                      initialize FAILOVER;
                   else
                      sleep for $r$ milliseconds; // retry to confirm
                      $j = j + 1$;
                   end if

              else if a recent $FAULT\_FLAG_k = TRUE$ is found

                  set $SPORADIC\_FLAG_k$ = TRUE;
                  set $CLOUD\_FAILOVER_i$ = TRUE;
                  initialize FAILOVER;
                  exit for; // note sporadic issues
              else
                  exit for; // false alarm save fault on k and exit

              end if
          end for
      end if

  end for

end if
```

Algorithm 1: Failover Fault Discovery for Cloud *I* [54]

7) Limitations

The model is predicated on the assumption that it is very rare for two major cloud providers to experience a down condition concurrently. As a result, the scope of the investigation is focused on utilizing two major public cloud PaaS providers. Though, in extreme cases, the model can be extended to accommodate more than 2 cloud providers.

IV. DESIGNING ZOEI – HUMAN-CENTERED CI

A. Characteristics of the ZOEI framework

As shown in Figure 1, the proposed reference architecture for building human-centered collective intelligence solutions showcases multiple interchangeable components depending on the specific application scenario under investigation. However, I argue that conceptually, CI applications will typically include the following generalized layers, components and characteristics:

- A *smart human-machine interaction environment* involving:
    - one or more *smart agents, devices, sensors* and
    - one or more *human subjects*
    - a means for detecting and exhibiting socially expressive *human-machine interactions*
- An optional *external environment* space (outside the smart interaction environment) where additional information (e.g. social media, the weather, etc.) can be gleaned to support a centralized knowledge management or intelligence system
- A resource-optimized and cost-effective *centralized knowledge store* – preferably hosted in a *cloud* environment – to support the multitude of smart agents that will need to collaborate with each other and share knowledge through interaction with:
    - Real-time *data stream storage* solutions, and
    - A set of *trained predictive models* and *integration services*
- Cross-cutting architectural concerns including but not limited to the following quality attributes: *security, privacy, trust, ethics, ease of use, reliability, recoverability, performance, scalability, availability* and more.

Cross-cutting architectural concerns like privacy, security and performance are usually relevant to multiple environments in the CI solution space, as depicted in the conceptual model in Figure 18. While, peer-to-peer (P2P) and machine-to-machine (M2M) network communication patterns can be useful for facilitating collaboration across swarms of collective agents, I propose a centralized intelligence data store as an effective (client-server) approach to simplifying the distributed collaboration needs of the smart agents in the solution space.

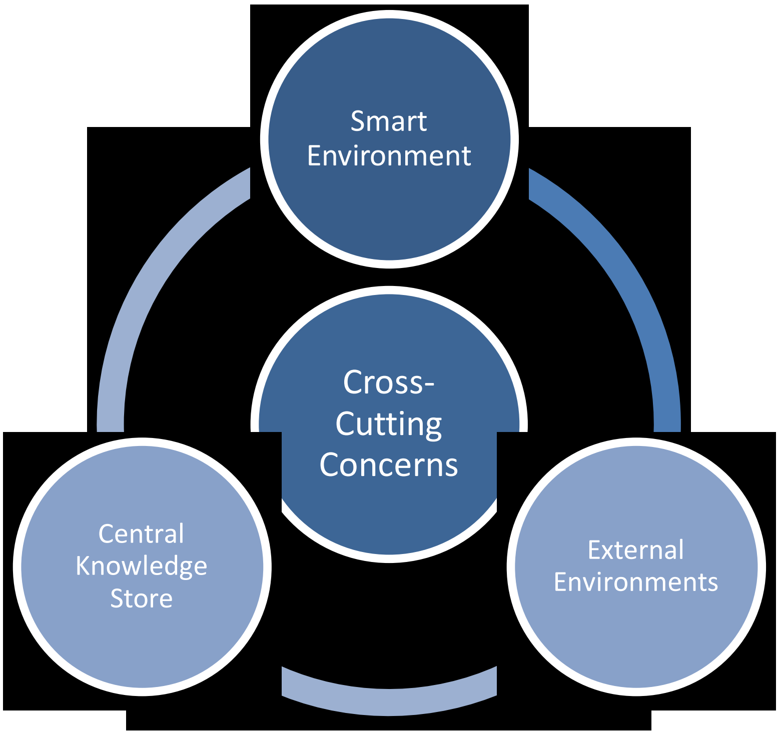


Fig. 18. The ZOEI framework – Conceptual Model

In the logical reference model expressed in Figure 1, the *human-machine interaction* (HMI) patterns in the *smart environment* makes use of *computer vision* techniques (supported by cameras) and *spoken language understanding* (SLU) via ASR features to represent the collective *eyes* and *ears*, respectively of the smart agent. These input signals support the detection and recognition of both verbal (e.g. speech) and non-verbal cues (e.g. posture, facial expression, etc.) in the multimodal HMI environment. To support a “believable” bidirectional interaction between the smart agents and the human subjects involved, output signals involving Text-to-Speech (TTS) features, among others are utilized to generate and demonstrate socially expressive behaviors. Through the use of a *feedback loop*, discerned cognitive features detected in the smart environment (e.g. emotion) can be confirmed and reinforced through HMI. Additional *individual* and *aggregate* data sources including social media content (captured in the external environment) can be leveraged to augment the collective intelligence held in the *central knowledge store*.

B. Architectural Concerns

Software architecture is an important transferable system abstraction that is useful for communication among several system stakeholders and supporting the early design decisions that govern the target solution [95]. The proposed architecture model seeks to provide a yardstick for driving HCCI system design discussions. In the proposed reference architecture, the cross-cutting concerns are investigated to ensure reliability and trust between the human subjects and the target system. The non-functional requirements for the CI system should itemize key cross-cutting concerns for the system.

I argue that *high availability* can be a critical concern in implementing mission-critical CI systems. Although, it is not always the case, availability tactics including fault-detection, recovery and prevention are often expected by end users across the solution space [94]. In the central hosting environment (e.g. *cloud*), there is often a need to *scale* the solution automatically as additional smart agents are employed. The ability to recover from various types of disasters (especially in a mission-critical solution) is of importance in an operationalized solution.

Performance, in terms of the response time involved with processing data within the smart environment and alternatively processing it through the centralized knowledge store becomes a basis for tradeoff analysis. When small ubiquitous sensors are involved in the smart environment, computational overhead and efficiency, data storage constraints, network communication bandwidth, memory, and other resource consumption constraints will need to be evaluated to determine how much data processing should be performed on the local devices involved versus in the centralized "cloud" environment. When the smart environment supports faster network access mediums including wireless fidelity (WiFi), most of the data processing can be offloaded to the centralized family of backend services. However, in slower bandwidth areas and in occasions where online access is not available, the system will not to be able to adjust to some level of offline storage and processing. Minimizing or eliminating resource contention (hence, blocked time [95]) is of equal importance in the proposed tradeoff analysis.

In some cases, the smart environment might be portable. Smart agents and sensors might be used interchangeably to collaboratively solve complex problems. To ensure reliability and instill trust from the human subjects, privacy, ethics and security concerns must be addressed across the solution space. When humans are involved, ethical and privacy-preservation concerns must be considered very carefully. I argue that this cross cutting concern must be tackled as part of the design of the solution rather than as an afterthought.

C.Illustrative Application Use Cases

While there are several human-centered CI applications that can be drawn on to evaluate the efficacy of the proposed reference model, I will focus on 4 major CI application scenarios as case studies for highlighting the key tenets of the proposed model and driving its evaluation. The application scenarios involved include:

- *Use Case 1*: Designing a humanoid health-coach for Childhood Obesity intervention
- *Use Case 2*: Designing a joke telling humanoid robot in social entertainment
- *Use Case 3*: Designing an mHealth-based Smoking Cessation intervention
- *Use Case 4*: Designing an affect-driven movie recommendation system

In the following section, I will describe how each of the listed scenarios fits the human-centered CI problem space. Subsequent chapters will evaluate the aforementioned challenges of this research study in relation to specific components of these application scenarios.

D. Use Case 1: Humanoid Health Coach for Childhood Obesity

As illustrated in Figure 19, this application scenario seeks to encourage kids to interact with a NAO T25 humanoid robot (acting as a health coach) in a bid to spark an interest in physical exercises and healthy diet choices.

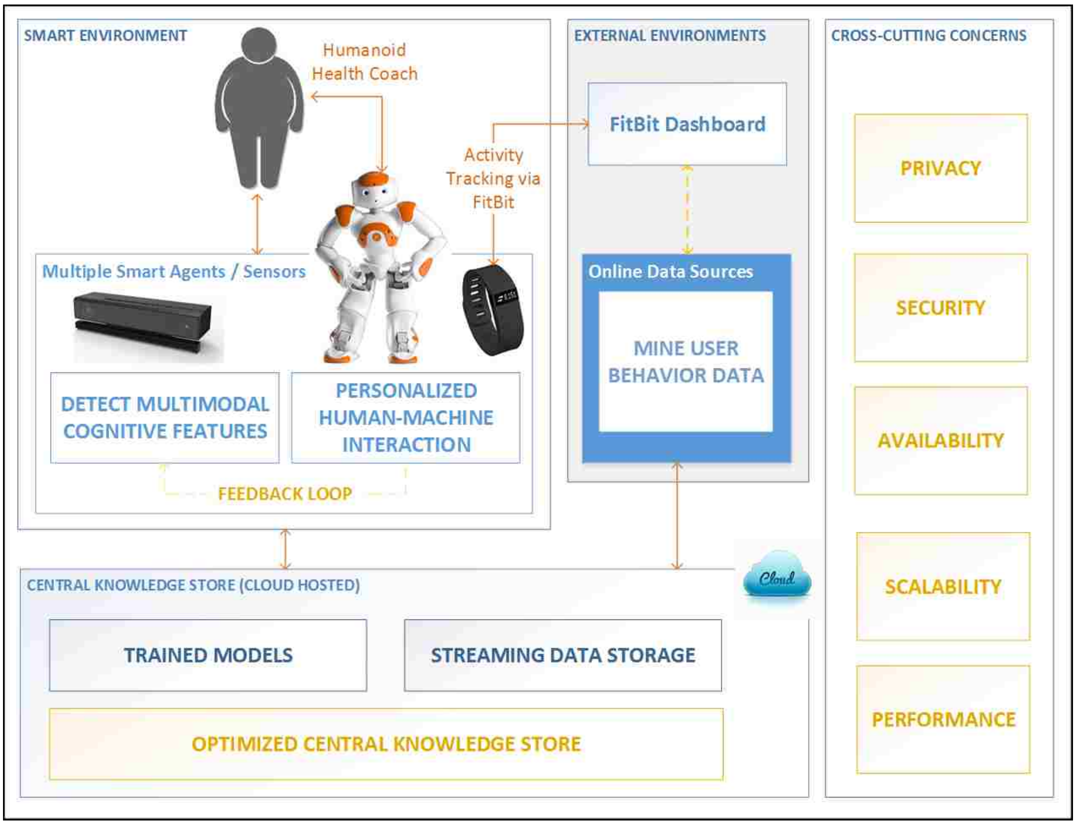


Fig. 19. Humanoid Health Coach in Childhood Obesity Intervention – Logical Model

In this application scenario, the smart environment involves the use of a Fitbit Charge sensor device for tracking physical activity including calories burned, miles walked, steps taken, and stairs climbed. The sensor device syncs the data collected about the individual to an external dashboard web site. This case study regards the online dashboard as being in the external environment layer of the ZOEI framework. The NAO T25 robot and the Kinect for Windows v2 platform are used in the smart human-machine interaction space. The robot gleans intelligence from a centralized data store that keeps physical activity data extracted from the Fitbit dashboard and augmented by unstructured human subject data aggregated from interactions with the child (by using motivational interviewing techniques) and stored in the cloud hosted environment.

Privacy of the end-user data captured in this scenario is the most important cross-cutting concern. Facial recognition and emotional intelligence in the HRI dialogue are critical cognitive features in this scenario. By implementing a facial recognition feature, the HRI dialogue is personalized to suit the human subject in the HRI dialogue.

E. Use Case 2: Affective Entertainment Humanoid Joke Teller

Cynthia [24] posits that attempts at nurturing human technology relationships will be bolstered among humans if the technology in question, is capable of displaying rich social behavior. Emotion detection and generation often enhances the perception of a humanoid robot as a believable human-like system. As robots take on human-like behaviors, they tend to apply acting skills to demonstrate their sociable skills. In normal human to human dialogue, knowing the right things to say to someone in an effort to influence their perception is often encouraged, particularly, when it comes to showing that one cares or loves someone. One of the core tenets of a service or care robot in an elderly care scenario is predicated on the idea that the robot exudes the feeling of compassion in a way that reassures the elderly person that the robot genuinely cares about the participant.

As I dissect the human signals that go into demonstrating care among humans, some of the recurring themes that often bubble up include trust and compassion. Compassion in a care robot might necessitate the expression of sympathy in the humanoid when the human companion is in a sad emotional state or mood. Beyond the expressive display of sympathy, the care robot might be able to influence the human's emotional state by trying to cheer up the human while maximizing its contextual awareness of the human's current emotional state [38]. For example, if the human is in an excited state, the robot might need to imitate that emotional state by showing expressive behaviors that are synonymous with excitement.

The case study for this experiment [38], explores a scenario where the humanoid robot is focused on entertaining the human counterpart by telling jokes. The hypothesis of the study is grounded on the idea that by refining the robot's content selection algorithm based on feedback signals collected about the human's affective state, the system can progressively tell funnier jokes and effectively influence the human's emotional state.

As illustrated in Figure 20, I utilized the NAO T14 humanoid robot built by Aldebaran Robotics along with Microsoft's Kinect for Windows sensor as smart devices in the smart environment. The NAO T14 is a humanoid torso robot with 14 degrees of freedom (2 on the head, 5 in each arm and 1 in each hand), 2 cameras, 2 lateral speakers, and 4 microphones. In support of human-centered collective intelligence, the ability of the CI system to draw from the accumulated knowledge in recommending relevant and personalized content to the interacting users remains critical. The robot worked in concert with the Kinect sensor to monitor affective state. A human observer was allowed to collect affective state data for validating the gleaned affective state picked up by the sensors in the smart environment. I used a cloud-hosted web service as an integration medium for communicating affective signals as well as user profile data gleaned from both the Kinect Sensor and the humanoid. In this scenario, the external environment consists of a number of online funny jokes databases. Using a screen-scraping utility program, I crawled joke content from those web sites, cleansed the data and uploaded them to the cloud-hosted data store. The reinforcement learning approach was used to train the model for recommending jokes to the humanoid robot based on the human's previous emotional response to similar jokes. The most prevalent cross-cutting concerns in this scenario involve privacy preservation in the smart environment as well as the performance of the cloud-hosted solution in generating personalized jokes.

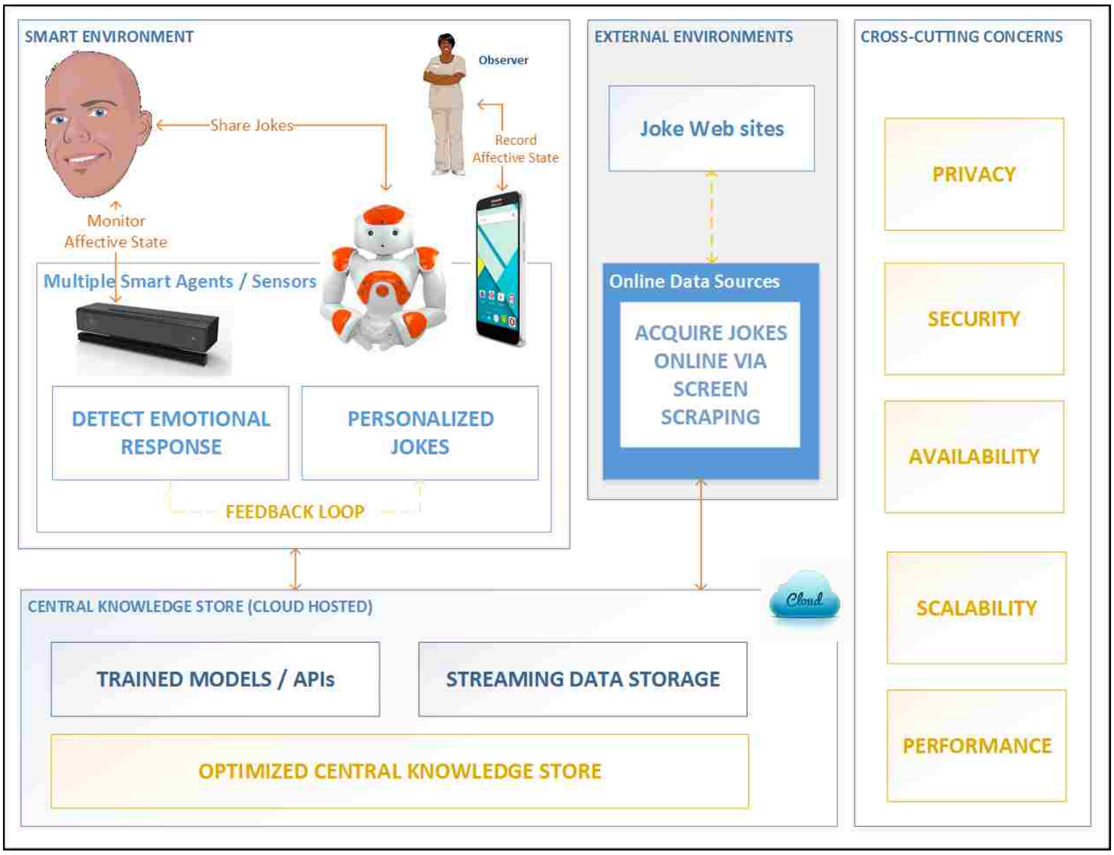


Fig. 20. Joke-Telling Companion Robot in an Entertainment Scenario – Logical Model

F. Use Case 3: mHealth Smoking Cessation intervention

In the mHealth Smoking Cessation use case, motivational SMS messages were personalized for the human subject based on his or her current stage in the progression towards smoking cessation abstinence [49], in addition to messages that the human subject had personally indicated as being motivational, as well as how recently he or she had received a given motivational message. An SMS server was utilized to call a cloud-hosted web service in the Microsoft Azure Cloud and subsequently distribute the personalized SMS messages on 3 times a day to motivate participants towards cessation.

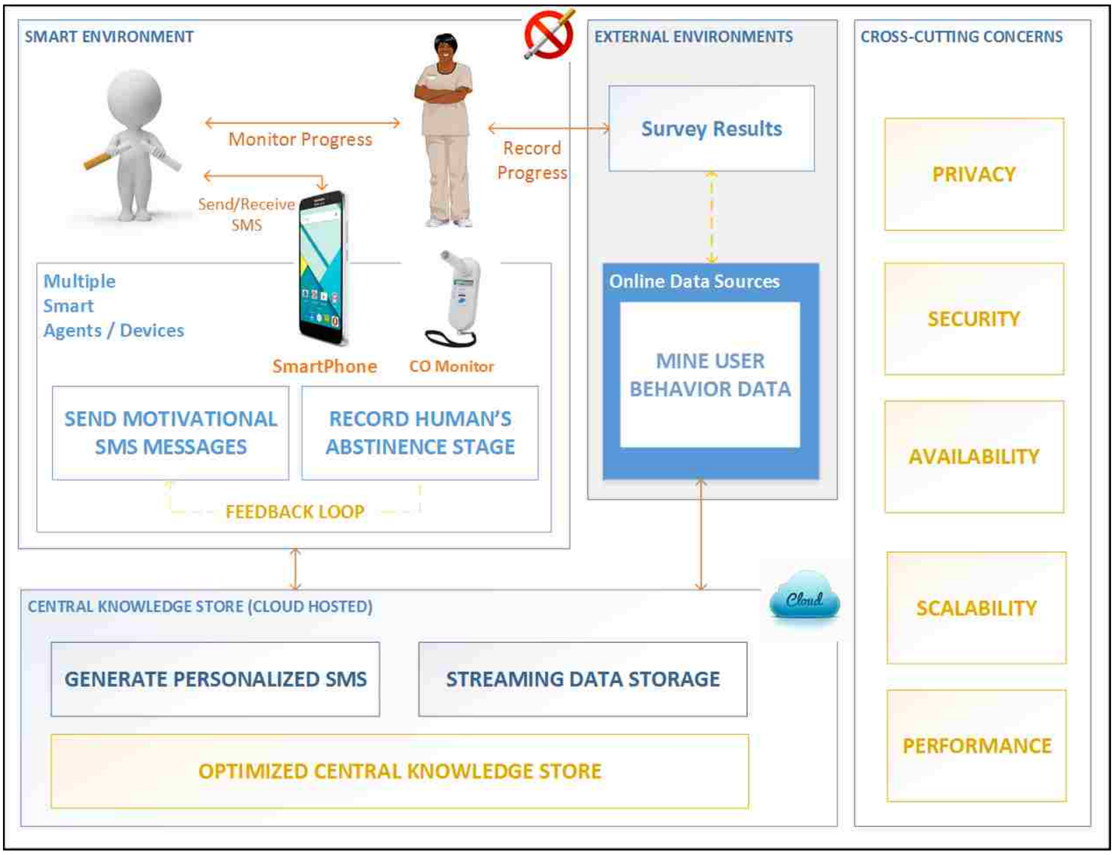


Fig. 21. mHealth Smoking Cessation Intervention – Logical Model

The user's smartphone was utilized to receive the motivational messages. In some cases, the participants responded to the SMS messages in an attempt to have a conversation with the motivational software agent. The level of carbon monoxide in the human subject's exhalation was measured by using a carbon monoxide breath monitor (breath CO monitor) as clinical aid for assessing carbon monoxide poisoning. In addition, the human nurses visited participants in the study on a weekly basis and recorded their survey results in a cloud-hosted data store. The results of the survey were mined and used to determine the human's stage in the abstinence continuum and hence the type of custom messages that will be appropriate to motivate behavior change. In essence, the survey acted as a *feedback loop* for further personalizing the SMS messages.

This research study was implemented for a 3-year period commencing in the Fall of 2013. The key cross-cutting concerns in this use case were *privacy* preservation of the individuals involved in the study as well as *high-availability, performance* and *reliability* of the system for generating and sending SMS messages as well as holding the survey results data.

G. Use Case 4: Affective Movie Recommendation System

In this scenario, a user is able to watch multiple movie trailers on a tablet device (iPad) as well as through a Kinect for Windows mounted TV in the smart environment. As illustrated in Figure 22, the user's emotional response to the movie trailers (mined from the YouTube video service) are used to rate the movies (on a scale of 1 through 10) which invariably serves as a *feedback signal* for influencing movie recommendations for the user in question. The ubiquitous Kinect Sensor device is used to identify specific users assembled in front of the family TV. Information garnered from the Kinect sensor is transmitted through a mobile service to the cloud storage location.

A cloud-hosted movie recommendation model leverages previous media content viewing patterns and the preferences of influential people in a particular household user's circle of online social network (OSN) friends to recommend future movies that will be of interest to the user. In the *external environment*, the Internet Movie Database (IMDB) [106], the YouTube Player Application Programming Interface (API) [108] as well as the OSN Facebook Graph's API [107] are used to mine data about movies as well as user preferences regarding movies based on their social profile. Data mined from the Facebook Graph API in the *external environment* along with the aggregate affective response of a user to similar movie trailers (collected in the *smart environment*) are employed to infer the preferences of influential friends in a given household member's OSN circle as well as the YouTube API [108] for streaming movie trailers. A trained recommender system hosted in the Microsoft Azure cloud is used to build a model for movie suggestions. The most critical cross-cutting architecture concern in this scenario is end-user privacy.

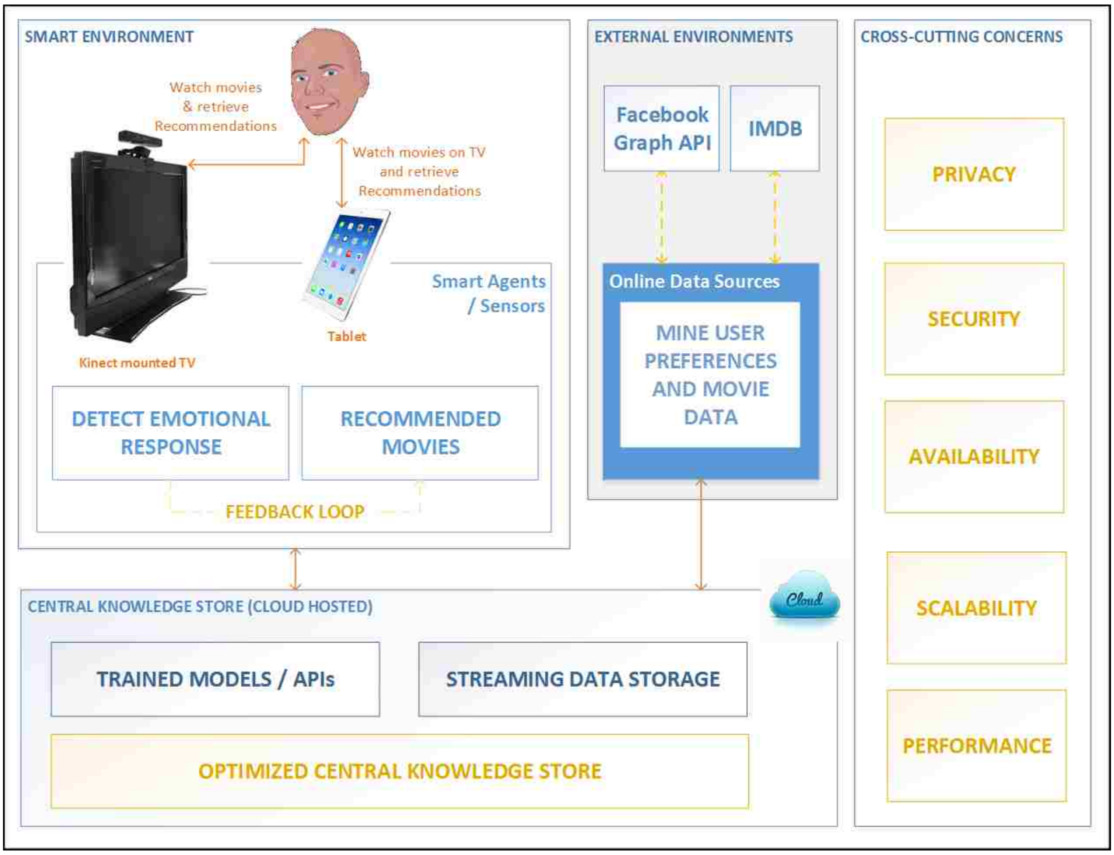


Fig. 22. Affective Movie Recommendation System – Logical Model

H. Evaluation

In evaluating the proposed reference architecture, I investigated various components of the framework (using a series of experiments) in the context of the use case scenarios itemized in this section. In addition, I offer a *goodness-of-fit* comparison of the 4 use case scenarios in *Table V* based on the key characteristics of the proposed framework.

TABLE V. COMPARISON OF USE CASES FOR GOODNESS-OF-FIT WITH THE PROPOSED MODEL

KEY CHARACTERISTICS	**Use Case 1** Childhood Obesity intervention	**Use Case 2** Humorous Humanoid Joke Telling	**Use Case 3** mHealth Smoking Cessation	**Use Case 4** Movie Recommendations
Involves a Smart Environment Layer	Yes	Yes	Yes	Yes
Utilizes external data sources in the External Environment	Yes	Yes	Yes	Yes
Utilizes a centralized knowledge-based Artificial Intelligence (AI) models	Yes	Yes	No – but utilized a centralized knowledge store	Yes
Persists data in a Cloud environment	Yes	Yes	Yes	Yes
Employs multimodal cognitive features	Yes – emotional intelligence via ERFE and Sentiment	Yes – emotional intelligence via ERFE and Sentiment	Yes – textual inference of SMS response	Yes – emotional intelligence via ERFE
Supports multiple agents or sensor devices in the Smart environment	Yes – Kinect sensor, Fitbit, NAO robot	Yes – Kinect sensor, NAO robot	Yes – Multiple smartphones and tablets	Yes – Kinect sensor, iPad tablet
Involves verbal and non-verbal cues in human-machine interactions	Both	Both	Yes – SMS only	Both
Involves content personalization	Yes – personalized motivational dialogue	Yes – personalized jokes	Yes – personalized SMS messages	Yes – personalized movie suggestions
Involves solving a human-centered problem	Yes	Yes	Yes	Yes
Critical cross-cutting concerns	- Privacy - Performance	- Privacy - Near real-time Performance	- Privacy - High-Availability	- Privacy - Security - Performance

I. Summary

Based on the aforementioned characteristics of the ZOEI framework, I evaluated 4 human-centered CI use case studies through various experiments as described in the ensuing paragraphs to confirm the efficacy of the proposed reference architecture.

V. THE MULTIMODAL COGNITIVE ENGINE

A. Overview

As mentioned in Chapter 3, the first aim of this research study is focused on investigating the design of multimodal cognitive intelligence in HMI scenarios. As illustrated in the proposed reference architecture (in Figure 1), a human-centered CI solution often has a need to recognize and express cognitive features within the smart environment to support socially expressive human-machine interaction. Emerging commercial applications like Sony's Aibo robotic dog [96] and Cynthia Brezeal's Jibo device [97] are among several devices that seek to have an ability to interact with human subjects in very engaging and entertaining ways [96]. Brezeal [96] posits that the innate social-emotional intelligence in the overpoweringly social human species makes it possible for humans to understand and interact with other complex beings in our world.

I classify a constellation of software agents and/or *sociable robots* [96] that are capable of working together to observe, understand, and cooperate with humans to solve complex problems as human-centered CI solutions. I argue that a multimodal approach is often more likely in a collective intelligence scenario where multiple devices in the smart space might play different roles by drawing on their strengths to collectively solve complex problems. Of all the potential cognitive features that can influence a machine's effective interaction with humans in a smart space, I will focus on evaluating the design of *social-emotional intelligence* in agents that can support the human-centered CI class of problems.

B. Challenges

For the implementation of emotional intelligence as a cognitive feature in a smart interaction space, the research challenges investigated include:

- *Challenge 1*: near real-time *sentiment detection* in speech as a verbal signal of emotion and,
- *Challenge 2*:*facial expression analysis* as the non-verbal cue signal to support multimodal affect recognition.

C.Experiment 1: Sentiment Detection in Speech

1) Research Questions or Hypothesis

The application scenarios evaluated in a bid to investigate the listed challenges pertaining to this facet of the reference architecture include the the *speed* of training predictive models with large datasets and the level of *accuracy* of the predicted scores. In other words, what are the best practices for evaluating best-fit-models for various scenarios.

2) Methodology

For evaluating sentiment analysis, I utilized the Sentiment140 [55] dataset to train a predictive model and expose the trained model as an interactive web service hosted in the Microsoft Azure cloud. In implementing a facial expression analysis engine, I also built a predictive model hosted in the Azure cloud as a web service end point. In the training dataset, *positive* labels have a score of 4, while a score of 2 represents *neutral* and 0 represents *negative* polarity. Figure 7 and 8 illustrate the machine learning processes employed to build the respective predictive models for sentiment and facial expression analysis in the cloud-hosted solution. The NAO T12 humanoid robot and the Kinect for Windows v2 sensor device (shown in Figure 23) were used together and interchangeably to translate speech to text prior to calling the interactive web service to discern the polarity of human verbal feedback.

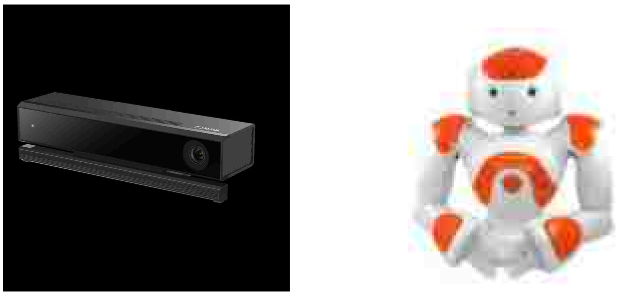


Fig. 23. Kinect for Windows v2 sensor (on the left) and the NAO T12 Robot (on the right)

3) Algorithms

As described in Chapter 3, several algorithms including Bayes Point Machine [90], SVM [91], and Neural Networks (NN) [92] were evaluated to select the best supervised machine learning model for sentiment analysis. In investigating facial expression analysis, the NN and SVM algorithms were investigated.

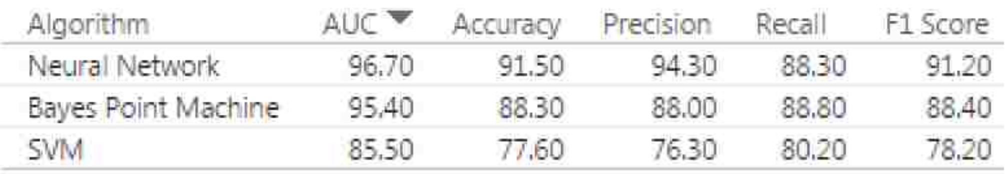
4) Limitations

While pitch, tone, body posture, and others are all very useful features in detecting emotion in speech, this particular study focuses on investigating only sentiments and facial expressions as sample multimodal affect signals.

5) Results

For *Challenge 1*, the built-in Automatic Speech Recognition (ASR) features of the NAO T12 humanoid robot was employed to detect text from speech in the smart environment. To determine the best model for supporting this feature, I evaluated the listed algorithms to determine their accuracy in predicting sentiment polarity in speech. As illustrated in Table VI and Figure 24, I found the two-class neural network implementation to yield the best results across several key metrics for evaluating machine learning classification problems including: *Precision, Accuracy, Recall, F1 Score,* and *Area under the Curve (AUC).*

TABLE VI. SENTIMENT ANALYSIS – TRAINING RESULTS FOR PREDICTIVE MODELS



Algorithm	AUC ▼	Accuracy	Precision	Recall	F1 Score
Neural Network	96.70	91.50	94.30	88.30	91.20
Bayes Point Machine	95.40	88.30	88.00	88.80	88.40
SVM	85.50	77.60	76.30	80.20	78.20

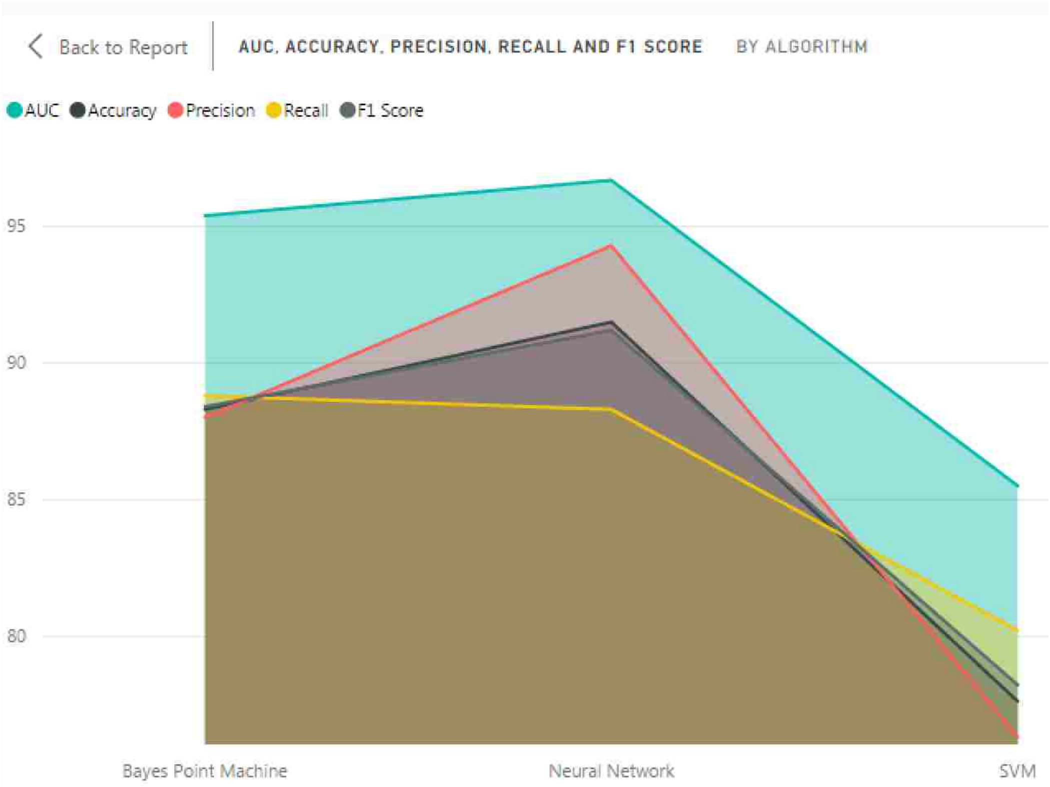
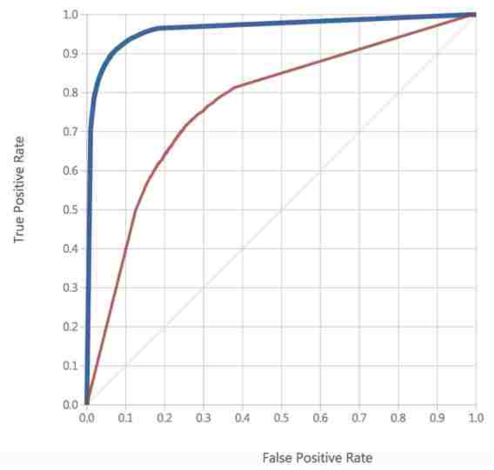


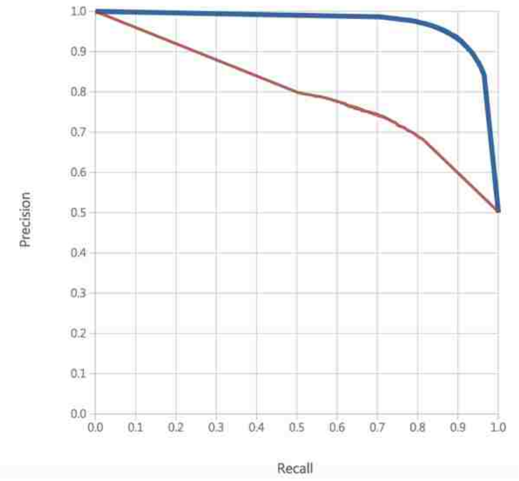
Fig. 24. Visualization of Sentiment Analysis Algorithm Performance

The representative *Receiver Operating Characteristic* (ROC) and *Precision-Recall* curves along with additional supervised learning metrics [92] for the evaluated algorithms (i.e. NN, SVM and BPM) are represented in Figure 25 below.

ROC Curve	Precision / Recall Curve

NEURAL NETWORKS (NN)

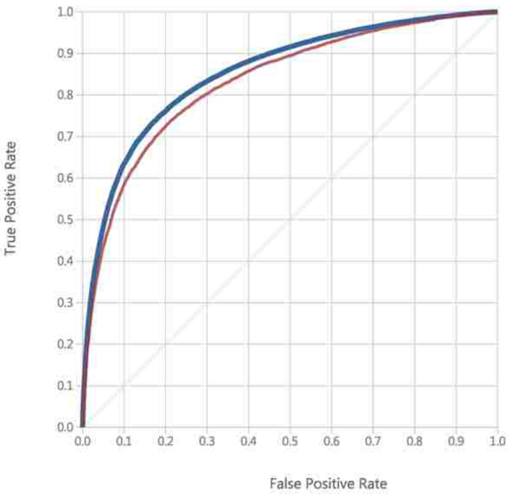


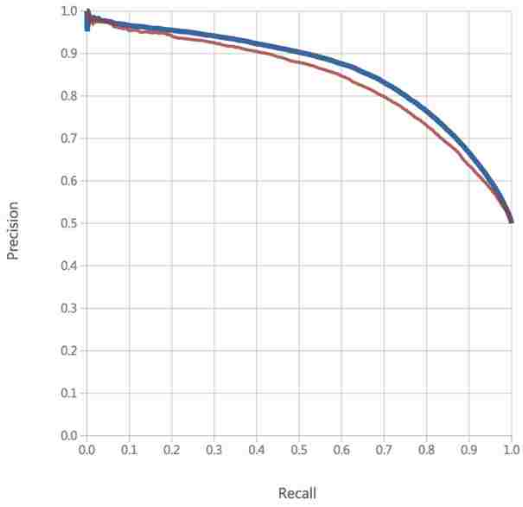


True Positive	False Negative	Accuracy	Precision	Threshold	AUC
57098	6902	0.916	0.936	0.5	0.967
False Positive	True Negative	Recall	F1 Score		
3905	60095	0.892	0.914		
Positive Label	Negative Label				
4	0				

Model Training Time: 13.33 minutes

SUPPORT VECTOR MACHINE (SVM)

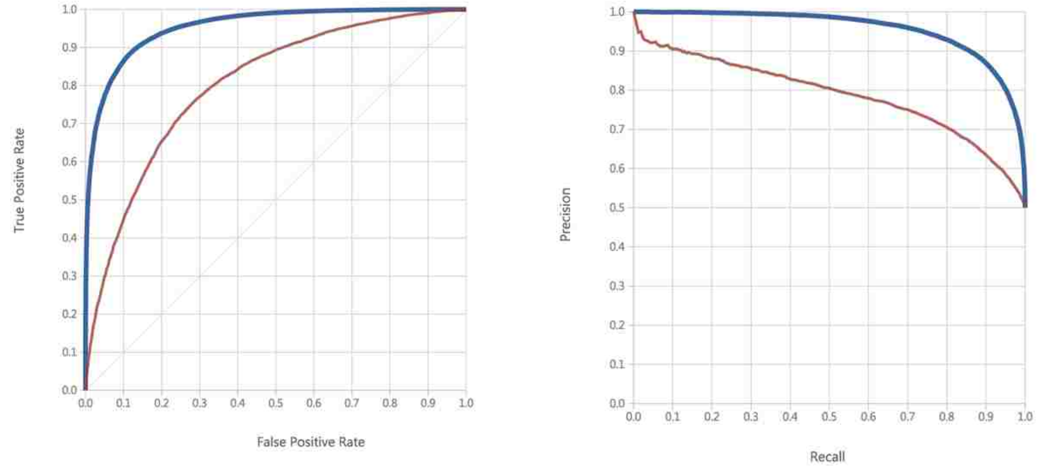




True Positive	False Negative	Accuracy	Precision	Threshold	AUC
51339	12661	0.776	0.763	0.5	0.855
False Positive	True Negative	Recall	F1 Score		
15980	48020	0.802	0.782		
Positive Label	Negative Label				
4	0				

Model Training Time: 7.19 minutes

BAYES POINT MACHINE (BPM)



True Positive	False Negative	Accuracy	Precision	Threshold	AUC
56839	7161	0.883	0.880	0.5	0.954
False Positive	True Negative	Recall	F1 Score		
7775	56225	0.888	0.884		
Positive Label	Negative Label				
4	0				

Model Training Time: 7.96 minutes

LEGEND**:**

🟦 Scored dataset

🟥 Scored dataset to compare

Fig. 25. Visualization of Predictive Sentiment Classification Model Evaluation

6) Discussion

While the binary classifier built using the *neural network* took longer to train (i.e. almost two times as long as the SVM and BPM models), it presented the best model from a precision, accuracy and recall perspective. It offered the fewest false positives and false negatives. If True Positives are represented by *Tp*, False Positives denoted by *Fp*, True Negatives denoted by *Tn*, and False Negatives denoted by *Fn*, then the Precision and Recall performance metrics represent the following formulas:

$$Precision = \frac{T_p}{(T_p + F_p)}$$

$$Recall = \frac{T_p}{(T_p + F_n)}$$

In comparing the three predictive classification models, a trained model with the highest Area Under the Curve (AUC) is regarded as the better model irrespective of the *threshold* configuration (of 0.5 in this experiment). The best model (i.e. Neural Network) had a 96.7% AUC score. Upon selecting the best trained model, the predictive model is published as an interactive model which is then consumed by the Kinect and NAO devices to support speech-recognition based sentiment analysis use cases.

D. Experiment 2: Emotion Detection through Facial Expression Analysis

In the application scenarios for joke telling and childhood obesity intervention, a Kinect for Windows v2 sensor device was used to acquire full frontal facial expression image data to be analyzed in a cloud hosted trained model for real-time emotion detection. To investigate the use of a centralized service for Emotion Recognition through Facial Expression (ERFE) analysis, I developed a representative Android Mobile App for capturing facial images and subsequently processing them using the cloud-hosted emotion detection service under investigation. In addition, the cameras on the NAO robot were also used to acquire images that were then sent to the central service for processing. The investigation sought to confirm the approach of performing real-time facial expression analysis remotely (in support of a collective intelligence approach) compared to the approach that previous studies have taken to building facial expression analysis features on a single local device [27]. With this approach, multiple devices with access to cameras can collectively utilize a central processing service to improve the performance of the emotion detection task.

1) Research Questions or Hypothesis

This experiment sought to explore the best practices for acquiring real-time image streams from a sophisticated camera like the Kinect for Windows sensor v2 device in a bid to send the captured images to a centralized emotion classification API hosted in the cloud. Assuming multiple camera sources are used in a given smart environment, additional images from other cameras (i.e. from a smartphone and a NAO robot) are captured are evaluated for emotion recognition.

2) Methodology

Using Visual Studio as an Integrated Development Environment (IDE) and the C# programming language, I developed a Windows Presentation Foundation (WPF) application for capturing images from the Kinect for Windows v2 sensor. The application polls the sensor periodically in real-time, captures image frames from the sensor's image stream and converts the array of image bytes to a grayscale bitmap. The bitmap image is then saved as a JPEG file and submitted to the trained emotion service API hosted in the cloud. The API detects faces within the image and subsequently evaluates the expressions in the face to classify the emotional state (i.e. happiness) detected with a numerical score. As demonstrated in Figure 9, the emotional states under investigation include: *Anger, Contempt, Disgust, Fear, Happiness, Neutral, Sadness,* and *Surprise*.

In the facial expression analysis problem, there are three key problem areas including:

i. *Face detection* in the captured image

ii. *Detect facial feature points*

iii. *Emotion classification* for the identified face

The AT&T face database [98] was used to train the model. The database features 40 human subjects each with 10 different images. The images were captured under different conditions of light, time of day and facial expressions and details (i.e. smiling, not smiling, open eyes, closed eyes, etc.). As shown in the sample training data in Figure 26, the pictures were taken with a dark homogenous background from an upright frontal position with some tolerance for side movement [98]. The emotion service seeks to identify faces in the input image, detect face points like nose tip, mouth curvature, eye locality, etc. and classify the human's emotion based on previous classifications for other images already in the face database.

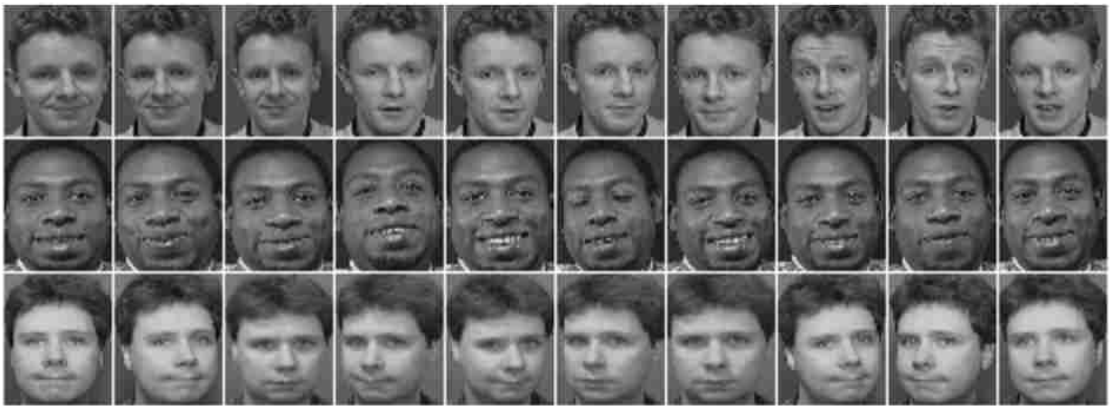


Fig. 26. Sample training data for facial expression analysis

The Microsoft Azure cloud was used to train a model and host the centralized web service for face detection and emotion classification. Several components of the machine learning service were implemented using both the R and Python programming languages.

3) Algorithms

The Haar Cascade [99, 100] face detection algorithm exposed through the OpenCV frontal face detection library (also known as the Viola-Jones method) is used to implement face detection. The Haar Cascade algorithm makes use of four main stages [99] for face detection including: *Haar Feature Selection*, *Creating and Integral Image*, *Adaboost Model Training*, and *Cascading Classifiers*. The *Adaboost* machine learning algorithm is employed to select the best possible features in the image and train the classifiers. To implement the cascade classification approach, the final or "*strong*" classifier $h(x)$ is created as a linear combination of several weighted simple "*weak*" classifiers $h_j(x)$ [100].

$$h(x) = sign\left(\sum_{j=1}^{M} \propto_j h_j(x)\right)$$

Each of the $h_j(x)$ classifiers then has a threshold function based on the feature f_j.

$$h_j(x) = f(x) = \begin{cases} -s_j, & if\ f_j < \theta_j \\ s_j, & otherwise \end{cases}$$

During the model training stage, the following values are determined – *threshold value*: θ_j, *polarity*: $s_j \in \pm 1$, and *coefficients*: $\propto_j$.

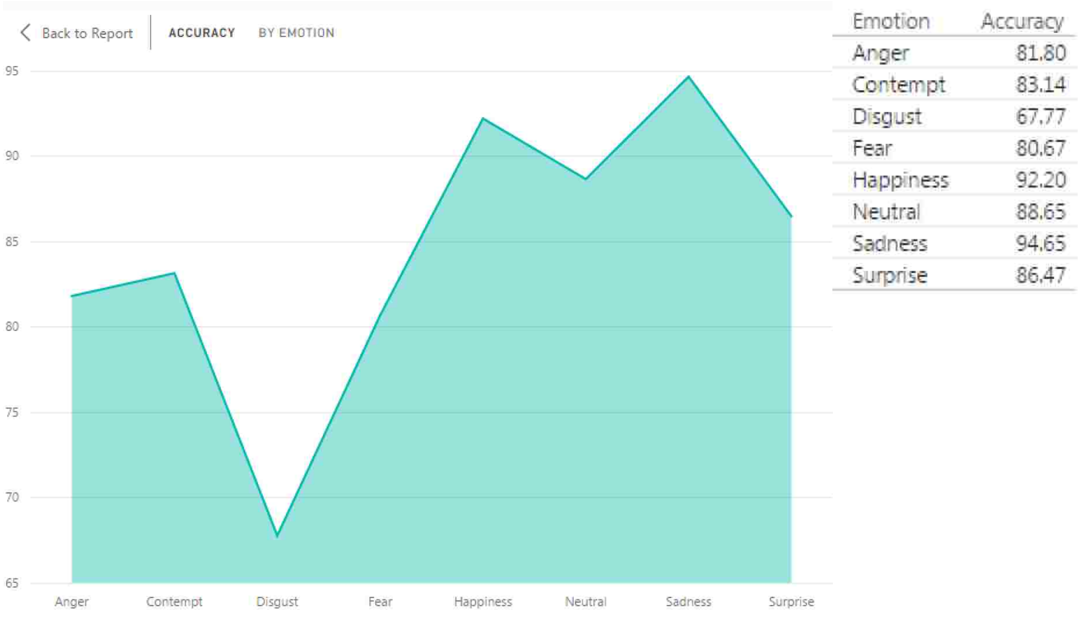
Specific landmarks (i.e. <x, y> vectors) on the face were tracked to support the facial feature point extraction problem. However, the subsequent emotion detection problem utilized a multi-class SVM [91] classifier (LIBSVM) as a supervised machine learning algorithm.

4) Limitations

The accuracy of the facial detection system was sensitive to light conditions captured in the image under investigation. In this case, light creates variance. The best results are achieved with frontal face images. While I did not test the system with a full video file, successive images were captured and analyzed for the overall emotion expressed within a given time interval.

5) Results

As depicted in Figure 9 and Figure 27, the multi-class SVM classifier did very well in predicting the *happiness (92.20%), sadness (94.65%)* and *neutral (88.65%)* states with training. Figure 27 depicts the accuracy of the trained model across all the 8 emotional states under investigation. The facial detection process performed at approximately 96.56% accuracy in detecting full frontal faces in the captured images across multiple camera options. The results can be improved by using deep learning techniques as well.

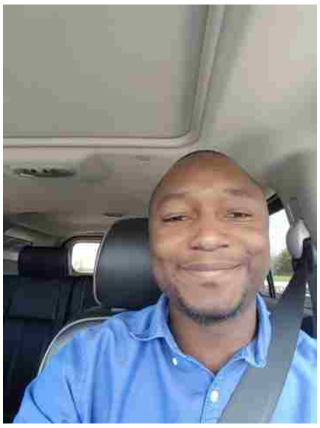


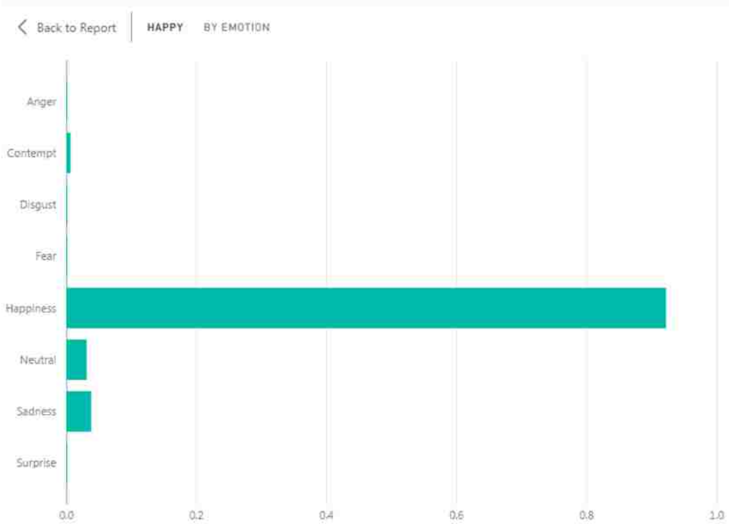
Emotion	Accuracy
Anger	81.80
Contempt	83.14
Disgust	67.77
Fear	80.67
Happiness	92.20
Neutral	88.65
Sadness	94.65
Surprise	86.47

Fig. 27. Overall ERFE Analysis Results

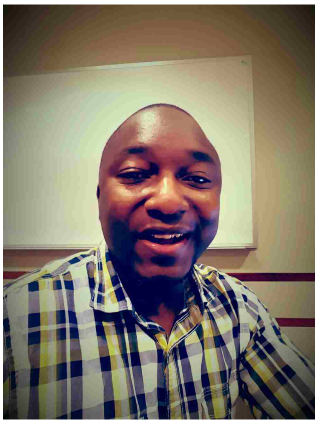
In a bid to support multiple devices communicating with the trained predictive model hosted in the Azure cloud simultaneously, I tracked the response time from when a given message is sent to the service endpoint to the point at which a valid response is received from the service. The average response time recorded was less than 650 milliseconds for a set of 50 images sent to the ERFE service for emotion classification.

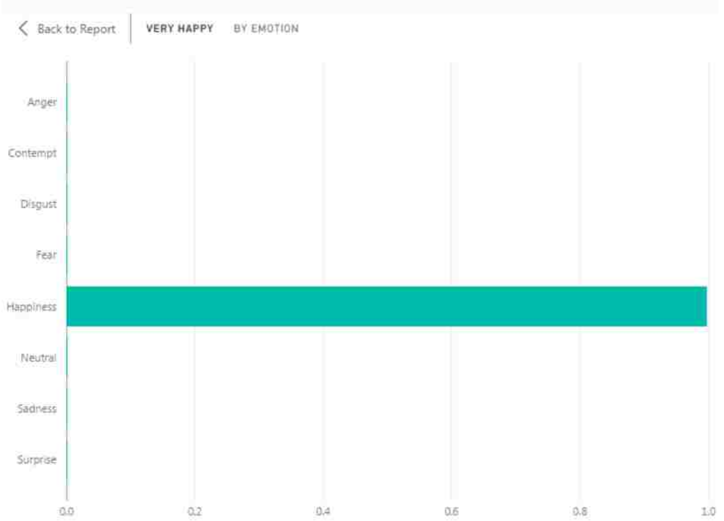
Predicted Emotional State: Happy (Smile) ~ Funny | Predicted Happiness Score: 92.21%



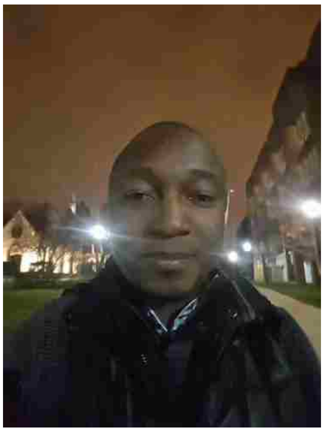


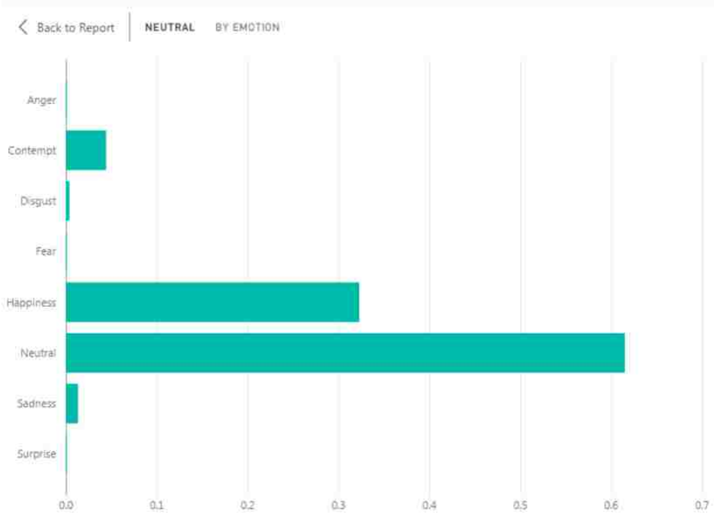
Predicted Emotional State: Happy (Laugh) ~ Very Funny | Predicted Happiness Score: 99.78%





Predicted Emotional State: Neutral ~ Indifferent | Predicted Neutral Score: 61.51%





Predicted Emotional State: Sad (or Displeased) ~ Not Funny | Predicted Sadness Score: 73.02%

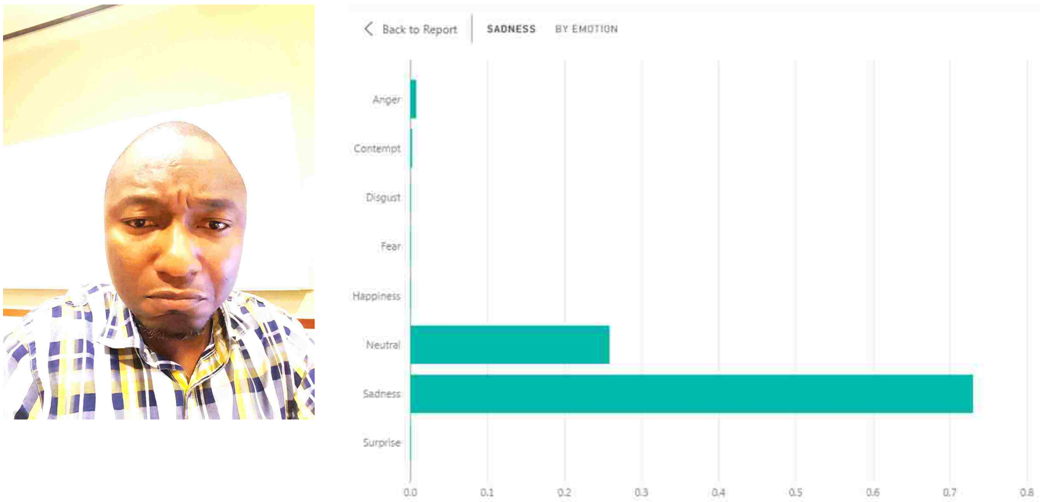


Fig. 28. Sample ERFE Analysis Results – Joke Telling Use Case

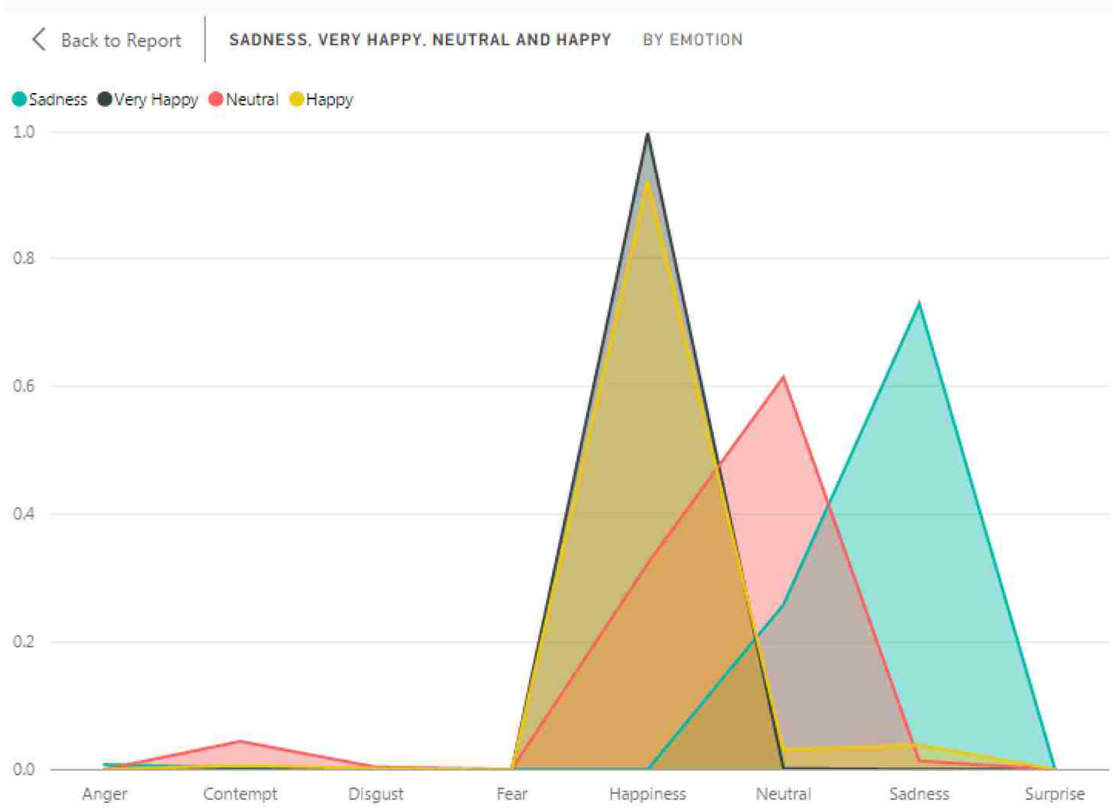


Fig. 29. Visualization of the Sample Emotion Prediction Scores for each of the 8 Emotions (i.e. Anger, Contempt, Disgust, Fear, Happiness, Neutral, Sadness, and Surprise) with respect to the 4 Emotional States shown in Figure 28 (Very Happy, Happy, Neutral/Indifferent, and Sadness/Not Funny)

6) Discussion

For the approach implemented in this experiment, the emotion detection service can be grossly improved by acquiring even more training images of additional subjects. Additional facial landmark features can also be defined and analyzed to improve the emotion recognition service. I expect the model to improve with time as the system acquires more training image data to aid further model retraining efforts.

Remarkably, Picard [62] posits that the four most common basic emotions are: *Fear, Anger, Sadness*, and *Joy (or happiness).* In the joke telling application scenario, the accuracy of the happiness, neutral and sadness emotional state prediction was very useful in detecting the level of "happiness" demonstrated by a human subject when a funny joke was uttered. The relatively poor performance exhibited in detecting other emotional states (e.g. angry, etc.) was not a key concern for this specific scenario. In the experiment, I tracked the individual emotion prediction scores and further categorized jokes as "*very funny*", "*funny*", "*indifferent*" and "*not funny*" based on the recorded aggregate emotional recognition scores as indicated in Figure 28 and 29. In this scenario, the robot utilized a collaborative filtering approach through the *feedback loop* to confirm if the human was interested in hearing additional jokes.

E. Summary

Based on the success of the cloud-hosted machine learning models implemented for real-time Sentiment Detection and ERFE and in experiment 1 and 2 respectively, there is promise for employing several cognitive services for real-time human-machine interaction scenarios where multiple devices and sensors play different roles in the smart environment. In the use cases that I explored for both experiments, the NAO robot and the Kinect for Windows sensor collaboratively interacted with a cloud-hosted backend integration service that exposed knowledge and intelligence as a service while achieving near-real-time response performance with minimal impact to prediction accuracy.

VI. THE CONTENT PERSONALIZATION ENGINE

A. Overview

Collective Intelligence (CI) can be defined as the ability of a series of agents to collaboratively solve significant and complex problems that would be otherwise challenging to solve by a single agent [10]. To support collective intelligence, the ability of the CI system to draw from the accumulated knowledge in recommending relevant and personalized content to the interacting users remains critical [1, 10, 11, 38].

Building knowledge-based artificial intelligence (AI) often involves the intimate connection between *Reasoning*, *Learning*, and *Memory* [101]. These three AI processes contribute to the overarching architecture of AI agents. In collective intelligence scenarios, we would expect machines to be able to leverage both short-term and long-term memory. I argue that a centralized knowledge base hosted in the cloud is an effective approach to building a collective intelligence solution that is capable of drawing from *learnings* across multiple agents by referencing its *memory*. In the same vein, the CI devices or agents are able to think or select options based on the centralized knowledge store. The feedback loop between the *cognitive* and the *personalization* aspects of the ZOEI reference architecture serves to support the sharing of learnings (from the sensing devices in the Smart Environment) to enhance the reasoning of the personalization engine. Conversely, the reasoning or personalization aspect of the model can equally support the learning process.

In normal human to human dialogue, knowing the right things to say to someone in an effort to influence their perception is often encouraged, particularly, when it comes to showing that one cares or loves someone. One of the core tenets of an artificial intelligent (AI) agent or care robot in an elderly care scenario (for example, *Scenario 2* in this literature) is predicated on the idea that the robot exudes the feeling of compassion in a way that reassures the elderly person that the robot genuinely cares about the participant [38]. As we dissect the human signals that go into demonstrating care among humans, some of the recurring themes that often bubble up include trust and compassion.

Compassion in a care robot might necessitate the expression of sympathy in the humanoid when the human companion is in a sad emotional state or mood. Beyond the expressive display of sympathy, the care robot might be able to influence the human's emotional state by trying to cheer up the human while maximizing its contextual awareness of the human's current emotional state. For example, if the human is in an excited state, the robot might need to imitate that emotional state by showing expressive behaviors that are synonymous with excitement.

The use of unsupervised machine learning algorithms, reinforcement learning, and recommender system solutions are proposed for identifying profile similarities and clustering the demographic data that appear to be consistent with the cognitive signals observed for similar content. In scenario3, I implemented a *custom recommendation model* for personalized SMS messages in a persuasive mHealth-based smoking cessation intervention (i.e. illustrated in *Use Case 3*) based on the user's personal preferences and the stage in which the user is in the intervention process (with input data gleaned from periodic in-person surveys). However, in most cases, AI-based recommendation systems may be implemented through machine learning techniques [102]. The rationale for investigating reinforcement learning techniques for content personalization is predicated on the ability for reinforcement learning to allow agents to learn from delayed rewards over a period of time. Compared to supervised and unsupervised learning approaches, the feedback in reinforcement learning might take a while to for AI agents to understand as it mimics human learning patterns with trial and errors and occasional feedback on whether or not a previous choice was good or bad [102].

B. Challenges

To support the implementation of content personalization through knowledge-based AI in the overarching ZOEI framework I designed a couple of experiments to help investigate the following research challenges:

- *Challenge 1*: the implementation of a *reinforcement learning model for a humorous conversational robot* in supporting elderly care scenarios (i.e. illustrated in *Use Case 2*). The previously learned affective reactions of the human (in the *Smart Environment*) and jokes mined from online sources (in the *External Environment*) are used to influence the content personalization.
- *Challenge 2*: the implementation of a *recommender system for movie suggestions* based on a user's previous *social media profile* information (from the *external environment*) as well as the *sensed ERFE data* collected by observing a user's reaction similar movie trailers in the *smart environment* as a human-centered CI scenario (i.e. illustrated in *Use Case 4*).

C.Experiment 1: Applying Reinforcement Learning in a Humorous Robot

Drawing from *Use Case 2,* described earlier in the preceding sections, I experimented with applying reinforcement learning techniques [105] to personalizing jokes in a humorous humanoid robot by drawing from input signals from both the smart environment and the external environment while hosting the knowledge-based artificial intelligence store in a cloud environment [38]. The goal for applying the reinforcement learning technique in this scenario is centered on providing the humanoid comedian with the ability to tell even funnier and personalized jokes over a period of time while it learns from the affective reaction of human subjects to the content (jokes). I expect that beyond this scenario, several applications can benefit from applying this technique to content personalization.

1) Research Questions or Hypothesis

This experiment focused on investigating how to build personalized content based on the previously sensed affective state of the human as well as pre-classified content mined from various online sources through screen scraping techniques.

2) Methodology

In this case study, the humanoid robot interacts with the knowledge-based AI systems through a web service hosted in the Microsoft Azure Cloud environment to retrieve pre-classified funny jokes to be uttered and acted out in the smart environment. Each joke has a non-verbal classification that allows the humanoid to deliver the joke with expressive gestures (as shown in Figure 30) in an effort to exhibit believable behaviors. At the end of each joke, the humanoid robot prompts the human to confirm how funny the joke was and also indicates if he or she is interested in hearing additional jokes or funny tales [38].

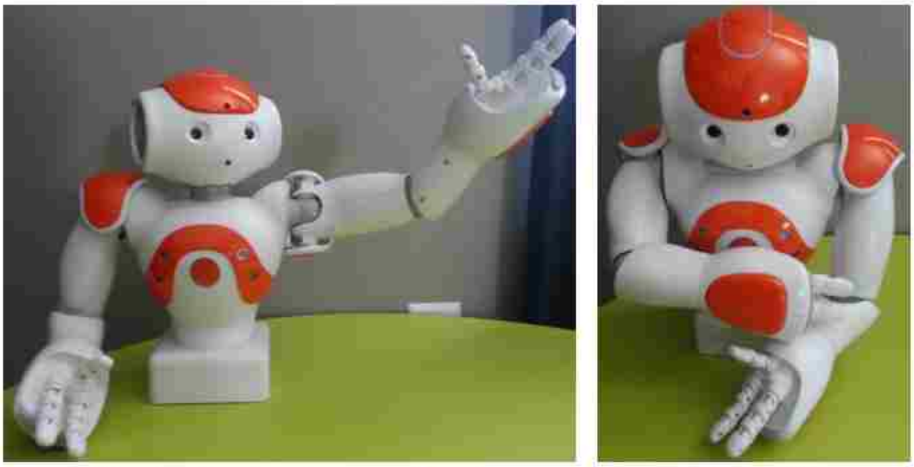


Fig. 30. Using hand gestures in humorous robot joke telling session to express affect

The dialogue system makes use of Automatic Speech Recognition (ASR), as well as face and emotion recognition features. In addition, the Text-To-Speech (TTS) capabilities of the NAO robot are used in combination with generated gesture interactions to convey human-like behaviors through a combination of verbal and non-verbal communications techniques. A web-based survey is used to collect additional affective state data during the HRI session by a human observer. Prior to the interaction session, anonymized participant demographic information is collected to help guide the content targeting features for selecting targeted jokes.

In my implementation of reinforcement learning for driving action (joke) selection, I employed the "∈-greedy" policy [102] which seeks to always pick a joke that has previously been confirmed as having the highest value of reward ("very funny") while considering the profile segment that the current user belongs to. Using some small probability ∈, the humanoid robot will pick a random joke occasionally to explore alternative jokes that may or may not previously tested for the current user's profile segment.

3) Algorithms

The Markov Decision Process (MDP) is at the heart of many reinforcement learning algorithms [103, 104]. MDP can be defined by a 4-tuple (*S, A, T, R*), where:

- *S* is the *state space* with states $s \in S$,
- *A* is the action space with actions $a \in A$ and $A(s)$ denotes actions spaces that depend on the current state of *s*
- *T (s, a, s')* is the unknown stochastic *transition dynamics* that indicates the probability of arriving in state s' from state *s* when action $a \in A(s)$ is taken.
- *R (s, a)* denotes an *average reward function* which represents the projected one-step payoff when an action *a* is taken in a state denoted by *s* [103].

A typical reinforcement algorithm seeks to unearth an optimal policy denoted by $\pi^*(s)$ that maps states to actions in a bid to maximize the *discounted long term reward* [104]. For this experiment, the reward is represented as $Q_{s,t}(a)$, where:

- s is the state – profile attributes of the current user,
- a is the action – joke,
- t is the number of times that the joke has been presented to another user with a matching profile segment as the current user,
- T represents the dynamics given by the partially stochastic state machine that derives funny jokes.

The reward in this scenario is affective feedback indicating that a given joke was funny. This feedback signal helps the learning agent to improve over time.

Two of the most popular reinforcement algorithms in use today include Q-Learning and SARSA [103, 104]. SARSA is an on-policy temporal difference learning algorithm for MDP problems – meaning that it estimates the value of the same policy that it is set to use for control [105]. The SARSA (s, a, r, s', a') algorithm makes use of the following update equation:

$$Q(s,a) \leftarrow (1-\alpha)\,Q\,(s,a) + \alpha\,[r + \gamma\,Q(s',a')]$$

where $0 \leq \alpha \leq 1$ is a learning rate parameter and $0 \leq \gamma < 1$ is the *discount rate* for future rewards and *r* is the immediate reward [104]. On the other hand, Q-Learning is an off-policy alternative to SARSA and makes use of the following update equation:

$$Q(s,a) \leftarrow (1-\alpha)\,Q\,(s,a) + \alpha\,[r + \gamma \max_{a' \in A(s')} Q(s',a')\,]$$

Compared to SARSA, the Q-Learning equation substitutes the $\gamma\, Q(s', a')$ term with $\gamma \max_{a' \in A(s')} Q(s', a')$ which allows for disconnecting the policy under evaluation from the policy that is used for control.

In this experiment, the learning agent (NAO robot) sought to map *States* (attributes of the current audience member) to *Actions* (pre-classified jokes in the database) in an effort to maximize a numerical *Reward* (i.e. the perceived funny rating). While I explored the use of both algorithms for reinforcement learning in this experiment, I resorted to using the Q-Learning approach because it converged faster for this scenario.

4) Limitations

The prototyped system affords human-robot interactions (HRI) between the humanoid robot and one human, at a time. Eventually, the solution can be expanded to handle multiple audience members with the deployment of additional sensors in the smart environment. I focused on testing only two reinforcement learning algorithms.

5) Results

To evaluate the HRI system, I employed two approaches including:

- Analysis of the affective HRI dialog for joke telling
- Performance analysis of the reinforcement algorithms

In this case study experiment [38], I invited 14 people with varying demographic backgrounds to interact with Humanoid in a joke telling HRI session. The age classifications and distribution of respondents explored for profile segmentation include: 3 *elderly people*, 9 *middle-aged*, and 2 *young adults*. The jokes in the cloud-hosted database was pre-classified as being either "*funny*" or "*very funny*" jokes. Non-verbal actions were tagged to some of the jokes in the database. The non-verbal actions were interpreted and performed by the humanoid robot during the joke telling session.

As illustrated in Figure 31, my analysis of the initial phase of the experiment described in the case study indicates that most participants (57.1%) found the pre-classified jokes as being "funny" on the average, while 35.7% of the participants found the jokes as being "very funny." 7% of the participants were indifferent to some of the jokes. At the beginning of the study, there were more "indifferent" scores, though as more participants interacted with the humorous robot, the average affective state score improved through the application of the reinforcement algorithm to process the affective feedback as a signal for further ranking the pre-classified jokes. My initial test revealed that applying the ∈-greedy policy [103] along with the Q-Learning algorithm provided more favorable results.

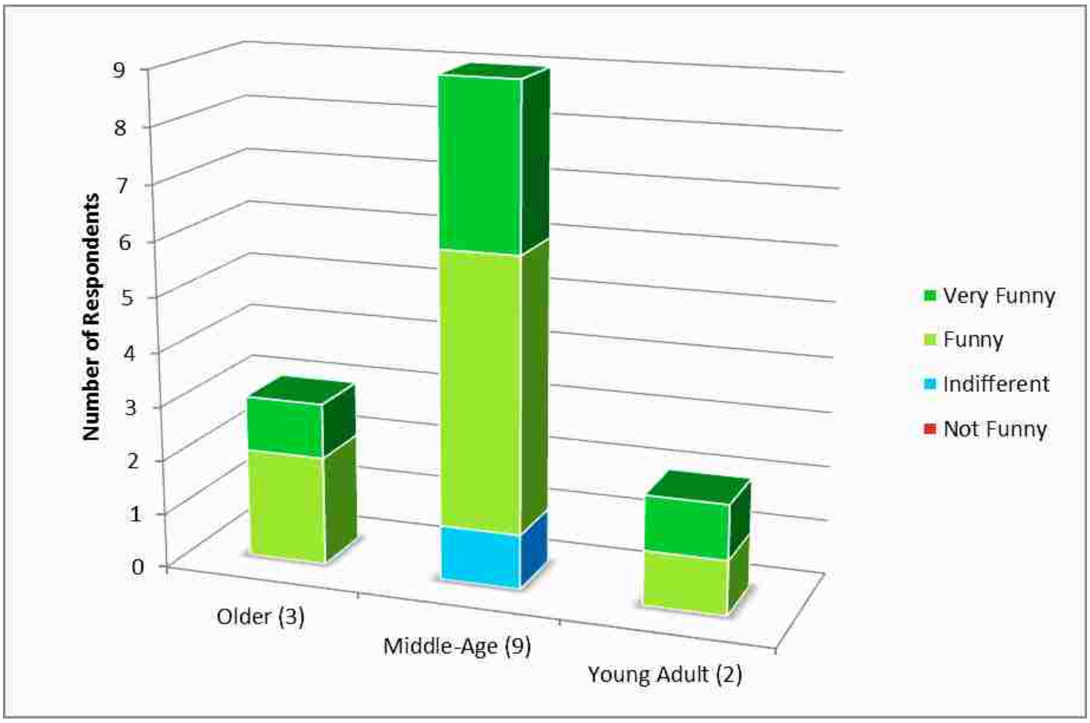


Fig. 31. Average Affective State Score by Respondents and Age Classified Profile Segments

6) Discussion

In this experiment, I implemented an HRI system that was designed to use affective state signals gleaned from the smart environment of a human-centered CI solution. These feedback signals were used to drive reinforcement learning techniques in order to maximize the reward of having the robot perform jokes that the human audience will find very funny [38]. Further work can be done to test the prototype over a longer period of time using people with vast demographic backgrounds and profile segment classes. However, the results of the experiment suggest that the Q-Learning reinforcement learning technique bodes well for a personalized joke telling use case as described in the study.

D. Experiment 2: Applying SMI and Recommender Systems

Using *Use Case 4*, I applied a combination of Social Media Intelligence (SMI) and Recommender systems to investigate the promise of the human-centered collective intelligence in personalizing movie recommendations. The main concept under investigation in this use case, is centered on using characteristics and preferences of humans gathered from both the smart environment and the external environment (OSNs) to make recommendations to other humans. As demonstrated by Amazon's capability for recommending products based on a user's previous purchasing behavior, *collaborative filtering* techniques [109] can be used to facilitate these types of personalization scenarios.

1) Research Questions or Hypothesis

Investigate best practices for applying recommender systems to human-centered collective intelligence scenarios involving external social media data sources as well as cognitive metadata (for example, affective response) from a user gleaned from a smart environment.

2) Methodology

I used the Microsoft Azure cloud for implementing the machine learning technique for the collaborative filtering. The python code that I implemented attempts to find movies rated by the target user and other users with similar demographic characteristic, emotional response, and social media-mined preferences (through the Facebook Graph API). The model learns from a collection of users who have previously rated a number of movies in the dataset. Using matrix factorization, the inferred user preferences and movie attributes are used to predict the rating that a given user who has not previously seen a given movie is likely to select. The recommender model is used to train the predictive engine and score new data.

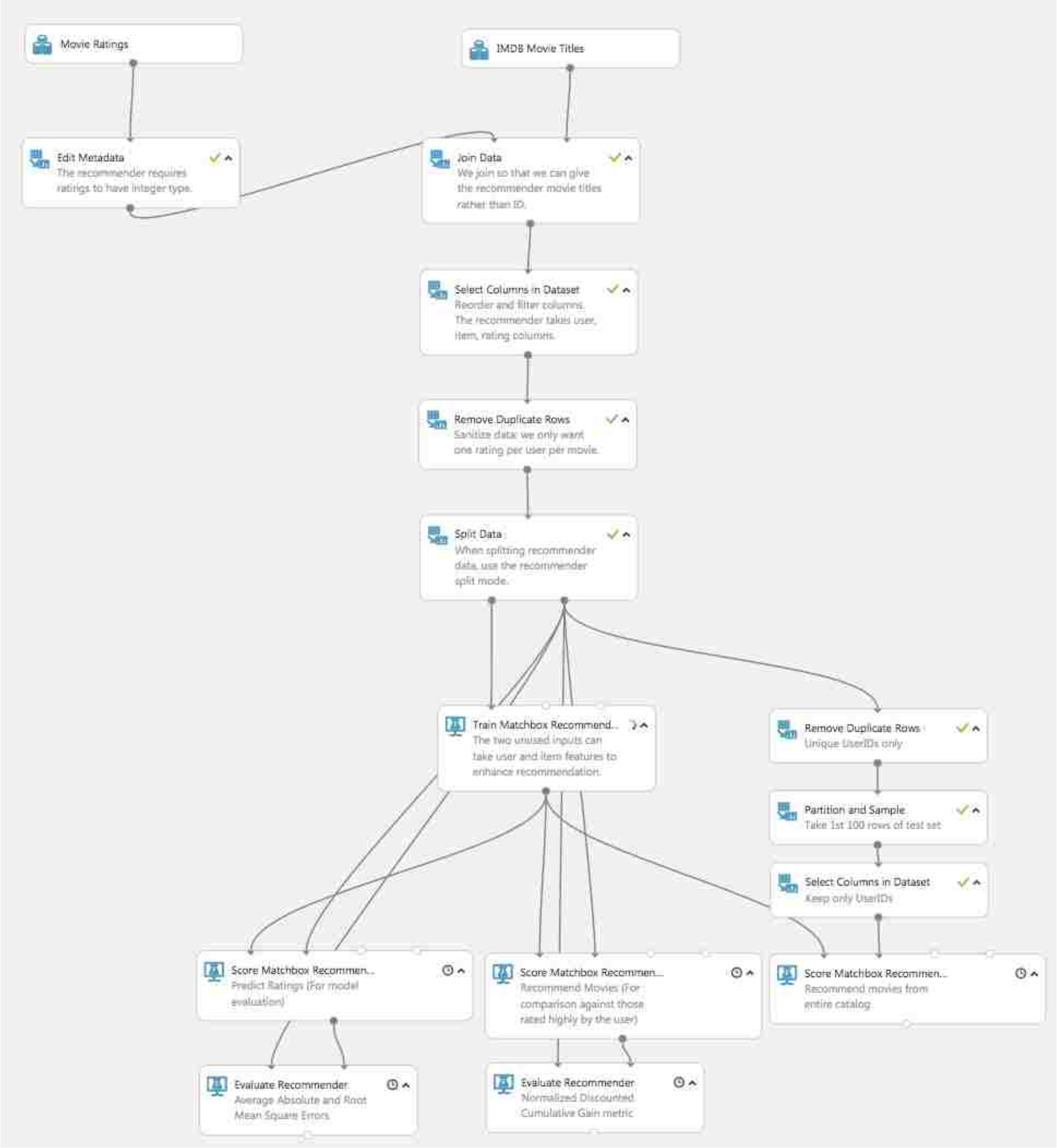
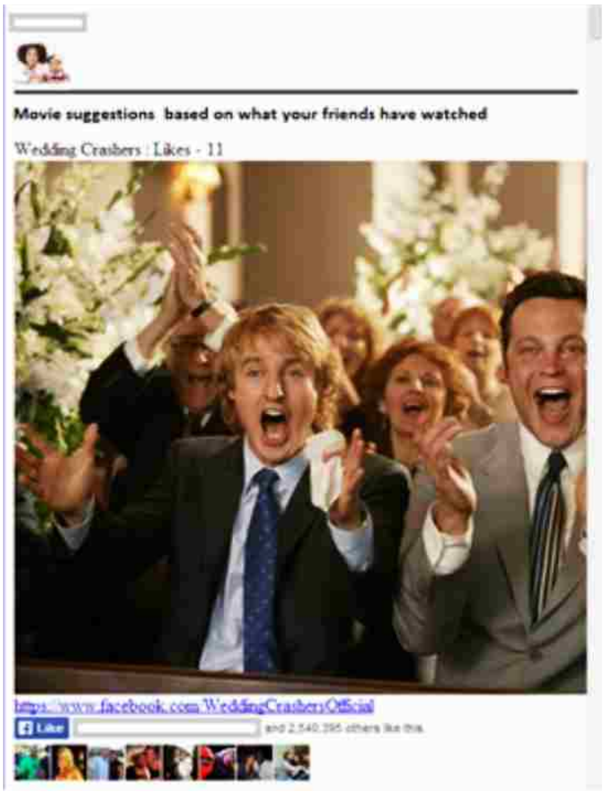

Movie Ratings
IMDB Movie Titles
Edit Metadata
The recommender requires ratirigs to have integer type.
Join Data
We join so that we can give the recommender movie titles rather than ID.
Select Columns in Dataset
Reorder and filter columns. The recommender takes user, item, rating columns.
Remove Duplicate Rows
Sanitize data: we only want one rating per user per movie.
Split Data
When splitting recommender data, use the recommender split mode.
Train Matchbox Recommend...
The two unused inputs can take user and item features to enhance recommendation.
Remove Duplicate Rows
Unique UserIDs only
Partition and Sample
Take 1st 100 rows of test set
Select Columns in Dataset
Keep only UserIDs
Score Matchbox Recommen...
Predict Ratings (For model evaluation)
Score Matchbox Recommen...
Recommend Movies (For comparison against those rated highly by the user)
Score Matchbox Recommen...
Recommend movies from entire catalog
Evaluate Recommender
Average Absolute and Root Mean Square Errors
Evaluate Recommender
Normalized Discounted Cumulative Gain metric

Fig. 32. The machine learning process flow for implementing the recommender system

The training data has 15,742 movies rated by 26,770 users in the movie ratings dataset provided by Dooms et al. [110]. Using a common *movie identifier* (labeled *MovieId*), the associated movie names were mined from the IMDB database [106] and joined to the ratings dataset. Associated movie trailers for 65% of the movies were extracted from YouTube using the YouTube API [108]. User metadata regarding movie genre preferences of the target user along with that of the user's closest Facebook friends were extracted using the Facebook Graph API [107] and utilized to augment the original data.

Affective response scores for various movie trailers played for a new user in question was also used as user metadata.

As depicted in the process flow in Figure 32, duplicate data for each user-movie pair was removed from the original dataset. Using the *holdout* method, 75% of the dataset was used for training the recommender model, while 25% was held out as testing data. To evaluate the model, it was used to predict the top 10 movies previously rated by other users that are likely to be most relevant to the user in question. The recommender model was published as web service in the Microsoft Azure cloud and consumed by the iPad mobile application to display the top 10 recommended movies. A sample screenshot of the iPad App is shown in Figure 33.



Movie suggestions based on what your friends have watched

Wedding Crashers : Likes - 11

https://www.facebook.com/WeddingCrashersOfficial

and 2,540,395 others like this.

Fig. 33. Screenshot of the movie recommendation iPad App

3) Algorithm

Collaborative filtering algorithms [109] typically seek to find similar users in a larger group of users in a bid to build an ordered list of common things that they would enjoy [1]. In typical collaborative filtering implementations, there is often a need to determine how similar users are in their preferences by computing a *similarity score* between user and every other user. Some of the algorithms often employed for calculating similarity scores include *Euclidean Distance* and *Pearson Correlation* [1]. In this experiment, I used the *Pearson Correlation* algorithm. Even though *Pearson Correlation* is more complicated, it tends to produce better results compared to the Euclidean distance algorithm for non-normalized data and, hence, protects against *grade inflation* [1]. The underlying movie recommender algorithm was based on factorizing the user-movie interaction matrix.

4) Limitations

The original training dataset had no affective response metadata except for affective data gleaned for new target users. With additional enriched training data, I expect that the affective response as well as the augmented social media metadata will contribute significantly to the recommended movies for new users.

5) Results

Through various random trial runs (as shown in Figure 34), 5 features and 30 iterations were determined to be the most favorable options for training the model with the goal of attaining the most acceptable performance. To evaluate the accuracy of the predictions, I determined the *Mean Absolute Error* (MAE) – that is the average difference between the actual and predicted ratings – as well as the *Root Mean Square Error* (RMSE) by using the held out (test) data. For the movie rating value scale between 1 and 10, my best MAE and RMSE scores were 1.20 and 1.73 respectively.

In addition, I computed a *Normalized Discounted Cumulative Gain* (NDCG) – a score that falls between 0 and 1 where 1 indicates a perfect ranking [109] that, in turn, represents a perfect match between the top 10 recommended movies produced by the model and a user's actual top 10 rated movies. My best NDCG score for the original dataset was 0.96. These scores are good in practice. It took about 10 minutes for the process to train the recommender model during each trial experiment. Figure 34 illustrates the results of my model tuning exercise. The recorded output was achieved by varying the number of features and iterations with 4 training batches to obtain an optimal performance rating.

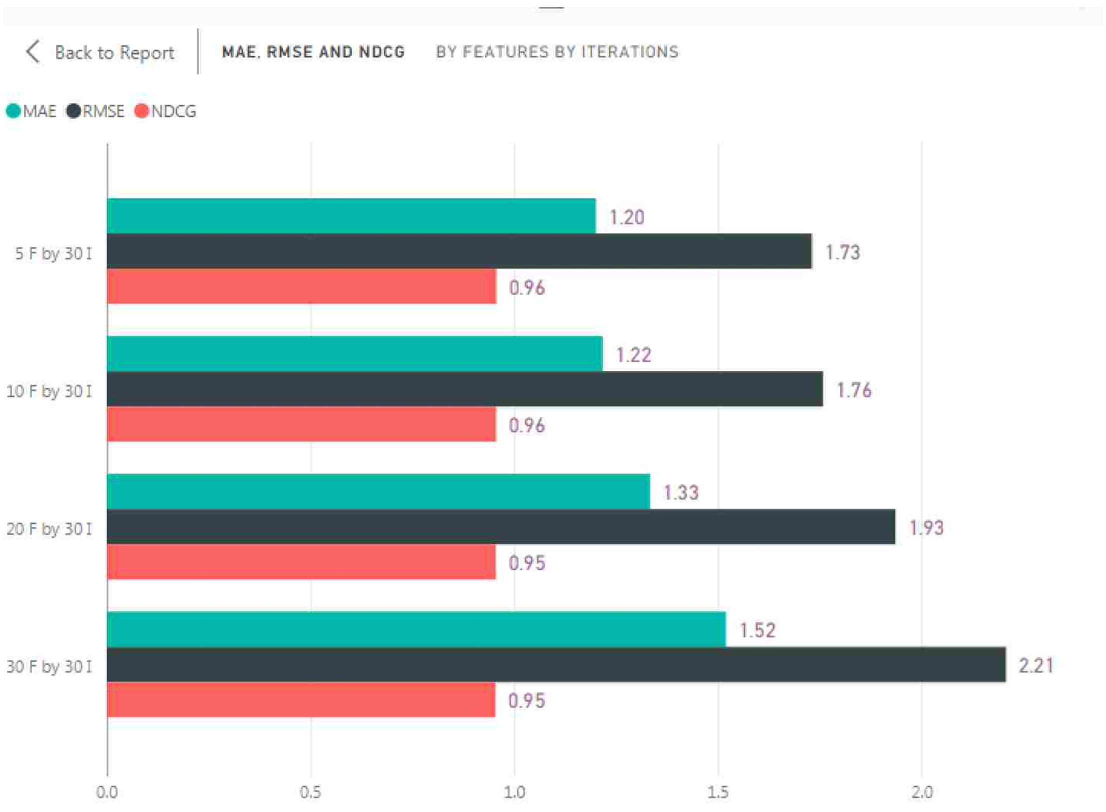


Fig. 34. Model tuning results for the collaborative filtering experiment

6) Discussion

In this experiment, I confirmed the efficacy of implementing recommender system based on collaborative filtering techniques in support of the overarching human-centered CI framework approach. Movie and User metadata was drawn from various sources including an OSN, an online movie database, and affective response sensed in a smart environment. Based on the chosen training data the cloud-hosted model predicts the top 10 movies with a 96% accuracy rate using NDCG as an evaluation metric.

E. Summary

Drawing from the two experiments described in this chapter, I was able to evaluate the human-centered collective intelligence framework proposed in this dissertation. I expect that my findings in investigating both the *collaborative filtering* and *reinforcement learning* scenarios will support future work.

VII. THE PRIVACY ENGINE

A. Overview

As the promise of the Internet of Things (IoT) and collective intelligence (CI) materializes in our everyday lives, we are often challenged with a number of concerns regarding the efficacy of the data privacy solutions that support the pervasive components at play in IoT applications. The privacy and security concerns surrounding IoT often manifests themselves as a treat to end-user adoption and negatively impacts trust among end-users in these solutions [46].

B. Challenges

I evaluated some of the key privacy and confidentiality challenges pertaining to implementing human-centered CI solutions including:

- *Challenge 1*: Using *Use Case 4*, as an illustrative case study, investigate how various facets of security and privacy implementations can be considered in a holistic reference architecture throughout the implementation lifecycle for designing human-centered CI applications and, more specifically, in affect-driven personalization
- *Challenge 2*: Using *Use Case 4* as a case study, I investigate common privacy problems and approaches to affect-driven personalization and, in turn, propose a conceptual reference architecture for this use case
- *Challenge 3*: Investigate key problems and best practices for designing confidentiality and inspiring trust in ubiquitous CI scenarios

C.Experiment 1: Reference Architecture for Privacy in HCCI scenarios

Trends pertaining to the use of the *Internet of Things* (IoT) to collaboratively solve complex problems in healthcare monitoring, online web site advertising, and smart home implementation scenarios, among others, are expected to continue to grow rapidly [46]. Nonetheless, one of the most critical deterrents to mainstream user adoption of IoT and human-centered CI systems is a looming distaste for how data privacy is enforced among the various collaborative systems typically at play in IoT applications. Beyond the privacy and security concerns encircling IoT systems, it is becoming more and more inevitable for pervasive collaborative devices to leverage web services for data sharing and communication to backend storage systems. With the advent of cloud computing, it is not uncommon for the mobile services that these pervasive devices communicate with, to be hosted in the *cloud*. Consequently, with the imminent domain-specific privacy and security concerns for cloud computing, IoT, pervasive systems and web services, it is important to establish a reference architecture that provides a holistic solution for implementing cloud-enabled applications and service interactions in IoT scenarios in a fashion that improves the overarching goal of attaining end-user trust and, in turn, improve user adoption of IoT applications (Apps).

I considered some of the key spheres of significance in arriving at a reference architecture that is aimed at achieving trustworthiness among end-users in IoT applications, as being reminiscent of the implementation of security and privacy in:

- the human-centered CI or IoT application, holistically,
- Ubiquitous computing systems in the solution,
- the participating Cloud computing systems, and
- the Service-Oriented Architecture (SOA) or Integration layer

This study advances my investigation into the application of cloud services and collaborative ubiquitous devices in mobile health (mHealth) intervention scenarios (as described in *Use Case 2*. In most mHealth use case instances, sensitive health-related data is collected and stored in a cloud-hosted solution. The reference architecture presented in this experiment provides a framework for ensuring that privacy and security take center-stage throughout the application development lifecycle in the pursuit of maximizing the promise of IoT, Ubiquitous computing and Cloud computing archetypes.

In addition, I seek to share a blueprint for developing software architecture that supports privacy and security in human-centered CI solution designs. I envision that this template solution for the CI domain can be adopted, refined and extended by software designers, engineers, and architects who seek to preserve trust across CI implementations. By promoting the adoption of this reference architecture, I hope to institute a foundation for ensuring consistency in addressing privacy and security concerns among current and future IoT implementations.

A reference software architecture for a given domain seeks to define the underlying components of the domain and their associated relationships [111]. The software architecture of a given implementation in the domain then becomes an instance of the domain reference architecture. Previous studies [111] suggest that establishing a reference software architecture promotes re-use, reduces maintenance costs, and serves as a benchmark for software governance. I expect this reference architecture to serve human-centered collective intelligence researchers and practitioners in the same capacity.

1) Research Questions or Hypothesis

Derive a generalized reference architecture for improving security and privacy concerns in human-centered collective intelligence systems. Describe the various layers and characteristics of the model and share some of the best practices employed.

2) Methodology

In most cases, end-users are likely to accept an IoT solution that is managed or hosted on a trusted cloud provider system [46]. I propose the use of a governance body for ongoing certification and regulation of standards pertaining to the all-encompassing extent of a typical IoT implementation. The proposed reference architecture is shown in Figure 12.

To test the hypothesis that our reference architecture is feasible for most modern IoT implementations, I reviewed the implementation of security and privacy solutions aimed at achieving trust in the *four use cases* described in this dissertation and compared the inherent layers in each scenario to that of my proposed conceptual reference architecture.

In addition, I developed a prototype of the case study described in this study and shared the way in which various security and privacy concerns are addressed in the work-in-progress solution with a few IT practitioner end-users. I collected feedback from these end-users through a survey to gauge their comfort level with the implementation of security and privacy solutions at various layers of the conceptual model.

3) Key Concerns and the Proposed Reference Architecture

The ensuing literature describes some of the key concerns inherent in each layer of the proposed reference architecture (shown in Figure 12).

a) Security and Privacy in the Ubiquitous Devices in the Smart Environment

In considering the security and privacy concerns of human-centered CI applications, it is important to hone in on some of the security and privacy challenges pertaining to pervasive devices and sensors that are often working ubiquitously to collect and exchange data in the environment. From a security and privacy perspective, some of the key requirements that can be addressed at this layer of the application include [112]:

- *User identification and validation* to control access while enforcing permissions and authorization levels for various components of the system
- *Tamper resistance* of the physical and logical device. Since IoT devices are typically unattended, physical attack vulnerabilities are critical.

- *Content security* - through digital rights management (DRM) of content used in the system
- *Data privacy* to protect sensitive user data.
- *Data communications and storage security* through protective measures for both data in-transit and data at-rest
- *Secure network communications* to ensure that network communications between ubiquitous devices and external services are only authorized through secure connection channels (for example, the wireless communication in the smart home environment of our case study can only be transmitted through the user's designated "home" wireless router, by default. Eavesdropping vulnerabilities in the wireless network must be curbed.
- *Privacy in ubiquitous computing* comes to play because the way in which the device or sensor collects data about the end-users might conflict with the user's privacy preferences for a particular scenario. For example, while a user might be open to having the Kinect sensor perform user identification to support the IoT system, he or she might not be open to having the Kinect record certain conversations in the smart home. These privacy barriers and preferences must be preserved in order to instill end-user trust in the system.

That notwithstanding, some of the key security features that can be incorporated in pervasive device architecture (that is considering both hardware and software requirements) include [112]:

- Lightweight cryptography approaches to support the low power, memory and processing power constraints in most pervasive sensors and actuators
- Security measures to protect the physical device

- An interface for determining and controlling the privacy preferences of the end-user. This might include a visual cue (for example, a green light) when the device is in recording mode. The ability to stop or pause the recording mode easily becomes critical as well
- Standard security protocols for direct device-to-device communication and device-to-service communication. For example, the Smart TV in our case study might need to send the user data securely to the cloud service in our case study through a secure socket layer (SSL) protocol over HTTPS communication.
- Secure on-device storage including RAM, Flash or ROM storage
- Secure operating system to protect data during runtime execution

In everyday human interactions, trust is often demonstrated when a user is able to confined in a close friend by sharing private or confidential information with the friend knowing that the friend will respect the display of trust by protecting the information from leaking to other unauthorized parties. Consequently, privacy goes hand-in-hand with trust. Privacy is sometimes defined as a critical human right "to be left alone" or an elementary need for an end-user to establish and maintain a private barrier to protect his or her information [113]. In devising a privacy solution at this level, Solove's [114] taxonomy for addressing privacy might be considered during information collection, information processing, information dissemination, and in curbing invasion.

In smart pervasive environments, the information collection process is often invisible to the end-user by virtue of the built-in ubiquity of the solution. This often raises concerns among user privacy experts. In most cases, the end-user does not have access to the information that has been collected about his or her activities. Equally, the end-user often has minimal visibility and control over the processing and dissemination of the data collected in the smart environment. However, collective intelligence and IoT promote a lot of data sharing among multiple devices. It is more critical for devices in an IoT setting to conform to standard privacy protocols that provide end-users with a level of comfort and trustworthiness that their private data will be protected. These issues have to be considered in deriving an effective architecture for hardware and software privacy.

b) Security and Privacy in the Cloud Computing Layer

Cloud computing can be defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [30]. In a typical cloud system model, there is a [115] Cloud provider – who exposes cloud services, and a Cloud consumer – who consumes these services. In our reference architecture, the IoT App Provider is also considered as a Cloud consumer.

Vulnerabilities in cloud systems can be categorized as [118] being related to Cloud Multi-tenancy, Elasticity, Availability of information (SLA), Information Integrity and Privacy, Secure Information Management, and Cloud Secure Federation. It is important the IoT provider considers these vulnerabilities in arriving at a secure solution.

Nonetheless, vulnerabilities in cloud solutions can differ for a given cloud deployment model. Some of the cloud deployment models in use today include [120]:

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud
- Virtual Private Cloud

Beyond the considerations for each cloud deployment model, there are unique security and privacy issues in each delivery model. I consider the following layers (shown in Figure 35) in an IoT solution that makes use of a *public cloud* deployment solution:

- *Services Layer* - which includes:
    - Software Applications
    - Data management systems
    - Operating Systems
- *Server Virtualization layer*
- *Physical Hardware layer* - which includes:
    - Physical hardware
    - Network communication infrastructure

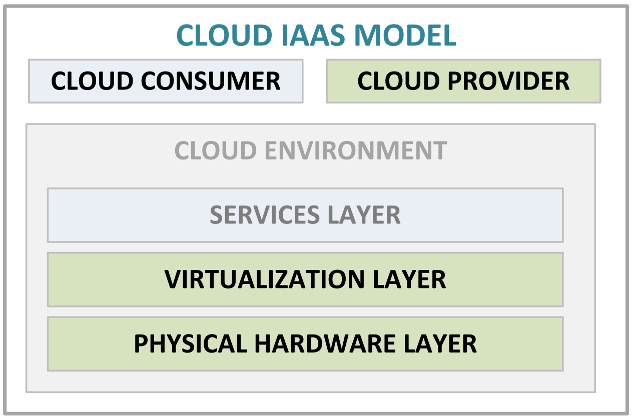


Fig. 35. Logical View of layers in Pervasive Devices [46]

Some of the popular cloud delivery models [118, 119] include:

- *Infrastructure-as-a-Service (IaaS):* Where the cloud provider offers storage and computing services on-demand. The cloud customer manages the virtual machines (VMs) and other associated infrastructure components hosted in the cloud – including data storage, operating system and applications hosted on the VMs. Resultantly, security and privacy concerns at the application and operating system level are managed by the cloud customer. The cloud provider will handle security and privacy concerns at the datacenter hosting level including the virtualization and physical hardware layers.

- *Platform-as-a-Service (PaaS):* In this delivery model, the cloud provider exposes a set of services and application programming interfaces (APIs) for developers to host web sites and services without having to deal with the scalability issues of the application as the solution usage grows. The cloud customer will have minimal control over the security practices used at the operating system-level.
- *Software-as-a-Service (SaaS):* In this scenario, the cloud provider exposes specific applications to consumers for use with a multi-tenancy approach that might use a subscription-based pay-per-use model. The Cloud Consumer will have even less control over the privacy and security implementation in this cloud-hosted solution since the entire service layer is managed by the cloud solution provider.

For a cloud consumer in an IoT setting, the trust model detailed in Itani and Kayssi's findings [115] can prove to be useful:

- *Full Trust* – where insensitive data is safely transmitted, stored, and processed without encryption on the cloud service
- *Compliance-based Trust* – where sensitive consumer data needs to be encrypted and sometimes anonymized in support of legal compliance regulations. An example might be compliance requirements for the Health Insurance Portability and Accountability Act (HIPAA) in mHealth scenarios.

- *No Trust* – where highly-sensitive customer data must be concealed from the cloud provider.

c) Security and Privacy in the IoT Apps and Service Layer

Security issues in integrating mobile agents and devices with services can be categorized as [121]: *Confidentiality*, *Authentication*, *Authorization*, *Integrity*, *Non-repudiation*, *Privacy*, and *Availability*. In most typical IoT App scenarios multiple service endpoints can be employed in the solution. The IoT system interacts with its own cloud-hosted service layer as well as external services. The IoT application user interface might have its own privacy and security concerns. In addition, the third party external services used in the solution might need to be governed to ensure that they protect the end-user's privacy and security preferences. For example, if the IoT application interacts with the Facebook Graph API [107] (similar to *Use Case 4*) – as shown in Figure 36, the end-user might have specific privacy settings set on Facebook (an OSN) that needs to be protected in the IoT system.

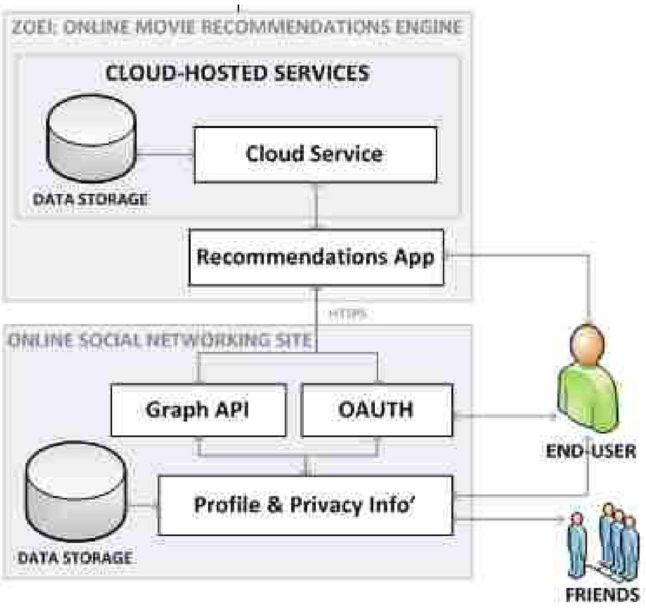


Fig. 36. External OSN service (Facebook) API interactions between an end-user and the IoT movie recommendations application [46]

d) Cross-Cutting Governance Layer

In investigating an overarching solution that can protect end-users from the security and privacy vulnerabilities inherent in pervasive and cloud systems, I believe that it might be useful to introduce a trusted third-party security and privacy governance organization and/or a standard protocol for monitoring and developing ongoing compliance requirements that can be used to certify and regulate cloud and ubiquitous monitoring device providers in a bid to garner the kind of trust that is needed in such a big sphere of concerns.

From a cloud provider perspective, Ponemon Institute [117] recommends a number of proactive steps to be taken to protect sensitive information in the cloud environment including:

- Employ policies and procedures that stress the importance of protecting sensitive data in the cloud
- Assess the security status of third party vendors prior to sharing sensitive information through a thorough audit or review of the vendors' security qualifications
- Establish a functional role dedicated to information governance oversight to ensure better security practices are employed
- Provide transparency into the security infrastructure to help instill confidence in cloud consumers that information stored in the cloud is secure

I believe that a third-party governance institution that can address the need for third-party assessment, regulations at all layers of IoT systems, transparency, policies, standards and ongoing status certification will be greatly beneficial to improving the trustworthiness of IoT applications.

4) Illustrative Case Study

I utilized *Use Case 4* as the case study for evaluating the proposed reference architecture. In line with this, some of the major components that have their own facets for privacy and security concerns include:

- *End-User Preferences* for Security, Privacy and Trust
- *Cloud Computing*: in the form of a cloud-hosted web or mobile service and cloud-based data storage
- *Ubiquitous Computing*: represented by the Kinect Sensor, Tablet device and a Smart TV
- *Service Oriented Architecture (SOA):* in the form of the Facebook Graph API [107] (web service) used for inferring the preferences of influential friends in a given household member's OSN circle as well as the YouTube API (web service) for streaming a movie trailer
- *Network communication* across wireless networks for transmitting and receiving data between the ubiquitous devices in the Smart Environment, the External Environment, and the Cloud Service Environment

Conceptually, most of the major facets of a generalized IoT implementation are likely to include the fundamental components captured in Figure 37 below.

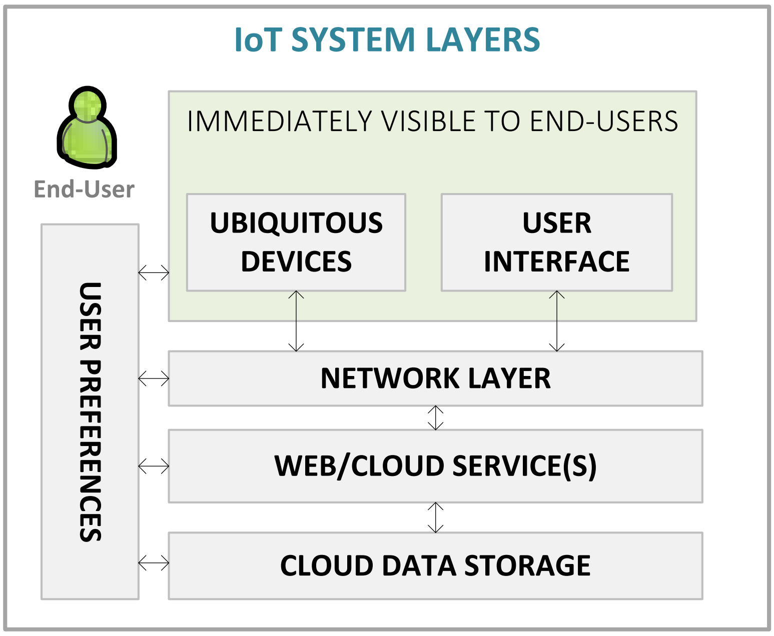


Fig. 37. Major facets for Security and Privacy in IoT App Scenarios [46]

End-users have preferences for security, privacy and trust that must be collected and adhered to at all facets of the solution. There is typically an optional user interface and a physical sensor or ubiquitous device for data collection. These physical data communication components communicate with external systems through a network communication layer using a communication protocol to a web or mobile service of some nature. These web services, in turn, persists streams of data to a backend storage device. The backend service engine and storage is hosted in the cloud.

Some of the concerns considered and lessons learned in enforcing privacy and security best practices at various layers of the reference architecture for this case study include:

- *Informed Consent:* I learned that end-users preferred to be notified when the Kinect sensor is collecting both sensitive and non-sensitive data in the smart environment. A visual cue by the form of a blinking green light indicator on the device while it is in recording mode proves to be useful.

- *Control over Privacy Settings:* A parent in the smart household may not want their children to have access to uncensored content, so the parent might want control over media content suggestions that are surfaced to the children in the household. Also, the parent might want to limit how much data is stored by the IoT App (for example, exclude geo-location information from data collection).
- *Vendor Regulation:* A third-party regulation body could be employed to monitor and expose gaps in the system based on the end-user's pre-defined security and privacy preferences. Ongoing risk assessments on behalf of the end-users could prove to be useful.
- *Access to User Data and Opt-Out:* In some cases, participants prefer control over the data that is collected about them. End-users are also interested in how their data is used and seek to reserve the ability to opt-out and delete their data at will.
- *Ongoing Reputation Access:* Beyond the participant's initial consent to allowing the IoT App access to his or her Facebook (OSN) data, it will be useful if the participant can access the privacy of the IoT solution itself at any point in time and opt-out without any loom of lock-in.
- *User Identification and Authentication:* If the identity management system throughout the IoT implementation is not accurate, uncensored content that might be appropriate for the parent but inappropriate for the child might be surfaced mistakenly to the child.
- *Physical Security and Wireless Networks:* Prevention of eavesdropping in the wireless network as well as measures to enforce security of the physical objects in the environment proves to be critical.

5) Limitations

While the reference architecture was evaluated specifically by using *Use Case 4*, the components and key concerns of the proposed model considered all 4 use cases described in this dissertation.

6) Results

Of the 18 distributed surveys, I received 14 usable responses with questions centered on evaluating the importance of the various facets in the reference architecture and how it affects their overall level of trust in the human-centered CI or IoT system:

- *Trust in the underlying Cloud data storage system*
- *Trust in the ubiquitous devices and user interface*
- *Trust in the vendor services involved in the App*
- *Need for a third-party regulating body*

Participants (end users) were asked to indicate their rating with a scale of 1 through 3 (where 3 means the characteristic is *Important*, 2 represents *Indifferent,* and 1 denotes *Not Important*). My analysis of the survey response indicates that most IT practitioners who responded to the survey (92.8%) were most comfortable with the IoT system when the immediately visible device or sensor exhibited security and privacy best practices.

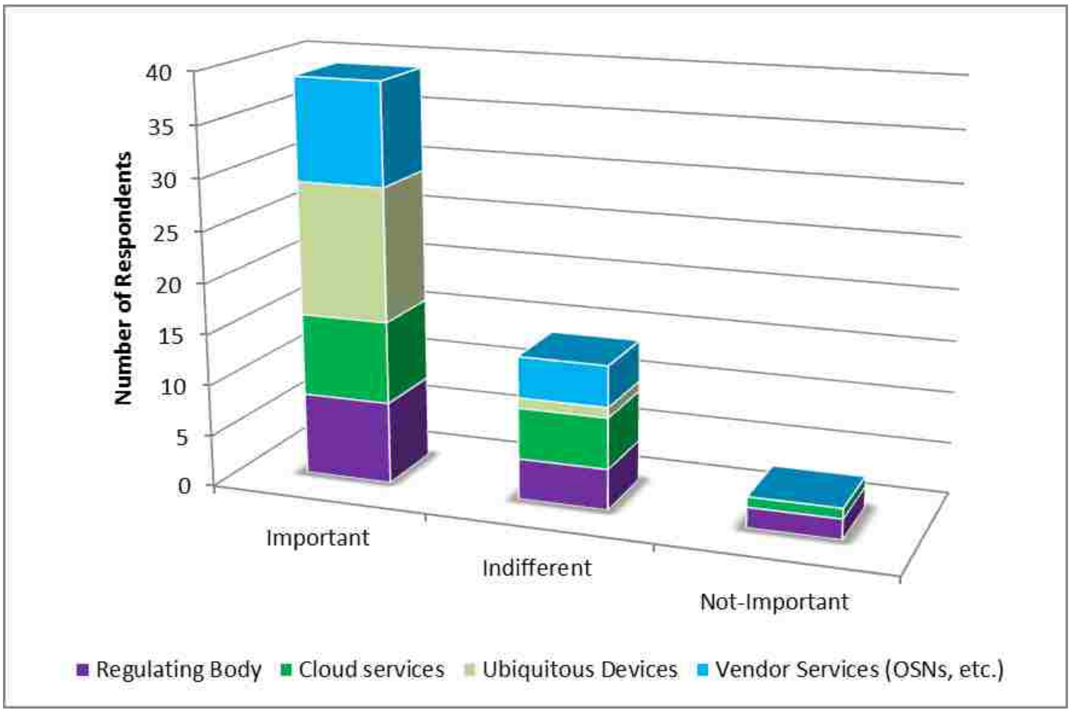


Fig. 38. Survey Response – IT Practitioners [46]

7) Discussion

Based on the findings of my user study, even though addressing key security and privacy concerns holistically helps to minimize end-user adoption barriers, perceptions related to the trustworthiness of an IoT application hangs significantly on the implementation of security and privacy best practices in the immediately visible IoT device or application user interface. Nevertheless, with growing concerns of security and privacy in IoT Application scenarios, I believe that the proposed reference architecture can be adopted by researchers and practitioners, at large, as a yardstick for guiding the implementation of security and privacy concerns at all facets of an overarching IoT or human-centered collective intelligence solutions architecture.

D. Experiment 2: Privacy Preservation in Affect-Driven Personalization

Emotion Analytics (EA) is a growing field for detecting and measuring the point-in-time emotional state of humans as a direct input to improving decision-making and content personalization [125]. Multimodal emotion recognition systems, often use a combination of data sources (including vocal intonations, gestures, facial expression data, pressure sensor data, electro-dermal response, infrared temperature, and others) to effectively predict a user's emotional state [62, 125]. Once a particular emotion or affect expression is sensed, an intelligent system can use its knowledge of the situation at hand to discern the emotional state which likely resulted in the detected affect expressions [62]. While the seeming benefits of EA resonates very well with marketing and advertising scenarios, it extends to other domains and scenarios including: pain detection in healthcare scenarios [126], emotional intelligence in human-robot interaction (HRI) research, lie detection, confessions and testimonies in legal analysis, engagement measurements in entertainment scenarios. *Use Case 4* described in this dissertation is a viable scenario for EA [58].

Collecting multimodal end-user emotion data often involves gathering image content, some speech data, textual data, sensor measurements, and more. It is quite prevalent to pursue crypto-graphical anonymization approaches when it comes to preserving the privacy of textual content in a typical data mining effort. However, when it comes to preserving the privacy of an end-user across other content types like images or video content used for facial expression analysis in a cloud-based emotion detection engine, a number of challenges have to be considered throughout, what I refer to as, the *Affect-Driven Personalization Lifecycle* (ADPL).

The three phases in the ADPL (shown in Figure 39) include:

- *Collect* – which involves data gathering
- *Analyze* – involving both real-time and batch data analysis to draw emotion-based insights
- *Recommend* – entails content recommendation

The *Collect* and *Recommend* phases in the ADPL can be used interchangeably as a starting point for the process depending on the use case in question. I constructed the ADPL to help generalize the various phases in the iterative radial cycle involved with affect-driven personalization.

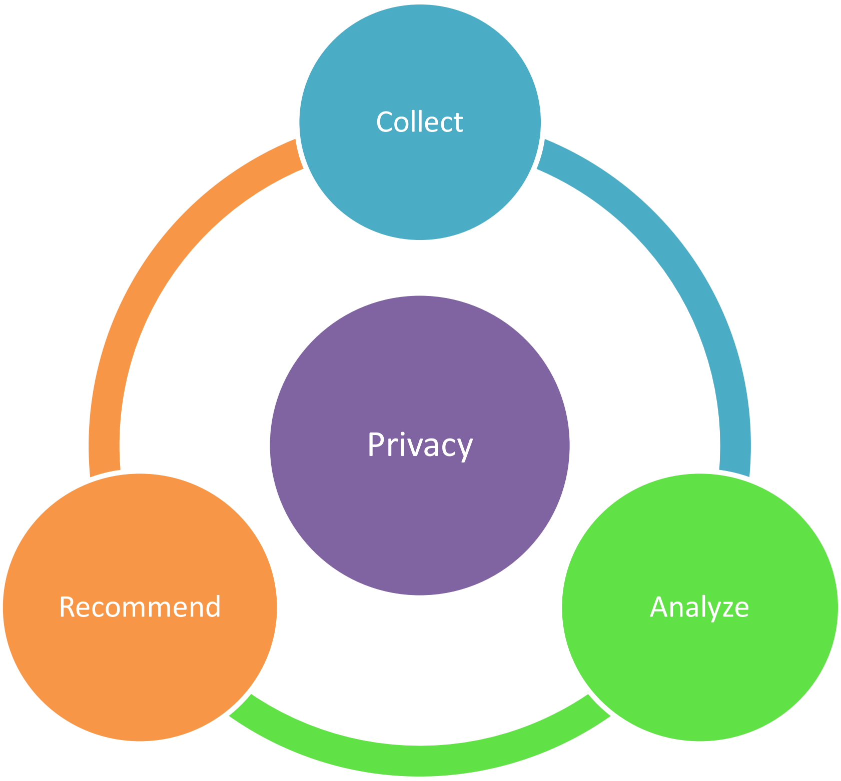


Fig. 39. Affect-Driven Personalization Lifecycle (ADPL) [58]

In *Use Case 4*, the ADPL takes the shape of the following steps:

- *Phase I: Recommend* – New "funny" jokes or digital content is generated and surfaced to the end user based on the predicted level of happiness that the joke is expected to exude
- *Phase II: Collect* – Emotion data is sensed by gathering the vocal, gesture and facial expressions of the end user

- *Phase III: Analyze* – The sensed data is analyzed to determine the level of excitement (or the intensity of "happy" emotional state) that was exhibited by the user in question, following the content delivery.

In the data mining field, the privacy-focused sub field known as *privacy preserving data mining* (PPDM) is gaining more and more popularity in recent times [122]. PPDM seeks to prevent the use of sensitive raw factual data about end users (often called *features*) as input to the data mining process, for example Social Security Numbers, Driver's License Number, and more. On the other hand, it also seeks to prevent the use of sensitive Data Mining (DM) results which can lead to end-user privacy violations [122].

Xu et al. proposed a *user-rule based methodology* for privacy protection across the *knowledge-discovery from data* (KDD) process [122]. When it comes to analyzing facial expressions in video and image content to derive emotion analytics, visual privacy protection techniques like *image distortion*, *blurring* and *object exclusion* are worthy of consideration [123, 124]. Regrettably, they are often known to demolish the inherent visual cues and behaviors that are critical to affect detection [123]. For image and video content analysis, researchers have found some success with privacy preservation through body reshaping and facial image editing techniques while preserving majority of the observable affect cues [123]. Nakashima et al. proposed an image melding-based method for modifying the facial regions discreetly to preserve the facial expressions [124].

While Health Insurance Portability and Accountability Act (HIPAA) laws in the US provide privacy protection for healthcare scenarios, non-healthcare scenarios are often left with no legal protection unless there is evidence of probable cause for harm. As depicted in the ADPL, we envision a world where end-user privacy protection is preserved throughout the lifecycle.

1) Research Questions or Hypothesis

In this section, I investigate the best practices for implementing privacy preservation techniques across the affect-driven personalization lifecycle. I offer a conceptual framework for supporting this task (as shown in Figure 13).

2) Methodology

During this investigative study, I examined various issues and approaches to implementing privacy preservation in the ADPL. I proposed a lifecycle model and an associated conceptual architecture. In addition, I provided a guide for implementing two illustrative use cases and shared the results of comparing the emotion prediction scores of privacy-preserved target images and that of non-privacy for ERFE analysis [58].

3) Key Concerns

Traditional online advertising scenarios are often susceptible to privacy violations of end users. Leon et al. posit that an end-user's privacy preferences are not only determined by the sensitivity of the information that is gathered by online advertisers [127]. In their quantitative analysis, the researchers found the following factors to be quite important to an end-user's privacy preferences in behavioral advertising scenarios: *scope of data collection and use*, the *relevance of the data collected to advertising*, and the *expected benefits of divulging a specific type of data* [127].

Affective systems are capable of amassing highly personal, intimate and sensitive data regarding our everyday lives over long periods of time. Beyond the potential for a malicious user to extract an end user's affective data, end-users can be easily identified through reverse image search capabilities. When not safeguarded, these data points can be susceptible to use in future lawsuits, insurance claim reviews, prospective employee background checks, and more [62].

While a person's emotional state detected in *Use Case 4* might be useful for personalizing future funny jokes to entertain the individual, he or she is not likely to want to share that affective state information with third-party telemarketers who might find a person in a good mood, a prime candidate for receiving the best deals for today [62]. Yet, based on Leon et al.'s findings [127], if the advertising or deal of the day is specifically relevant to the user's mood, it might trigger a different type of welcoming response. Ultimately, end-users are going to be interested in having the ability to control who can access their affective information.

Traditional batch-based data mining or data science processes often encompasses the following steps to derive knowledge or insightful results:

- Data preprocessing including data cleansing, integration and selection
- Data or feature transformation
- Data mining through appropriate methods including clustering, classification, regression, recommendations
- Pattern evaluation and visualization [122].

Rightfully so, Xu et al. acknowledge that privacy is not something that can be applied to a specific aspect of the KDD process [122]. Much like any security problem, it is important that the total system is evaluated for privacy preservation instead of focused on a specific aspect of the process. This is in line with my proposal to employ privacy preservation techniques at all stages of the ADPL process.

4) Relevant Approaches

While most PPDP studies have explored universal approaches to privacy preservation [122], it is important to note that privacy preservation requirements vary from user to user. I propose a stage where the ADPL system can learn the privacy preferences of the end user, where possible. By default, the ADPL system is expected to have some privacy preserving settings that maximizes the privacy protection. An end user can opt to relax the strictness of a given set of privacy rules as he or she sees fit.

- *Personalized Anonymity:* Depending on the opportunities for learning an end user's privacy preferences, a variant implementation of the *personalized anonymity* [122] concept can be pursued using the classic *k*-anonymity model*, p*-anonymity, etc. as a privacy preservation measure. The goal of anonymization in this case is to prevent an adversary from discovering information about a given user.
- *Multi-party Privacy Preservation:* Secure multi-party computation (SMC) is a facet of cryptography that assumes that for a number of participants, P_1, P_2,... P_n, where each participant has some private data, X_1, X_2,...X_n, the participants will be interested in the value of a public function *f* on *n* variables at the point X_1, X_2,...X_n. The idea is to present each participant in the ADPL scenario in question with their own data and the aggregate result [58]. Each participant will only have access to their own emotional state information and not the emotional state of other participants in the scenario [122].

  Imagine 3 people in a household are watching a movie using a *Kinect for Windows* mounted Smart TV. Assuming the goal of the ADPL system in this scenario is focused on detecting the collective mood (or emotional state) of the audience and subsequently selecting a movie or TV ad content that will be most suitable for the collective mood of the audience, the SMC protocol will prove to be very useful for privacy preservation [58]. This protocol can be employed at the machine learning algorithm layer to ensure privacy preservation during the KDD process.

- *Encrypted Data Provenance:* provenance techniques can be applied to the results of the ADPL process through tagging or annotation methods so it's associated ancestral data can be derived at a later date [122]. However, by encrypting the provenance data we can achieve some level of security protection in case a third-party attempt to retrieve the annotations for unauthorized use.
- *Image-Melding and Reshaping Techniques:* during the *Collect* phase of the ADPL, facial image blocking and melding techniques [124] can be used to block out images of multiple users who have not authorized the ADPL system to capture their photos. In addition, image manipulation used to achieve reshaping can be employed to mask the identity of the user in question when it comes to gesture recognition scenarios [123].
- *Result Aggregation:* in addition, the *Analyze* phase or the analytical engine can be fashioned so that it performs real-time analysis of the raw data and subsequently destroys the input data and only stores the aggregate results once the analytical engine has passed the learning stage of the KDD process.

5) The Reference Model

The reference model features various components as shown in Figure 13. The model seeks to implement privacy preservation best practices at each phase in the ADPL.

- During the *Collect* phase, various privacy preservation techniques can be applied to different data types. For example, image and video content can implement image reshaping and image melding techniques to achieve visual privacy preservation whereas textual data can be anonymized. Additionally, the SMC protocol can be leveraged to support multi-party scenarios.

- At the *Analyze* phase, aggregated results can be persisted to the associated data store in lieu of saving the raw video or image data – that is, after the engine has processed the data. Encryption of data provenance annotations can be implemented at this stage as well.
- At the *Recommend* stage, the SMC protocol can be used to surface only data that is relevant to the individual in question or aggregate data specific to the scenario at hand.

Some of the prominent personas or actors in an ADPL solution include:

- *Cloud Provider*: Represents the cloud vendor who provides cloud services for analyzing raw emotion data in the Public Cloud. For example, Microsoft's Azure Machine Learning (Azure ML) solution can be used to build the emotion analytics engine.
- *ADPL Solution Provider*: Represents the ADPL solution provider who consumes cloud infrastructure and services in an effort to deliver the ADPL solution
- *End User*: Representing a consumer of the ADPL solution.

The following use cases illustrate how the logical model might implement each of the components described in the generic model.

6) Illustrative Case Study

Drawing on *Use Case 4* described in this dissertation earlier along with other relevant scenarios [58], I evaluated the efficacy of the proposed framework. For this use case, I employed the NAO T14 humanoid robot built by Aldebaran Robotics. The T14 robot is a humanoid torso robot with 14 degrees of freedom, two cameras, two lateral speakers, and four microphones.

During the *Recommend* stage, the humanoid robot was used to present a ranked list of funny jokes from the Microsoft SQL Azure cloud data store. Using the microphones on the robot, the automatic speech recognition (ASR) capabilities of the NAO robot was used to record and manually annotate the user's response to the joke during the *Collect* stage. Depending on the content delivered, the user could speak out one of the following keywords to annotate the response as either: "*Very Funny*", "*Funny*", "*OK*" or "*Not funny*". In addition, the cameras on the NAO robot were used to capture images of the emotional state of the user and classified to determine the emotional response to each joke.

In this experimental study, I applied *skin recoloring* and *facial component blending techniques* [123] to manipulate the original image prior to sending it to the cloud-based emotion detection engine web service to detect the emotion expressed in the photo. The emotion recognition engine was hosted on the Microsoft Azure cloud. The aggregate emotional state derived from the analysis was persisted to the SQL Azure data store as an annotation of the degree of happiness that was expressed by the user in question to support future joke recommendations (see Figure 40).

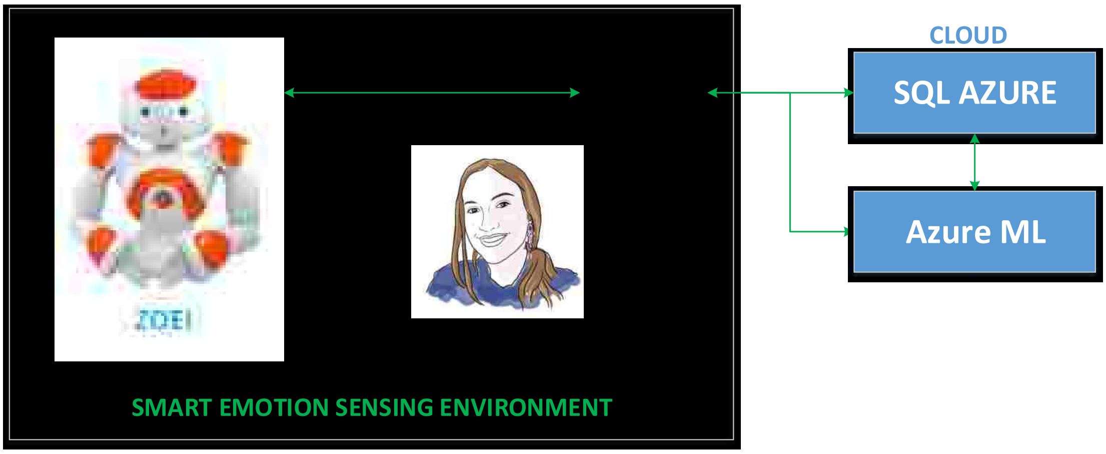


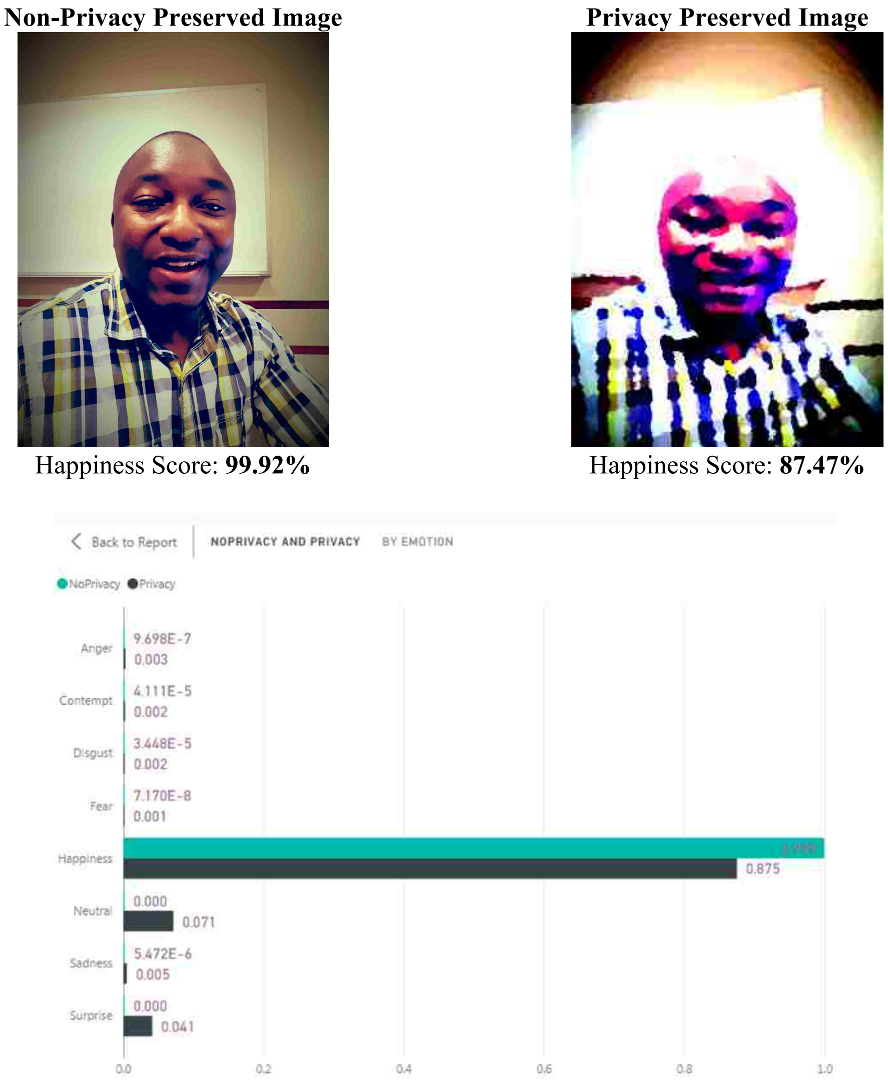
Fig 40. HRI joke telling scenario: Humanoid Robot [58]

7) Limitations

The framework can be extended to cover additional cognitive features in human-centered collective intelligence scenarios.

8) Results

I evaluated how the design and implementation of eleven use cases relates to the design of the generalized model [58]. The proposed model was employed successfully to achieve privacy preservation in images without significantly compromising the emotion recognition scores.



Non-Privacy Preserved Image

Privacy Preserved Image

Happiness Score: **99.92%**

Happiness Score: **87.47%**

Fig 41. Illustrative sample images and their associated ERFE scores for pre-distorted and distorted facial photos in support of privacy preservation in the ADPL

As shown in Figure 41, generally the prediction scores between the distorted *privacy preserved image* and the *non-privacy preserved image* followed the same pattern. In this example, the privacy preserved image was predicted as having a happiness score of 87.47% while the non-privacy preserved image had a score of 99.92%. Of the 15 images that I tested, there was generally a variance of less than 15% between the two emotion prediction scores. The image distortion techniques employed in this experiment were implemented through a *Python-Fu* script with the Gimp image editing tool [128] to manipulate the image prior to sending it to the cloud-hosted emotion detection engine for processing.

9) Discussion

While emotional analytics promises to influence many application scenarios across multiple markets and domains, there is a gap associated with a reference framework for implementing privacy protection across the lifecycle. I shared a reference model for implementing privacy-preservation in emotion analytics scenarios. I also illustrated how an affect-driven application use case can be expressed in terms of the generic ADPL reference model presented in this study. I expect that the proposed reference model will be adopted by researchers and practitioners across multiple domains to build affect-driven personalization applications that exhibit privacy preservation best practices.

E. Experiment 3: Inspiring Trust in Ubiquitous human-centered CI systems

With the recent proliferation of ubiquitous, mobile and cloud-based systems, security, privacy and trust concerns surrounding the use of emerging technologies in the ensuing wake of the *Internet of Things* continues to mount. In most instances, trust and privacy concerns continuously surface as a key deterrent to the adoption of these emergent technologies [47]. The ensuing paragraphs will present a *Secure, Private and*

Trustworthy Protocol (named SPTP) that was prototyped for addressing critical security, privacy and trust concerns surrounding mobile, pervasive and cloud services in human-centered Collective Intelligence (CI) scenarios. The architecture of the SPTP protocol is illustrated in Figure 11. The efficacy of the protocol and its associated characteristics are evaluated in CI-related scenarios including multimodal monitoring of Elderly people in smart home environments, Online Advertisement targeting in Computational Advertising settings, and affective state monitoring through gameplay as an intervention for childhood obesity.

1) Research Questions or Hypothesis

This study seeks to investigate best practices for building pervasive human-centered collective intelligence systems that inspire end-user trust in the system at large. A reference architecture and protocol design named SPTP is proposed for this task.

2) Methodology

In evaluating this experiment, I considered *Use Case 4* (discussed earlier in this dissertation) among other case studies [47]. I employed the use of an end-user survey to confirm the perceived benefits of the proposed SPTP protocol.

3) Key Concerns and Relevant Approaches

Privacy can be defined as an essential human right "to be left alone" or a rudimentary requirement for a private sphere of protection [113]. I present a brief overview of some of the characteristics of the security, privacy and trust problems in ubiquitous systems, cloud solutions and healthcare solutions.

a) Security, Privacy and Trust (SPT) in Ubiquitous Systems

While privacy concerns are typically high among savvy end-users of electronic commerce and online social networking web sites, it is more pronounced when it comes to adopting pervasive solutions [47]. Ubiquitous systems are known to unobtrusively and cunningly collect large streams of data about our past, current and future activities, in a bid to improve their ability to serve our needs [3]. However, this clandestine approach to data collection might sometimes conflict with a savvy user's privacy preferences. In most cases, concerns regarding user privacy also bleed into trust barriers pertaining to ubiquitous technology adoption. Though, Seigneur et al. posits that there is an inherent conflict between privacy and trust [113].

As the adoption rate of ubiquitous systems matures, the impact of security attacks in pervasive devices becomes critical to end-users. Some security attacks might be aimed at collecting personally identifiable information (PII) regarding users to be sold in exchange for financial gains. In smart environments, data might be collected in ways that are invisible to the end-user. With the growing adoption of wearable computing and pervasive sensors, the data that is collected about end-users can be even more private. More so, the concept of the Internet of Things (IoT) and Collective Intelligence (CI) encourages a lot of data sharing among various systems [3]. The sheer level of detail and intimacy of the data that can be collected by ubiquitous systems about end-users creates a need for these structures to subscribe to a level of privacy protection that can create an altitude of comfort and trustworthiness among end-users.

b) Security, Privacy and Trust in Cloud Computing

Cloud computing can be defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [30]. The adoption of public cloud solutions typically calls for tradeoff analysis of SPT concerns with the cost-benefit and compliance considerations of the solution in question. The compliance requirements in one country might be different from the compliance requirements in another country [129].

In addition, cloud computing comes with its own stigma of often being perceived as an insecure platform for application hosting [47]. The three main cloud service delivery models include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [118] [119]. In addition, some of the cloud deployment models in use today include Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud, and Virtual Private Cloud [120]. The security or privacy concerns for each cloud service delivery and deployment model are different.

Some common approaches to addressing these SPT concerns suggest the use of *regulatory frameworks for accountability* [131] and *provision of redress within cloud environments* [130] *responsible governance data among cloud providers*, and *privacy enhancing technologies (PET), encryption, anonymisation, security mechanism*, and more. Data encryption and cryptographic-enforced access control is particularly necessary to ensure privacy and security. Self-healing, randomized, efficient, and distributed protocols can also be used to detect node replication attacks in pervasive computing environments.

c) Health Information Security and Privacy Compliance

In spite of the adoption and improvement of health information privacy protection in the US through the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [132], there are ongoing concerns about data privacy associated with electronic health solutions. While it might seem important that ubiquitous and cloud technology providers comply with HIPAA and PCI compliance requirements, these organizations only regulate healthcare and Ecommerce applications, respectively. This leaves gaps for non-compliant vendors to remain susceptible to other vulnerabilities that can cost end-users notable security and privacy breaches.

To present an overarching solution that will protect end-users from the security and privacy vulnerabilities inherent in pervasive and cloud systems, I strongly believe that third-party organizations may need to step in and develop compliance requirements that can be used to certify and regulate cloud providers and cater to the various cloud service delivery and deployment models discussed above. SPTP can then be employed to communicate and verify compliance to the standard security and privacy policies.

4) Relevant Approaches

While several privacy frameworks and trust management protocols have been proposed over the years, I am not aware of any generic protocol that combines security and privacy policy validation and certification to drive trust management, and particularly in healthcare, cloud service and online web site scenarios. Recent studies in this area can be categorized as either:

- *high-level frameworks*: with a focus on legal compliance and risk assessments) or
- *low-level frameworks*: with a focus on technical implementation of access controls to data [47].

Neither of these approaches offers a panacea. Arguably, the most popular privacy protocol that is identical to the proposed approach is the *Platform for Privacy Preferences* (P3P) project [133, 134]. P3P turned out to be difficult to implement and further work on the protocol has been suspended. I propose SPTP as a generic security, privacy and trust protocol that will transcend web and other ubiquitous computing scenarios, whereas the domain of focus for P3P was web-based solutions.

Nevertheless, the mission of SPTP is consistent with the goals of P3P in enabling web sites to express their privacy practices in a standard form that can be verified by user agents [134] and make it easier for end-users to recognize the level of privacy compliance of a given solution without having to read the full privacy policy [133]. One of the limitations of P3P is that, while it facilitates better communication about privacy policies it does not act as an enforcement mechanism for privacy.

5) The Reference Model

In arriving at a solution to end-user privacy standardization gaps in ubiquitous human-centered collective intelligence scenarios, I propose a protocol that is capable of tagging private data with an access control list (ACL) that can be defined and managed by the originating end-user across multiple platforms. In addition, I propose that the protocol is applied to data *in-transit* and *at-rest.* The protocol should be able to retrieve and validate the *privacy policy* of a given web page or ubiquitous system against the privacy ACL defined by the owner of the private data. The data owner should also be able to gain access to his or her data and make a decision to opt-out when need be. The end-user should also be able to observe the current privacy reputation score of the subscribers to the protocol.

In addition, the protocol is designed to be administered and enforced by a third-party regulating body to create an unbiased regulation of privacy standards and policies aimed at protecting the end-user. Most importantly, the protocol implementation must ensure ease of implementation to avoid the previous plight of P3P. I prefer to look at a holistic standard protocol that can be used to regulate user data privacy and security across ubiquitous and traditional web solutions to ensure consistencies in expectations across various mediums, domains and scenarios. The conceptual architecture of the

SPTP protocol (shown in Figure 11) is described in the context of an illustrative case study in the ensuing section.

6) Illustrative Case Study

For *Use Case 4* (described earlier in this dissertation), some of the key privacy challenges include:

- *False Sense of Trust by Affiliation:* The end-user might wrongfully perceive the entire solution to be secure and trustworthy because authentication to the application is supplied by a trusted party (Facebook through its API [107]).
- *Access to Private Data Storage:* Without access to the innards of the application, the end-user can be blind-sided by the system's clandestine collection, storage and transmission of personal identifiable information (PII) and other private data elements.
- *Ongoing Certification and Reputation Status:* The end-user has no way of determining the application's current reputation for privacy and security when he/she accesses the App on the tablet device.
- *Data Privacy Access Control:* Once the profile data crosses the system boundaries of the OSN, there's no guarantee of access control protection.
- *Security in Public Cloud Storage:* There's no guarantee that PII or private data stored in the centralized knowledge store cannot be leaked to other solution providers sharing the public cloud's resources.
- *Web Cookies:* Control over data that is made accessible to third-party web sites is desired.
- *Informed Consent:* The end-users will prefer to be notified when both sensitive and non-sensitive data is collected about them in the smart environment.

- *Ongoing Reputation Access:* After the participant reviews and consents to the program, ongoing access to the privacy reputation of the solution at any point in time and opt-out options would be desirable.
- *Data Access:* In some cases, participants will be interested in having control over the data that is collected and how the data is used.
- *Hardware Vendor issues:* A standard that is adhered to by all sensors in the multimodal environment would be ideal.

To test the efficacy of the proposed SPTP protocol, the Kinect for Windows sensor is mounted on a television in a smart living room. In addition, a human subject is able to periodically interact with a NAO Humanoid robot. Using keyword detection techniques, private data collected by both the Kinect Sensor and the Humanoid Robot is transmitted and persisted in an SPTP tagged form through a Windows Azure Cloud Web Service (PaaS) to a storage account. The simulation seeks to demonstrate the use of several heterogeneous systems in a collective intelligence-inspired solution for activity monitoring [11]. The Kinect sensor is able to transmit data to the cloud storage service through a wireless (WiFi) connection established through a connecting computer. The NAO robot and the Kinect Sensor were both programmed to displays a consistent visual cue when in *data recording* mode.

In this case study, the user's privacy preference ACL is applied to each recorded data segment in the form of a tag that can only be decrypted using the user's privacy identifier. An *informed consent form* is presented to the target end-user describing the scope of monitoring and his rights to the data. A digitally-signed online form indicates the type of activity that will be monitored and stored. The user's preferences are captured as an ACL tag that is subsequently applied to future recordings.

The human subject is also able to review information collected in the smart environment (through a web portal) to ensure that it conforms to his or her predetermined privacy preferences.

When the user decides to revoke a portion or all of the data that was previously collected about him or her, there is an option available through the web site to facilitate this. The user's preference is then subsequently honored in all third-party systems that have previously consumed the private tagged data within a period of time – that is, for the services that also subscribe to the SPTP protocol.

7) Limitations

The SPTP solution can be exposed to a wider audience to fully expound the promise of SPTP in ubiquitous and online systems.

8) Results

To test the hypothesis that SPTP is likely to inspire trust in the adoption of ubiquitous systems among adults, I conducted a survey to study the acceptance of the proposed approach after demonstrating the use of the SPTP protocol in a simulated smart environment for monitoring and interacting with a humanoid robot.

Of the 20 distributed surveys, I received 14 usable responses. The questions asked in the survey were categorized as *Consent, Cues*, *Access*, and *Reputation*. The survey respondents were also categorized as *technologically savvy* (i.e. 9 IT practitioners) and *non-savvy end-users* (5 participants with no IT practitioner background). The age range of the respondents fell between 25 and 53 years old. Participants were asked to indicate their rating with a scale of 1 through 3 (where 3 means the characteristic is *Important*, 2 represents *Indifferent,* and 1 denotes *Not Important*). The results of the user study are illustrated in Figures 42 and 43.

My analysis of the survey response indicates that most IT practitioner respondents (66.7%) were concerned with having some form of verbal or visual cue present when information that they perceive to be private is recorded and transmitted. In general, users concluded that having a dedicated third-party service that regulates and certifies security and privacy in these environments could contribute to their level of trust in the system. Most of the non-savvy users expressed strong interests in having the robot instill a sense of connectedness and show unconditional care as a key driver for trustworthiness of adopting the simulated smart-environment.

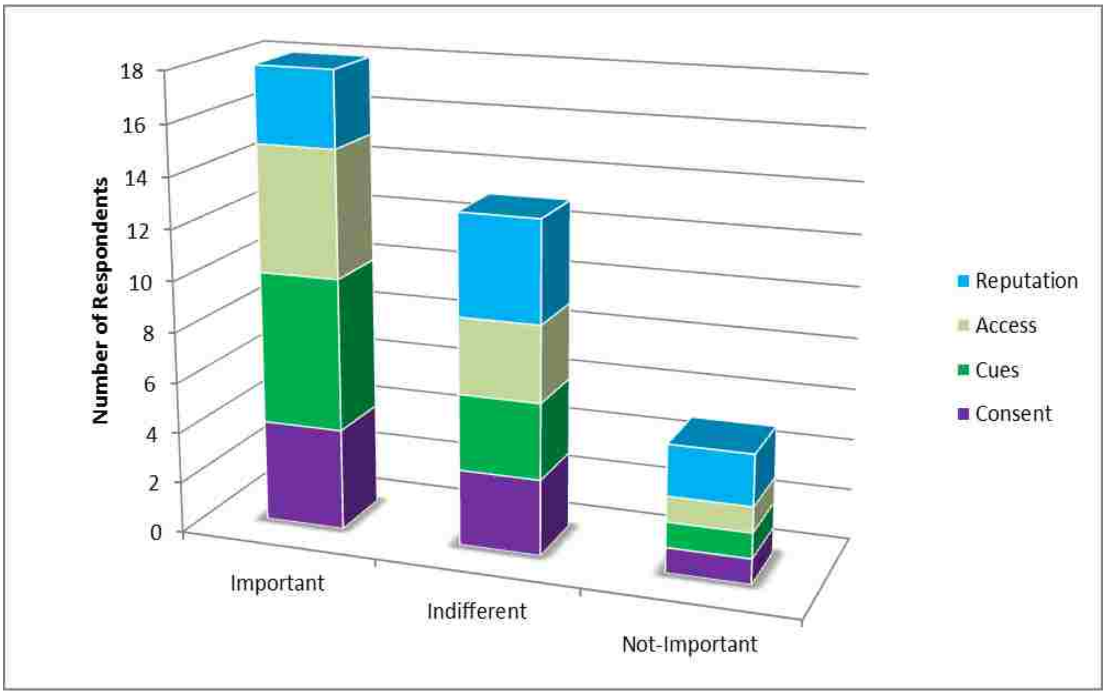


Fig 42. Technologically Savvy End-User Response

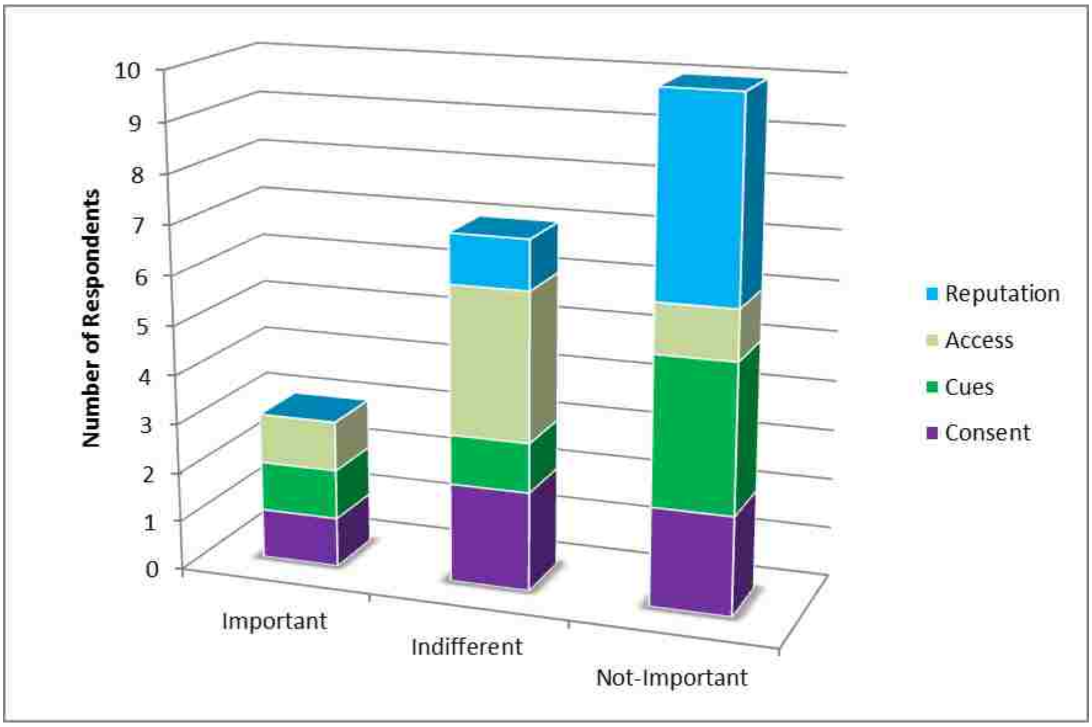


Fig 43. Non-Technologically Savvy End-User Response

9) Discussion

With the outburst of cloud services and the advent of pervasive and context-aware services, it is increasingly necessary to ensure that sensitive data is not compromised. As the results of the survey indicates, the IT savvy users have more trust and confidence in cloud-enabled ubiquitous human-centered solutions if they can garner some form of assurance that a third-party privacy protocol that enforces compliance standards has certified the application for use.

Similar to the Data Security Standards (DSS) compliance requirements that often governs the Payment Card Industry (PCI) I envision that it will be useful for third-party entities to adopt our proposed protocol or a variant of it, for managing the expectations for trustworthiness among cloud-enabled ubiquitous systems and web sites.

F. Summary

While there are several cross-cutting concerns involved with human-centered collective intelligence scenarios, I examined some of the key challenges and relevant approaches to preserving privacy and inspiring end-user trust in all-encompassing CI solutions. I proposed several reference architectures for guiding the design of privacy preservation, trust and ultimately security features across multiple application scenarios.

I. CLOUD RESOURCE OPTIMIZATION

A. Overview

To address some of the key cross-cutting architectural concerns itemized in the ZOEI framework, with respect to *automatic-scaling* or *transparent elasticity* (based on runtime conditions), *high availability*, and *performance*, I propose the use of cloud computing solutions to facilitate the data storage and machine learning process needs appropriate for supporting production-ready human-centered collective intelligence solutions. While all the use cases considered in this dissertation made use of the Microsoft Azure cloud, I contend that most of the features utilized in the application scenarios can be enabled through other leading mainstream public cloud computing providers including Google and the Amazon Web Service cloud platform.

Erl et al. [29] posit that some of the key business drivers for cloud adoption are inspired by:

- *capacity planning*,
- *cost reduction*, and
- *organizational agility*.

When it comes to operationalizing a fully-featured CI solution, it is important to understand some of the key risks and challenges associated with selecting a cloud backend for the job. For the scope of this dissertation, I will focus on investigating a few challenges associated with using *public clouds*. Erl et al. stated that the most critical challenges in cloud computing include [29]:

- *increased security vulnerabilities* pertaining to overlapping trust boundaries when the cloud service provider shares resources across multiple cloud consumers,

- *reduced operational governance* stemming from the cloud provider’s control over its own platforms,
- *limited portability between cloud providers* imposed by dependencies on proprietary platform features that are not transferable from one cloud to another
- *multi-regional compliance and legal issues* associated with regulatory compliance concerns pertaining to the geographic location of the cloud provider’s data centers.

The previous section touched on key privacy and security challenges associated with utilizing cloud computing.

B. Challenges

In this chapter, I share my findings from investigating the following challenges associated with adopting a public or hybrid cloud solution to support the data storage and computing needs of human-centered CI systems:

- *Challenge 1*: cloud portability and high availability concerns associated with utilizing multiple public cloud providers, particularly for mission-critical CI scenarios including healthcare applications, and others.
- *Challenge 2*: investigate best practices for selecting various cloud delivery models in support of the potential *big data* processing needs associated with social media intelligence (SMI) and human-centered collective intelligence scenarios. In most human-centered CI scenarios, multiple agents and sensors would be expected to stream large amounts of data (*from the smart interaction environment*) for processing and storage, while social media and other online data sources (from the *external environment*) would be possibly merged into the data stream to derive collective insights.

C.Experiment 1: Implementing Multi-Cloud Portability

In recent years, we have witnessed several cloud outages across multiple high-profile cloud providers who are otherwise considered to be widely reliable in terms of cloud service uptime [54]. Unfortunately, when a cloud provider experiences an outage it can have a major financial and functional impact on mission-critical applications hosted on the provider's infrastructure. In 2013, some of the prominent cloud outages lasted anywhere from a five-minute failure to a week-long service disruption [135]. These unplanned outages can sometimes contribute unacceptably to an immeasurable cost to brand reputation and, resultantly, lost business. Reliability is quite indispensable in mission-critical systems and it can have a major toll on customer trust [136]. It goes without saying that lost trust stemming from the lack of high-availability is not surprisingly a major deterrent to the adoption of cloud computing solutions of various kinds.

Some notable high-profile cloud service disruptions recorded towards the end of the year 2013 (that is, within a five-month span as illustrated in Figure 44) include [135]:

- *Facebook.com and Apps*: June 2013 – lasted thirty minutes affecting all Facebook hosted Apps and, of course, the social networking site as well.
- *Google.com and Google Cloud Apps:* The Cloud Apps outage occurred in July 2013 lasting forty minutes and affecting Gmail, Google Calendar, Google Talk, Google Drive, Google Documents, Google Spreadsheets and Google Presentations [137]. Also, in August of that year, Google.com was down for about five minutes.
- *Microsoft's Outlook.com:* August 2013 – sporadic disruptions during a three-day period. In November 2013, sporadic issues lasting hours caused service

disruptions for Windows Azure Cloud, Office365.com, other Microsoft web properties, and more dependent cloud consumer applications.

- *Amazon.com and AWS:* August 2013 – The initial outage affected Amazon.com, which happens to be an Ecommerce software-as-a-service platform – lasting about 45 minutes. A few days later, the Amazon Web Services (AWS) cloud reported performance degradation issues on its Elastic Computing (EC2) service as well as connectivity problems with its Elastic Load Balancing systems at the North Virginia datacenter. The issue emerged again in September lasting under two hours.
- *Apple's iCloud:* June and August 2013 – partial service disruption affecting a cross-section of its users. Some of the affected features include iMessage, Photo Stream, Documents in the Cloud, Backup and Restore, and iPhoto Journals.
- *Verizon's Terremark Cloud (Healthcare.gov):* in October 2013 the *Healthcare.gov* web site went down for several hours due to a service disruption in the Verizon cloud datacenter.

To highlight the severity of cloud outages on cloud consumer applications, I focused on examining the impact of cloud service disruptions on mission-critical systems like human-centered CI solutions and online healthcare applications that leverage cloud services.

While a number of enterprise organizations and individual cloud consumers often patronize solutions built on the *Software-as-a-Service* (SaaS) delivery model, most web-based cloud consumer applications are likely to leverage a *Platform-as-a-Service* (PaaS) cloud service delivery model. In the PaaS model, developers can leverage services that are built and maintained by the cloud provider. Consumers can easily upload their code to the cloud (for example, Google Cloud, Windows Azure, etc.) to take advantage of the automated high-scalability features inherent in the model, as the target application's usage intensifies [138, 139]. For the sake of this study, I focused on the widely used *public cloud* deployment model.

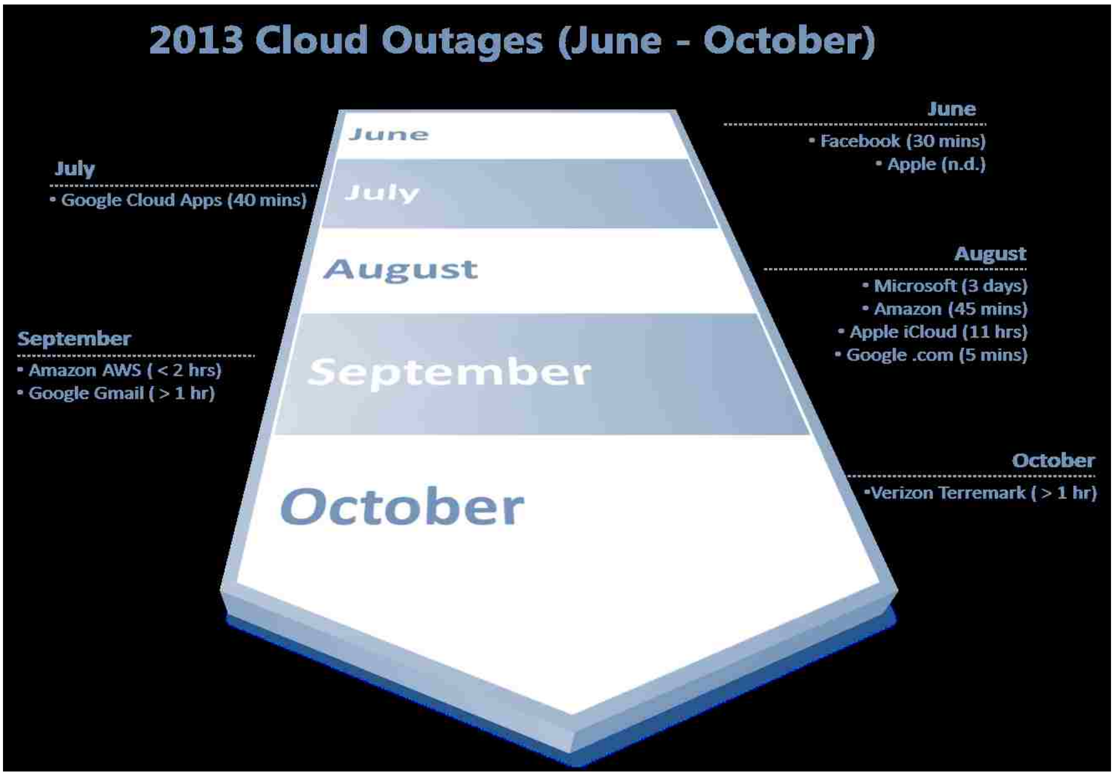


Fig 44. 2013 Cloud Outages – June - October [54]

In practice, most cloud vendors do not present easy opportunities for porting a given cloud hosted solution from one cloud vendor or provider to another. In this study, I explore some of the portability gaps in PaaS solutions today. The proposed reference architecture goes beyond the high-availability problem in PaaS scenarios by also exploring interoperability and portability quality attributes for building software solutions that can be easily ported from one cloud provider to another. To afford our template solution the ability for automatic failover between PaaS vendors, I established a common platform for building the prototype solution which was, by itself, an interesting problem to explore.

1) Research Questions or Hypothesis

Investigate some of the key characteristics in this area of concern and present a reference architecture for automatic failover between multiple Platform-as-a-Service (PaaS) cloud delivery providers in a bid to maximize the delivery of architecturally significant quality attributes pertaining to High-Availability (HA), Performance and Disaster Recovery (DR) in a prototypical mission-critical application.

Hassan and Holt [140] posit that establishing a reference architecture promotes re-use, reduces maintenance costs, and serves as a benchmark for software governance. I expect this reference architecture to serve cloud solution architects and developers in a similar fashion.

2) Methodology

Using a case study involving Microsoft's Windows Azure cloud and the Google App Engine cloud platforms, I investigated some of the key characteristics in this area of concern and present a reference architecture for automatic failover between multiple Platform-as-a-Service (PaaS) cloud delivery providers in a bid to maximize the delivery of architecturally significant quality attributes pertaining to High-Availability, Performance and Disaster Recovery in a mission-critical application prototype.

To test the efficacy of this reference architecture, I evaluated a case study featuring a mission-critical movie recommendation and video streaming software solution prototype that is primarily hosted on the Windows Azure PaaS cloud solution. I simulated a number of cloud outages on the Windows Azure PaaS solution to test the proposed failover automation solution. The solution was involved with shifting incoming web site requests destined for the movie recommendations engine to a redundant Google App Engine PaaS solution that was capable of taking over the previous Azure PaaS workload to minimize downtime and ensure high-availability.

3) Key Concerns and Relevant Approaches

Previous studies focused on a combination of *datacenter redundancy solutions* within a given cloud provider, *server clustering*, *load-balancing*, *data replication*, *capacity planning strategies*, *aging infrastructure refresh policies* within the cloud provider, and *internal cloud monitoring and automation approaches* for minimizing the impact of cloud service disruptions [54]. However, it is important to note that some of the recent cloud outages transcend multiple datacenters hosted by a given cloud provider. In other words, some of the outages reported in the past couple of years took down an entire cloud provider (for example, Microsoft Azure).

As a result, I propose an automation strategy for monitoring external cloud services hosted on a given cloud provider's PaaS infrastructure, by utilizing ongoing data replication solutions between multiple cloud provider data stores while implementing an automatic failover solution to minimize the impact of cloud service disruptions on mission-critical applications. Knowing that public clouds often employ a *pay-as-you-go* model [139], I fashioned the proposed solution in a way that minimizes the cost of data replication between cloud providers. The proposed reference architecture can be employed to improve high-availability, fault-tolerance, disaster recovery, and resilience against performance degradation issues affecting a given cloud provider.

4) The Reference Model

In creating the generalized *reference architecture* for improving high availability in *cloud-provider-down* conditions, I offer a cross-cloud hybrid PaaS solution illustrated in Figure 16. The ensuing paragraphs examine the characteristics of the proposed reference model.

a) Code Portability and Interoperability in PaaS

Due to wide variations in application programming interface (API) implementations across multiple cloud providers, I created an abstraction layer to port the application source code in order to meet the API requirements for both Cloud A and Cloud B. At the time of code deployment to the cloud, the build process generated two separate deployment packages that were, in turn, deployed to the various destination platforms.

b) SLA Monitor Agent

A Service Level Agreement (SLA) Monitor Agent was implemented as a background process that is deployed on both cloud provider instances and remains accountable for monitoring performance and service disruptions on the cloud service hosted on an opposing cloud platform to maximize service uptime. For example, the SLA Monitor Agent on Cloud B will typically monitor the cloud service on Cloud A and vice versa. The monitoring agent is capable of failing over and failing back a cloud service automatically when a service disruption is discovered and subsequently when the service is restored, respectively.

The SLA Agent sends poll messages ($STATUS_1\ to\ STATUS_k$) to the cloud service under investigation, for example, while monitoring the active $Web\ App$ in Figure 3. The monitor then receives polling response messages (that is, $STATUS\_TIME_1$ to $STATUS\_TIME_k$) that indicates the elapse time. When the cloud service is unreachable, the value "*TIMEOUT*" is returned. Based on the threshold parameters defined for retrying the poll process, the agent can determine whether or not the event was a very infinitesimal disruption (or a false positive) and, hence, does not warrant a failover.

In the event of a failover, the agent will notify the cloud consumer's administrator and also run automated scripts to complete the failover process (e.g. using Azure PowerShell scripting commands). All activities discovered by the SLA agent are logged into an SLA event log data store. The overall SLA reports and analysis of the cloud service can be reviewed through a data visualization interface.

c) Failover and Failback

I propose an *active-standby* data storage setup between the clouds. This is achieved through data replication between the two clouds. However, the web front-end service will be setup with an *active-passive* configuration and failover will only occur from Cloud A to Cloud B in an instance where the primary cloud, is no longer available or experiences service degradation. The architecture also supports automatic and manual failback scenarios where the system will redirect traffic from Cloud B back to Cloud A (the primary cloud) when A has been confirmed to be reliable and capable of taking on web traffic. During failback, data replication from cloud B to cloud A is initiated by the *SLA monitoring agent*. When the monitoring agent confirms that cloud A's data store is fairly consistent with that of cloud B, the front-end service failback process will be initiated.

d) Algorithm for Cloud Failover

The fault recovery algorithm implemented for this model is described in *Algorithm 1* (earlier in this dissertation). The two *status* conditions under which a failover will occur include situations where performance degradation in a given Cloud Provider is detected by the SLA Monitoring Agent or the active Cloud Provider is down.

e) Recovery Time and Recovery Point Objectives

It is quite complex and near impossible to automatically switch between clouds with zero tolerance for data loss [32]. Hence, I defined a recovery time objective (RTO) and an associated recovery point objective (RPO) in both failover and failback scenarios. The cloud *Monitoring Agent* is focused on delivering the least amount of time for functionality recovery by obtaining a very low RTO.

f) Database and Storage Replication

Storage data replication is achieved through a custom array replication solution that is governed by the SLA Monitor Agent. Data replication is achieved through a custom log shipping process that is optimized to ensure that in the event of a service failover; only 15 minutes' worth of data entered in Cloud *A* and pending replication to Cloud B will be lost. To secure sensitive data transfers between the two clouds a virtual private network (VPN) is implemented.

g) Dynamic DNS (DDNS)

Domain names are typically hosted by multiple distributed data stores globally [14]. This makes it difficult to map a domain name that was previously pointing to Cloud A's IP address for a web application, to a new IP address presented by Cloud B's hosted web application during a failover. Using the *Dynamic Domain Name Service* (DDNS) feature, I was able to satisfy the requirement for implementing automated near-instantaneous DNS record updates to minimize downtime associated with domain name propagation globally. Because each PaaS cloud provider presents a unique IP address and domain name for the cloud-hosted PaaS web site, I employed a domain name that was agnostic to both cloud providers. This domain name was hosted by an external DNS service provider.

5) Illustrative Case Study

Drawing on *Use Case 4* described earlier in this dissertation, I implemented a prototype solution for delivering web-based personalized movie recommendations and video streaming content. The web site was deployed to both the Google App Engine and the Windows Azure PaaS platform. An SLA Monitoring Agent was also deployed to both clouds, taking into account the reference architecture described earlier. The *active cloud* was defined as the Windows Azure cloud (*Cloud A*) whereas Google's App Engine represented (*Cloud B*) the passive cloud platform (see Figure 16).

The Movie Recommendation application (App) features static image content which is stored on the cloud storage service and other Software-as-a-Service solutions as well as Facebook [107]. Other data elements served on the web site are dynamic in nature and can be supplied to the end-user through a database call invoked by the web application based on the user's interaction with the application. Figure 45 depicts some of the cross-component interactions that are imminent in this scenario.

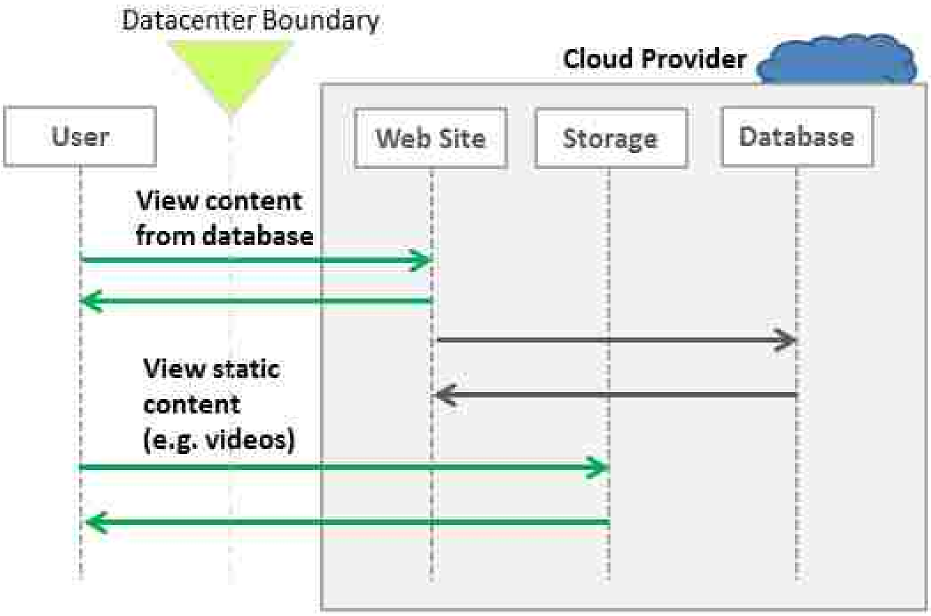


Fig 45. Cloud Bandwidth Profile of our Video Streaming App [54]

I explored this example, as a archetypal mission-critical scenario, in the sense that if this type of web-based application were to take center-stage as a core entertainment resource for end-users, then the SLA expectations for the application could be comparable to that of Netflix, Google TV, Amazon Prime, and the likes.

In evaluating the prototype solution, I selected the Google App Engine and Microsoft's Azure PaaS solutions because they currently offer support for multiple programming languages which makes it a bit easier to implement our deployment abstraction layer.

6) Limitations

Though, *cloud vendor lock-in* can be achieved by keeping PaaS APIs a bit difficult for porting code between clouds, I expect that with time most PaaS solution providers will improve the code portability quality attribute and further minimize the learning curve associated with pursuing this approach.

The proposed reference model is also predicated on the assumption that it is very rare for two major cloud providers to experience a down condition concurrently. As a result, the scope of my investigation is focused on utilizing two major public cloud PaaS providers. Though, in extreme cases, the model can be extended to accommodate more than 2 cloud providers.

7) Results

Some of the key events logged in the SLA Monitor's log during the simulation test include:

- *Timeouts* – indicating that the cloud service was no longer accessible
- *Poor Elapse Time* – indicating how long it took to access a pre-defined critical transaction in the web application based on a pre-determined performance threshold
- *Cloud Failover* – due to a number of consecutive timeouts or poor elapse time notifications
- *Cloud Failback* – indicating that the application has been successfully failed back to the original Windows Azure PaaS platform

The SLA Monitoring Agent was able to detect simulated server timeouts and software performance degradation failures with minute detection granularity. I was able to optimize the *retry waiting period threshold value*, the *number of consecutive timeouts used for sifting out false positives*, and the *polling interval parameters* to reach an optimal and performant solution that was capable of detecting service interruptions fairly quickly and, in succession, initiate the failover and notifications process.

To minimize the effect of network flooding and some degree of self-inflicted denial-of-service issues, I adjusted the *polling scheme* so each subsequent retry will implement a multiplier of the original retry wait time till the maximum number of retries was reached.

For this experiment, I relaxed the recovery time objective (RTO) to minimize the potential cost of replicating multiple videos and associated data across the VPN connection. In the experimental trials, the longest period of time tracked for performing a full cutover from *Cloud A* to *Cloud B* was recorded in the *execution time for DNS update replication* in some geographically dispersed test locations.

8) Discussion

Based on the findings from my HA and DR simulation tests, we described a template solution architecture for implementing automatic failover between PaaS cloud provider platforms. In this study, I highlighted opportunities for using DDNS, an abstraction layer for cross-cloud deployment solutions and a custom replication solution for achieving high availability failover for mission-critical solutions that seek higher SLAs in cloud systems. Based on some of my lessons learned, I presented an algorithm to help shape future implementations of automatic failover in PaaS scenarios. Needless to say, with growing concerns regarding recent cloud service disruptions among high-profile cloud providers, it is in the interest of cloud consumers who employ the PaaS model to consider adopting and extending the reference architecture presented in this study.

D. Experiment 2: Implementing Social Media Intelligence in the Cloud

As the social media upsurge of today continues to mount, opportunities to derive collective intelligence from online social networking (OSN) content sources are inevitably expected to grow [48]. While enterprise organizations and research institutions make a dash for identifying rich insights and opportunities to tap into the millions of conversations and user profile relationships exposed by this new social-influenced big data phenomenon, architectural concerns regarding the storage and processing of large datasets unearthed by OSNs, along with performance, scalability, fault-tolerance, security, privacy, and high-availability solutions have become an area of concern for social media intelligence (SMI) solutions.

In this study, I present a reference architecture, for designing SMI solutions in support of the overarching human-centered collective intelligence class of problems. In addition, I showcase a case study for SMI applications (*Use Case 4*) built on this architecture. The study was focused on implementing Social Graph Influence (i.e. in a Facebook-influenced Movie Recommendations solution).

1) Research Questions or Hypothesis

Investigate the challenges and approaches to implementing social media intelligence solutions using cloud infrastructure. Derive a reference architecture to support future solution designs.

2) Methodology

I evaluated the ‘goodness-of-fit’ in applying the model to two case study solutions and presented the results from my performance analysis of cloud-hosted solutions across multiple cloud providers like Amazon AWS, Microsoft Azure and Google Cloud.

3) Key Concerns and Relevant Approaches

In the face of recent advancements in big data and cloud computing technologies, my research goals are well aligned to building high performance data intensive solutions that leverage collective intelligence from various sources. Invariably, large-scale SMI solutions happen to offer a good platform for evaluating some of the architectural boundaries that I wish to investigate.

From the implementation of SMI for social influenced search results ranking on Microsoft's Bing.com search engine [141], to widespread applications in delivering contextual and relevant advertisements on web sites, there is a wide spectrum of opportunities for harnessing large-scale SMI solutions to drive a competitive advantage. While there are several scenarios that can leverage social media influenced collective intelligence solutions, I am particularly drawn to evaluating data intensive and computing intensive case studies that cut across the two major classes of SMI entities (shown in Figure 15). Some of the architectural concerns and requirements pertaining to these scenarios are described in the ensuing section.

a) Social Influence in Movie Suggestions

A natural way to determine suggestions for movies that a given user might be interested in, could entail asking friends who have similar tastes as the user in question or people who knowingly or unknowingly appear to influence the user to provide recommendations. If that scenario is transposed into a world where most of our friends and other people who potentially share similar "tastes" in movies as we do, then perhaps harnessing the power of social intelligence to simulate an *always-on* web of recommendations based on preferences gleaned from similar users and our self-reported "friends" could be a very viable option. That, in essence, is the premise of this particular case study – that is, *Use Case 4*.

This interesting and useful SMI solution is not without significant architectural concerns. Some of the characteristic architectural concerns and non-functional requirements that will need to be addressed in a reference architecture that supports this type of solution include but are not limited to [48]:

- *High Performance:* A large-scale implementation of this solution across multiple households will require an interactive web service solution that is capable of withstanding high web traffic generated from various sources including multiple devices and platforms (i.e. Smart TV Apps, Table App, Web Site App, etc.).
- *Automatic Scalability:* It will prove to be expensive to support the high traffic demands of an interactive web service on a traditional datacenter hosting platform. Consequently, a public cloud-hosted solution that offers a *pay-as-you-go* option might be useful for weathering the proverbial turbulent storms that can be caused by periodic and seasonal spikes in content demands. For example, the needs for movie content viewing might be higher during the evenings when most people are home relaxing than in the middle of the day when majority of the population is working or in school.
- *High Availability:* Since end users might depend on this engine to suggest the next show that they watch, the solution will need to be able to withstand minor service disruptions and remain fault tolerant.
- *Fast Machine Learning Algorithm:* In determining the similarity score and social influence of a given user's Facebook friends (in support of social intelligence)**,** optimized algorithms will be useful in processing and generating relevant insights quickly.
- *Security and Privacy:* Social media, by default, comes with a looming privacy connotation, and rightfully so. Leveraging a cloud-hosted solution opens up

further concerns about privacy and security. End users are going to be concerned about the ubiquitous need for this solution to glean social intelligence data from their Facebook profile. Facebook's OAuth authentication strategy [107] can be used to address issues with authentication but authorization remains a different area of concern.

- *Data Storage:* In this case a relational database management system (RDBMS) will be useful for storing the structured data.

b) *Sentiment Analysis in Social Content*

While the social profile SMI application described in the previous scenario presents challenges with managing large structured data sets, Social Content Analysis (in the SMI classification spectrum) deals with larger datasets consisting of user-generated content (UGC). The analysis of unstructured social media content data often requires the use of big data storage and analysis techniques. It is estimated that the size of the "digital universe" was 0.18 zettabytes in 2006 – where a zettabyte is equivalent to one billion terabytes [142]. *Big Data* is here to stay though the growth of unstructured data is at an unprecedented high. There were over 30 petabytes of UGC data stored, analyzed and processed by Facebook in 2012 [143]. In the same vein, Twitter was supporting about 175 million tweets daily as of 2012 [143].

It comes with no surprise that some of the architectural concerns for a big data solution that supports SMI might differ slightly from that of a social profile analysis solution that is more focused on analyzing structured data in most cases. Of course, there are hybrid solutions that require the storage and analysis of both types of SMI entities.

Some of the unique concerns in this scenario include:

- *Data Storage:* In this case, unstructured data will be processed by a batch process. Data consistency is not as critical in this batch processing scenario as it is in the interactive solution presented in the first scenario
- *Elastic Scalability:* Horizontal scalability is of the essence in this scenario. Making use of a cloud hosted Hadoop solution exposes opportunities to scale up and down seamlessly
- *Fault-Tolerant Storage System:* A graceful fault-tolerant distributed file system like the Hadoop File System (HDFS) proves to be useful when running the solution on commodity hardware [144]
- *Bandwidth*: Network bandwidth is usually a scarce resource in MapReduce implementations though making use of data locality optimization minimizes this concern [144]
- *Efficient Classification Algorithm:* An efficient algorithm for classifying sentiments in the twitter messages is critical.

4) The Reference Model

Considering the SMI scenarios described in the previous section, I designed a technology agnostic reference architecture that takes into account key non-functional requirements and architectural quality attributes. The reference architecture diagram is presented in Figure 17.

a) Key Characteristics

By employing a public cloud-hosted solution in the reference architecture, a lot of the heavy-lifting regarding elastic auto-scaling, load-balancing, fault-tolerance and high availability zones across datacenters is intrinsically offloaded to the cloud provider. As a cloud consumer, the SMI application owner might still need to make tradeoff decisions regarding which type of cloud deployment model is best suited for each component in the reference architecture.

For example, for an SMI web service interface, I recommend the use of a Platform-as-a-Service (PaaS) cloud solution in lieu of an Infrastructure-as-a-Service (IaaS) model in order to maximize the promise of auto-scaling and minimize the time investment needed to manage virtual machines and their associated operating system requirements on the cloud platform.

In my investigation, I leveraged various services across public clouds including Amazon AWS cloud, Microsoft's Azure cloud and Google's cloud for various scenarios. Consequently, the proposed architecture transcends any one specific cloud platform. I encourage the use of various machine learning algorithms to build social media intelligence. Leveraging Apache Mahout for implementing distributed or scalable machine learning algorithms can be useful in solving collaborative filtering, clustering and classification problems. I found it useful to leverage Python as a programming or scripting language that worked consistently across various cloud provider platforms.

b) Logical View of the Architecture Model

A logical view of the proposed reference architecture is illustrated in Figure 17. The actors or personas involved in the architecture are also labeled in the illustration. The logical architecture consists of a Presentation or Front-End Tier, a Data Management Tier, and a Storage Tier. These layers and components can be implemented differently for each SMI solution. Though, in most cases all layers are fully utilized.

c) Key Cross-Cutting Concerns

Some of the recurring quality attributes that appeared to resonate well with the cross-cutting non-functional requirements identified in my architectural analysis of the case studies presented in earlier include:

- High Performance
- Elastic Scalability
- High-Availability and Disaster Recovery
- Fault-Tolerance and Durability
- Fast and Scalable Machine Learning Algorithms
- Security and Privacy.

d) Architectural Components and Relationships

The reference architecture features various architectural components. Notably, I identify some of the most prominent personas or actors in a cloud-hosted SMI solution as:

- *Cloud Provider*: Represents the cloud vendor who provides cloud services in the Public Cloud. For example, Amazon, Google, Microsoft.
- *Cloud Consumer*: Represents the SMI solution provider who consumes cloud infrastructure and services in a bid to deliver social intelligence solutions.
- *Social Media User*: Representing a consumer of social media who the SMI solution seeks to glean information about.
- *Friends*: In the general sense, these groups of users tend to have a relationship of some sort with the Social Media User. Both parties participate on a Social Media communications channel like an OSN.

I identify a load-balanced and auto-scaling application tier as a layer that represents a set of cloud-hosted infrastructure dedicated to maximizing the performance and availability of the end-user experience with an interactive component of the SMI solution (for example, an SMI web site and/or associated web services that will be responsible for surfacing insights to end-users). I recommend the use of a PaaS solution for this tier to minimize the cost of hardware and system maintenance while benefiting from auto-scaling capabilities. For the data tier, I showcase the implementation of a MapReduce (Hadoop) Layer that can be used to process unstructured data and fed back into either a relational database management system (RDBMS) or a NoSQL solution depending on the needs of the solution, by using an Extract-Transform-Load (ETL) tool. On Amazon AWS cloud, for example, the Amazon EMR (Elastic MapReduce) feature will be used for this component. On the Microsoft Azure cloud, an equivalent solution that implements Apache Hadoop through the Azure HDInsight Service can be employed. Spark and the Azure Machine Learning platform are all viable options.

The interactive interface (web services) will communicate directly with the RDBMS or NoSQL data stores to read and write data. Ideally, a PaaS-based NoSQL solution like MongoDB is likely to deliver optimal performance in large data processing for unstructured data. Batch processing (ETL) tools can be employed to load data to the storage layer in the cloud IaaS implementation. The Python scripts can also live on the Storage layer of the cloud solution. Virtual machines (for example, EC2 instances on Amazon AWS) are used to drive the MapReduce processes. These instances can be scaled up and down to meet the requirements of the big data processing task at hand. The following illustrative case study explores how this logical architecture might implement the components described in the generic reference model.

5) Illustrative Case Study

We employ the collaborative filtering approach by utilizing movie preference data gleaned from Facebook.com, an online social networking (OSN) source for social media. I developed a Microsoft Azure cloud-hosted recommendations engine that is capable of deducing a similarity score between a given user and his Facebook friends. Using the Facebook Social Graph API [107], the preferences of friends with a high similarity score are used to drive the ranking engine. Facebook user preference information pertaining to movie genres and the actual number of “likes” recorded for movies by friends are used to deduce and rank movie suggestions, while taking into account the user’s own preferences and historical viewing behavior. The relation data was stored on Microsoft’s SQL Azure platform.

I simulated a futuristic scenario where the recommendations engine is leveraged at large-scale by multi-family households for recommending movie content by detecting and recognizing multiple users located in front of a smart television (TV) or a large screen tablet to watch a movie. A TV-mounted Microsoft Kinect for Windows sensor is leveraged to aid the simulated smart TV App prototype.

In this scenario, I sort out to employ social media influence intelligence retrieved from user similarity analysis implemented by using the *Euclidean Distance Score* approach [1] to find commonality between a given user and his Facebook friends. If a friend has a high similarity score, then the “likes” or movie preferences of the friend will be ranked higher on the list of recommendations served up by the movie recommendations engine. In addition, I explored the approach of implementing eigenvector centrality to determine friends who have more influence for a given user. Based on the influence score of a given friend (with high social influence), his or her movie preferences are, in turn, ranked higher.

I published the web application to the Microsoft Azure PaaS cloud platform using the proposed architectural approach in this literature to test the goodness-of-fit and performance of the template architecture when applied to a sample Social Profile Analysis SMI solution. In this implementation, a web interface using PaaS was used in the Front-End Tier of the logical architecture. The Azure CDN service was employed as a *Content Delivery Network* in the *Application Service* component of our model. SQL Azure was used for RDBMS solution. There were no ETL and MapReduce components involved with this implementation. However, the Azure Storage service was employed in the Storage Tier of our model.

6) Limitations

Additional case studies can be explored to confirm and extend the proposed reference architecture.

7) Results

In evaluating the efficacy of the architectural reference model, I used the following criteria:

- Goodness of Fit analysis of the reference architecture
- Scalability analysis
- Performance analysis.

a) Goodness of Fit Analysis of the Model

I assessed how the design and implementation of the several case studies matches the design of the generalized model [48]. I also compared previously published SMI solution implementations to our model to determine how these solutions could achieve some of the cross-cutting non-functional requirements identified here if they were to be implemented with a cloud-hosted solution that follows our model. In the nine use cases that I studied, the generic model was applicable. The model can be employed successfully (with some optional components based on the SMI solution requirements) to achieve high scalability, high performance, and high availability gains.

b) Scalability Analysis

The scalability of the architectural model is of critical importance. In my study, I noted that for horizontal scaling the EMR solution, I could easily adjust the number of nodes based on the workload in question to achieve a linear progression. In my on-premise database instance of SQL Server we were able to achieve vertical scaling by adding more memory and CPU cores to the database server hosting the database instance. However, in scaling out our SQL Azure cloud database I had to implement sharding – which allowed me to horizontally partition data across multiple databases.

c) C. Performance Analysis

While the cloud implementation inherently helps me achieve high performance, I was able to test the performance of SQL Azure queries for the same dataset against that of Google's BigQuery data store. I noted significant performance improvements when hosting structured data for the movie recommendations engine (378 million records) on BigQuery and running multiple queries simultaneously.

I also performed a *speedup analysis* (illustrated in Figure 46 below) by using the Amazon EMR solution for MapReduce processing in implementing the sentiment analysis solution.

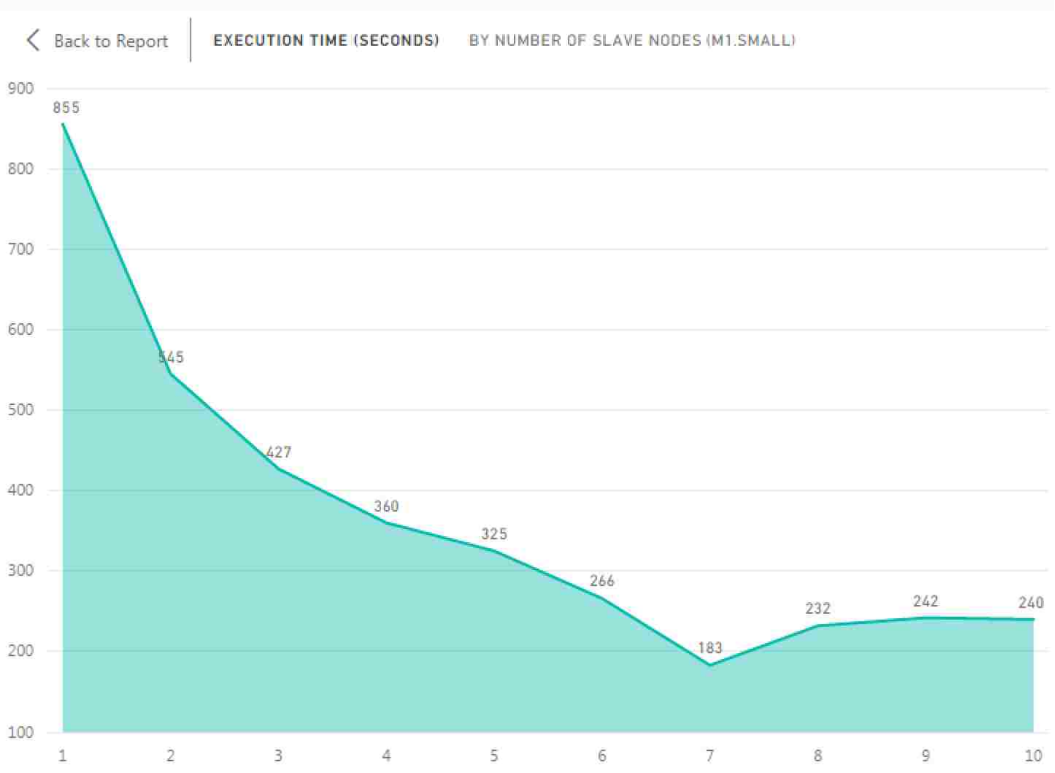


Fig 46. AWS EMR Cloud Platform – Speedup Analysis for sample SMI App [48]

In this case, the best execution time (of 183 seconds) is achieved by adding 7 "m1.small" virtual machine (VM) nodes to the cluster. Beyond the 7 nodes mark, subsequent addition of VMs led to minimal improvements (and in some cases, diminishing returns) while converging consistently below the 250 seconds mark for execution time. The execution times presented in the chart were recorded for the same MapReduce data processing workload.

8) Discussion

While the outburst of social media and big data tools have created numerous opportunities for social intelligence analysis and solutions, there is minimal guidance available today on the best way to build and sustain highly scalable, high availability and high performance SMI solutions. I shared a reference architecture to help guide researchers, solutions architects and developers in the implementation of cloud-based SMI and human-centered collective intelligence applications. Like most reference architectures, I am hopeful that the proposed strategy will promote re-use, minimize maintenance costs, and serves as a benchmark for SMI solution governance.

E. Summary

In this aim, I investigated some of the key challenges and approaches to using cloud computing services in support of building centralized knowledge-base driven artificially intelligent (KBAI) systems that leverage social media analytics and other data sources to drive human-centered collective intelligence solutions. I presented a couple of reference architectures and illustrative case studies to guide future implementations.

II. FUTURE DIRECTIONS AND CONCLUSIONS

A. Lessons Learned

In this dissertation, I highlighted some of the challenges, best practices and generalized reference models for designing solutions in a burgeoning area of research named human-centered collective intelligence (HCCI). Collective intelligence (CI) has several definitions in various contexts, however, I argue that the unifying theme hinges on the ability for a communal system to leverage multiple data sources and agents to solve a complex problem while utilizing machine learning techniques to arrive at an insightful and personalized solution. As more and more specialized agents and devices find their way into the smart homes and offices of the future, the concept of collective intelligence will remain a strong area of interest to help draw shared cognitive insights that help bridge the gap between machines and humans.

In my experience, HCCI solutions are more likely, than not, to share knowledge gleaned from multiple agents and data sources through a centralized intelligence store. That notwithstanding, HCCI solutions must consider several cross-cutting architectural quality attributes that are not limited to: *performance, security, privacy, trust, ethics, high-availability, automatic scalability, and usability*. These quality attributes must be considered throughout the solution implementation lifecycle. There are several evaluation methods involved with designing HCCI solutions.

The general theoretical literature on this holistic subject, and specifically in the context of multimodal human-centric solutions, is inconclusive on several fundamental questions involving design patterns and best practices. This exploratory study sought to investigate four key aims (pertaining to *emotion recognition*, *personalization*, *privacy*, and *cloud reliability*) in an effort to provide a conceptual reference architecture, named the ZOEI framework – for designing future HCCI solutions. The four key components of the ZOEI framework were investigated at length using two experiments each. The ZOEI framework is then explained using four relevant use case scenarios. While HCCI spans a vast gamut of applications, I examined some of the key challenges in each facet of the ZOEI framework across several application scenarios to prove the efficacy of the generalized reference model.

Some of my key takeaways from investigating various aspects of the ZOEI framework include the importance of implementing end user privacy preservation features in an HCCI application to inspire trust and, eventually, user adoption. It became evident that evaluation strategies for various machine learning tasks vary widely depending on the learning techniques employed. I have gained an appreciation for the importance of integrating multiple sources of end-user data in support of personalized human-machine interactions. As most people would imagine, warmhearted and personal experiences tend to make for better user experiences in lieu of the plain and one-size-fits-all alternatives [145].

I have learned throughout the course of this exploratory study, that the impact of emotion recognition in humans is far more extensive and yet pervasive than I previously estimated. I believe my understanding of the challenges involved with multimodal affect detection has enhanced my awareness of affect and other cognitive features in everyday human-to-human communications and, consequently, enhanced my own understanding of life.

B. Contribution of Dissertation

This dissertation proposes *human-centered collective intelligence* (HCCI) as an emerging area of research. Through several experiments and exploratory studies, I proposed the ZOEI framework as a reference architecture for designing HCCI solutions. I also showcased a number of challenges, solutions, and best practices for architecting various HCCI solutions. I am not (as of the time of publication) aware of any comprehensive framework that provides detailed insights into building KBAI systems in support of applications that seek to draw on social media intelligence and cognitive (or affective) intelligence to drive content personalization.

In addition, I proposed several reference architectures for modeling privacy preservation and cloud reliability solutions in HCCI scenarios. By facilitating a unique community of industry practitioners and researchers with this similarly distinctive body of knowledge, I hope to inspire the use of HCCI strategies as an evolutionary paradigm in human-centric application design.

C.Broader Impact

Oyama, Chang and Mitra [146] made an argument for the budding rise in context aware human-centric systems in smart home scenarios. I agree with the vision that it is only a matter of time before human-centered solution design takes center stage in software solution design as we know it today. Even so, as various sensory devices and agents emerge in the smart environments of the future, it will become more and more imperative that we establish a viable pattern for implementing cognitive solutions that will seamlessly safeguard end-user privacy but yet exalt personalization in human-machine interactions. At the intersection of those waves in transformation, I expect the ZOEI framework to serve as a blueprint for designing and implementing several HCCI applications to solve several complex problems that we face as humans. Some potential applications of this framework include, but are not limited to, electronic healthcare scenarios, entertainment scenarios, market research scenarios, and many more.

D. Conclusion

When it comes to multimodal cognitive feature recognition, I was able to experiment with and unearth several challenges, approaches, and evaluation techniques for affect detection through sentiment analysis of verbal (speech) data and emotion recognition through facial expression analysis (ERFE) as non-verbal cues in cloud hosted application solutions. I also investigated the best practices and challenges associated with affect-driven personalization using the state-of-the-art machine learning techniques including reinforcement learning and collaborative filtering-based recommender systems.

Correspondingly, I investigated innate privacy preservation challenges and techniques in affect-driven personalization scenarios, specifically, as well as related issues in IoT and HCCI applications in general. Through the exploration of cross-cutting infrastructure challenges with supporting knowledge-based AI solutions – as HCCI necessitates, I investigated some of the key concerns with cloud reliability in HCCI applications including multi-cloud portability and business continuity, and offered a reference architecture for selecting various cloud delivery models in support of HCCI scenarios.

A few decades ago, Simon [147] underscored the fact that broad-spectrum theories on thinking and problem solving must include the influence of affect. Several years into working towards humanizing machines, computer scientists are involved with pushing the limits to build intelligent systems which recognize, show and attempt to “have” emotions [62]. I share Picard [62] and Simon’s [147] sentiments regarding the importance of emotion analytics in intelligent systems. I, however, hold the opinion that the future of complex problem solving and artificial reasoning pivots on the amalgamation of knowledge from multiple data sources and devices. Hence, the reason why I focused on affect as a key aspect of the broader cognitive intelligence space. Future research can explore other types of cognitive intelligence features to extend the ZOEI framework.

Furthermore, facial expression, voice inflection, and posture are known to be the principal means for communicating human emotions [62]. This study examined sentiment analysis in spoken language understanding and facial expression analysis as key modalities for emotion recognition in investigating the proposed framework. Respiration patterns, heart rate, blood pressure, electro-dermal response, and temperature are all viable sources for emotion detection though their associated measuring devices often require physical human contact. Future research can explore the use of voice intonation, gestures, pupillary dilation, and posture analysis as additional sources for pervasive detection of affective signals in the multimodal cognitive feature recognition aspect of the ZOEI framework.

Emotions are known to sway our judgment about otherwise dispassionate actions. Additionally, emotion influences memory retrieval [62]. For example, a positive emotional state makes it relatively easier to remember positive things and vice versa. Future studies can investigate the application of affect-driven personalization on human memory recollection. Based on the success of this phenomenon, there are bound to be interesting application scenarios which can determine one's emotional state and subsequently present an appropriate content or ad to a human in an effort to inspire long-term memory recall of the presented content or product. Invariably, I am confident that my contribution in this area of research will inspire a new breed of cognitive HCCI application scenarios while serving as a blueprint for their design.

BIBLIOGRAPHY

[1] T. Segaran, “Programming Collective Intelligence”, *O’Rielly*, pp. 2 - 52, 2007.

[2] G. Clifford, D. Clifton, “Wireless Technology in Disease Management and Medicine,” *Ann. Rev. Medicine*, vol. 63, pp. 479–492, 2012.

[3] S. Lahlou, M. Langheinrich, C. Rocker, “Privacy and Trust Issues with Invisible Computers,” *Communications of the ACM*, vol. 48, no. 3, pp.59-60, March 2005.

[4] A. Joinson, U. Reips, T. Buchanan, C. B. P. Schofield, “Privacy, Trust, and Self-Disclosure Online,” *Human-Computer Interaction*, vol. 25, pp. 1-24, 2010.

[5] A. Sirageldin, B. Baharudin, L. T. Jung, "Hybrid scheme for trust management in pervasive computing," *Information Retrieval & Knowledge Management (CAMP), 2012 International Conference on*, pp. 45-49, March 2012.

[6] H. Lin, J. Shao, C. Zhang, Y. Fang, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 6, pp. 985-997, June 2013.

[7] N. Liampotis, I. Roussaki, E. Papadopoulou, Y. Abu-Shaaban, M. H. Williams, N. K. Taylor, S. M. McBurney, K. Dolinar, "A Privacy Framework for Personal Self-Improving Smart Spaces," *Computational Science and Engineering, CSE '09. International Conference on*, vol. 3, pp. 444-449, 29-31, 2009.

[8] K. Maekawa, Y. Okabe, "An Enhanced Location Privacy Framework with Mobility Using Host Identity Protocol," *Applications and the Internet, SAINT '09. Ninth Annual International Symposium on*, pp. 23-29, 20-24, 2009.

[9] G. O. Yee, “A Privacy Controller Approach for Privacy Protection in Web Services,” *In Proceedings of the ACM Workshop on Secure Web Services*, pages 44-51, 2007.

[10] V. Singh, A. Gupta, “From artificial to collective intelligence: perspectives and implications,” *5th International Symposium on Applied Computational Intelligence and Informatics*, pp. 545-549, May 2009.

[11] S. Alag, *Collective Intelligence in Action*, pp. 274 – 306, 2009, Manning.

[12] M. K. Lee, K. P. Tang, J. Forlizzi, S. Kiesler, "Understanding users! Perception of privacy in human-robot interaction," *Human-Robot Interaction (HRI), 2011 6th ACM/IEEE International Conference*, pp.181-182, March 2011.

[13] G. Pallapa, N. Roy, S. K. Das, "A scheme for quantizing privacy in context-aware ubiquitous computing," *Intelligent Environments, 2008 IET 4th International Conference*, pp.1-8, July 2008.

[14] X. Jiang, J. A. Landay, "Modeling privacy control in context-aware systems," *Pervasive Computing, IEEE*, vol.1, no.3, pp.59-63, July-Sept. 2002.

[15] J. Schreck, “Security and privacy in user modeling,” *Springer*, vol. 2, 2003.

[16] M. Peleg, B. Dizza, D. Dov, D. Yaron, "Situation-Based Access Control: privacy management via modeling of patient data access scenarios." *Journal of Biomedical Informatic,* vol. 41, no. 6, pp. 1028-1040, 2008.

[17] H. Lin, J. Shao, C. Zhang, Y. Fang, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 6, pp. 985-997, June 2013.

[18] N. Liampotis, I. Roussaki, E. Papadopoulou, Y. Abu-Shaaban, M. H. Williams, N. K. Taylor, S. M. McBurney, K. Dolinar, "A Privacy Framework for Personal Self-Improving Smart Spaces," *Computational Science and Engineering, CSE '09. International Conference on*, vol. 3, pp. 444-449, 29-31, 2009.

[19] American Psychology Association, "Protecting your privacy: Understanding confidentiality", http://www.apa.org/helpcenter/confidentiality.aspx

[20] C. Lee, Y. Cha, T. Kuc, "Implementation of dialogue system for intelligent service robots," *Control, Automation and Systems, 2008. ICCAS 2008. International Conference on, Seoul*, pp. 2038-2042 (2008)

[21] Oinas-Kukkonen, H., Harjumaa, M., "Persuasive Systems Design: Key Issues, Process Model, and System Features," *Communications of the Association for Information Systems*, vol. 24, no. 28 (2009)

[22] Nakano, M. et al., "A two-layer model for behavior and dialogue planning in conversational service robots," *Intelligent Robots and Systems, 2005. (IROS 2005). IEEE/RSJ International Conference on,* 2005, pp. 3329-3335, (2005)

[23] I. D. Addo, S. I. Ahamed, W. C. Chu, "Toward Collective Intelligence for Fighting Obesity," *COMPSAC*, pp. 690-695, (2013)

[24] C. Breazeal, "Designing Sociable Robots," *MIT Press*, (2004)

[25] B. Meerbeck, M. Saerbec., "Communication robots: Application challenges of human-robot interaction," Advances in Interaction Studies – New Frontiers in Human-Robot Interaction, pp. 257-277, (2011)

[26] N. Hagita, K. Kogure, K. Mase, Y. Sumi, "Collaborative Capturing of Experiences with Ubiquitous Sensors and Communication Robots," *Proceedings of the 2003 IEEE International Conference on Robotics and Automation*, pp. 4166-4171, 2003.

[27] T. Kanda, M. Shiomi, Z. Miyashita, H. Ishiguro, N. Hagita, "An Affective Guide Robot in a Shopping Mall," *Human-Robot Interaction (HRI), 2009 4th ACM/IEEE International Conference on*, pp.173-180, March 2009.

[28] K. Wada, T. Shibata, T. Saito, K. Tanie, "Effects of Robot-Assisted Activity for Elderly People and Nurses at a Day Service Center," *Proceedings of the IEEE, vol.* 92, no. 11, pp. 1780-1788, 2004.

[29] T. Erl, Z. Mahmood, R. Puttini, "Cloud Computing Concepts, Technology, Architecture," *Prentice Hall*, pp. 110-160, 2013.

[30] P. Mell, T. Grance, "A NIST definition of Cloud Computing," *National Institute of Standards and Technology, NIST*, 2009.

[31] P. Mell, T. Grance, "Effectively using the Cloud Computing Paradigm," *Gaithersburg, MD: NIST Information Technology, Laboratory,* 2009.

[32] M. McKeown, H. Kommalapati, J. Roth, "Disaster Recovery and High Availability for Azure Applications", *Microsoft Azure – MSDN,* April 2014. Retrieved from http://msdn.microsoft.com/library/azure/dn251004.aspx.

[33] I. Saha, D. Mukhopadhyay, S. Banerjee, “Designing Reliable Architecture for State-ful Fault Tolerance,” In Proceedings of *Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06)*, pp. 545-551, 2006.

[34] I. Saha, D. Mukhopadhyay, “A Distributed Algorithm of Fault Recovery for Stateful Failover,” *Theory and Applications of Models of Computation – TAMC, Lecture Notes in Computer Science: Springer*, vol. 4484, pp. 738-749, 2007.

[35] C. Chi-Chung, Y. Man-Ching, A. Yip, "Dynamic DNS for load balancing," *Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference,* pp. 962, 965, 19-22, May 2003.

[36] W. Itani, A. Kayssim, A. Chehab, “Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures,” *DASC '09 Proceedings of the 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp. 711-716, 2009.

[37] G. Zhao, Z. Li, W. Li, H. Zhang, Y. Tang, "Privacy Enhancing Framework on PaaS," *Cloud and Service Computing (CSC), 2012 International Conference on*, pp.131-137, 22-24, Nov. 2012.

[38] I. D. Addo, S. I. Ahamed, “Applying affective feedback to reinforcement learning in ZOEI, a comic humanoid robot,” *RO-MAN,* pp. 423-428, 2014.

[39] National Institute of Standards and Technology, “NIST Cloud Computing Standards Roadmap,” *NIST - US Department of Commerce,* 2013.

[40] I. Addo, S. Ahamed, S. Yau, B. Buduru, “A Reference Software Architecture for Improving Security and Privacy in Cloud-Enabled IoT Applications,” *MS 2014*, 2014.

[41] D. Pallmann, “Hidden Costs in the Cloud, Part 2: Windows Azure Bandwidth Charges,” 2010. Retrieved from http://davidpallmann.blogspot.com/2010/08/hidden-costs-in-cloud-part-2-windows.html.

[42] E. Vergaro, V. Squeri, G. Brichetto, M. Casadio, P. Marasso, C. Solaro, V. Sanguineti, “Adaptive robot training for the treatment of incoordination in Multiple Sclerosis,” *Journal of Neuroengineering and Rehabilitation*, pp.737, 2010.

[43] E. Kim, E. Newland, R. Paul, B. Scassellati, “Robotic tools for prosodic training for children with ASD: A case study,” *International Meeting for Autism Research (IMFAR)*, 2008.

[44] D. S. Ludwig, "Weight loss strategies for adolescents – A 14-year-old struggling to lose weight," *Journal of the American Medical Association (JAMA)*, vol. 307, no. 5, pp. 498-508, February, 2012.

[45] C. L Lisetti, U. Yasavur, U. Visser, U., N. Rishe, "Toward conducting motivational interviewing with an on-demand clinician avatar for tailored health behavior change interventions," *Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2011 5th International Conference on*, pp.246-249, May 2011.

[46] I. D. Addo, S. I. Ahamed, S. S. Yau, A. Buduru, “Reference Architectures for Privacy Preservation in Cloud-Based IoT Applications,” *International Journal of Services Computing*, vol. 2, no. 4, pp. 65-78, 2015.

[47] I. D. Addo, J. Yang, S. I. Ahamed, “SPTP: A Trust Management Protocol for Online and Ubiquitous Systems,” *COMPSAC*, pp. 590-595, 2014.

[48] I. D. Addo, D. Do, R. Ge, S. I. Ahamed, “A Reference Architecture for Social Media Intelligence Applications in the Cloud,” *COMPSAC,* 2015.

[49] G. M. T. Ahsan, I. D. Addo, S. I. Ahamed, D. Petereit, S. Kanekar, L. Burhansstipanov, L. Krebs, “Toward an mHealth Intervention for Smoking Cessation,” *COMPSAC Workshops,* pp. 345-350, 2013.

[50] G. M. T. Ahsan, D. Williams, I. D. Addo, S. I. Ahamed, D. Petereit, L. Burhansstipanov, L. U. Krebs, M. Dignan, “A Mobile Survey Tool for Smoking Dependency among Native Americans,” *ICOST*, pp. 213-218, 2014.

[51] F. Rahman, I. D. Addo, S. I. Ahamed, “PriSN: a privacy protection framework for healthcare social networking sites,” *RACS*, pp. 66-71, 2014.

[52] D. Williams, I. Addo, G. M. T. Ahsan, F. Rahman, C. Tamma, S. I. Ahamed, "Privacy in Healthcare," *In Privacy in a Digital, Networked World, Springer International Publishing*, pp. 85-110, 2015.

[53] I. D. Addo, S. I. Ahamed, W. C. Chu, “Modeling Confidentiality in Persuasive Robots,” *Inclusive Smart Cities and Digital Health – ICOST,* pp. 436-442, May 2016.

[54] I. D. Addo, S. I. Ahamed, “A Reference Architecture for High-Availability Automatic Failover between PaaS Cloud Providers,” *Trustworthy Systems and their Applications (TSA)*, pp. 14-21, 2014.

[55] A. Go, R. Bhayani, L. Huang, “*Twitter Sentiment Classification using Distant Supervision*,” *CS224N Project Report, Stanford, help.sentiment140.com*, vol. 1, no. 12, 2009.

[56] S. Marsland, “Machine Learning an Algorithmic Perspective,” *CRC Press*, 2009.

[57] R. S. Sutton, A. G. Barto, “Reinforcement Learning: An Introduction,” *MIT Press*, 1998.

[58] I. D. Addo, P. Madiraju, S. I. Ahamed, W. C. Chu, “Privacy Preservation in Affect-Driven Personalization,” *COMPSACW* 2016: In Press.

[59] P. G. Leon, A. Rao, F. Schaub, A. Marsh, L. F. Cranor, N. Sadeh, "Privacy and Behavioral Advertising: Towards Meeting Users’ Preferences." *In Symposium on Usable Privacy and Security (SOUPS).* 2015.

[60] A. Sauppe, B. Mutlu, “Design Patterns for Exploring and Prototyping Human-Robot Interactions,” *Proceedings of Human Factors in Computing* (CHI 2014), 2014.

[61] Q. He, A. Anton, “A Framework for Modeling Privacy Requirements in Role Engineering,” *In the Proceedings of REFSQ,* 2003.

[62] R. W. Picard, “Affective Computing,” *MIT Press,* 2000.

[63] L. N. Foner, "A security architecture for multi-agent matchmaking," *In Proceeding of Second International Conference on Multi-Agent System*, pp. 80-86. 1996.

[64] C. Breazeal, “Sociable Machines: Expressive Social Exchange between Humans and Robots,” *Massachusetts Institute of Technology*, 2000.

[65] J. Zhang; Y. Wang, V. Varadharajan, "Mobile Agent and Web Service Integration Security Architecture," *Service-Oriented Computing and Applications, 2007. SOCA '07. IEEE International Conference on*, pp.172-179, 2007.

[66] X. Niu, J. Ma, D. Zhang, “A Survey of Contextual Advertising,” *2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery*, pp. 505-509, 2009.

[67] R. Heath, A. Nairn, “Measuring Affective Advertising: Implications of Low Attention Processing on Recall,” *University of Bath School of Management Working Paper Series*, 2005.

[68] N. Hristova, G.M.P. O'Hare, "Ad-me: Wireless Advertising Adapted to the User Location, Device and Emotions," *Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004.

[69] Z. Cheng, B. Gao, T. Liu, "Actively predicting diverse search intent from user browsing behavior," *ACM, In Proceedings of the 19th WWW Conference*, pp. 221-230, 2010.

[70] I. Saha, D. Mukhopadhyay, "A Distributed Algorithm of Fault Recovery for Stateful Failover," *Theory and Applications of Models of Computation – TAMC, Lecture Notes in Computer Science: Springer*, vol. 4484, pp. 738-749, 2007.

[71] J. Li, P. Zhang, Y. Cao, P. Liu, L. Guo, "Efficient Behavior Targeting Using SVM Ensemble Indexing", 2012 IEEE 12th Internetional Conference on Data Mining, pp. 409-418, 2012.

[72] C. D. Fryar, M. D. Carroll, C. Ogden, "Prevalence of obesity among children and adolescents: United States, Trends 1963–1965 through 2009–2010," *Centers for Disease Control and Prevention (CDC) - NCHS Health E-Stat.*, September, 2012.

[73] Y. Wang, M. A. Beydoun, "The obesity epidemic in the United States—Gender, Age, Socioeconomic, Racial/Ethnic, and Geographic Characteristics: A systematic review and meta-regression analysis," *Epidemiologic Reviews – Johns Hopkins Bloomberg School of Public Health,* vol. 29, 2007.

[74] A. Rabbitt, I. Coyne, "Childhood obesity: nurses' role in addressing the epidemic," *British Journal of Nursing*, vol. 21, no. 12, July 2012.

[75] D. B. Allison, K. R. Fontaine, J. E. Manson, J. Stevens, T. B. VanItallie, "Annual deaths attributable to obesity in the United States," *Journal of the American Medical Association (JAMA)*, vol. 282, no. 16, pp. 498-508, October, 1999.

[76] A. Thomaz, C. Breazeal, "Robot learning via socially guided exploration," *Development and Learning, 2007; ICDL 2007, IEEE 6th International Conference on*, pp.82-87, 11-13 July 2007.

[77] C. D. Kidd, C. Breazeal, "Robots at Home: Understanding long-term human-robot interaction," *Intelligent Robots and Systems, 2008; IROS 2008 IEEE/RSJ International Conference,* pp. 3230-3235, 22-26, Sept. 2008.

[78] C. Frith, "Role of facial expressions in social interactions," *Philosophical Transactions of The Royal Society - Biological Sciences*, vol. 364, no. 1535, pp. 3453-3458, December 2009.

[79] G. Tur, R. De Mori, "Spoken Language Understanding - systems for extracting semantic information from speech," *John Wiley and Sons*, 2011.

[80] A. M. Bidgoli, "A language independent text segmentation technique based on Naive Bayes classifier," *Signal and Image Processing (ICSIP), 2010 International Conference on,* pp. 11-16, 2010.

[81] F. Peng, X. Huang, D. Schuurmans, S. Wang, "Text classification in Asian languages without word segmentation," *AsianIR '03 Proceedings of the sixth international workshop on Information retrieval with Asian languages*, vol. 11, pp. 41-48, 2003.

[82] J. Perkins, "Python text processing with NLTK 2.0 cookbook," *Packt Publishing*, November 2010.

[83] K. M. Flegal, M. D. Carroll, B. K. Kit, C. L. Ogden, "Prevalence of obesity and trends in the distribution of body mass index among US adults," *Journal of the American Medical Association (JAMA)*, vol. 307, no. 5, pp. 491-497, 2012.

[84] Y. Wang, K. McPherson, T. Marsh, S. Gortmaker, M. Brown, "Health and economic burden of the projected obesity trends in the USA and the UK," *Lancet*, vol. 378, no. 9793, pp. 815-825, 2011.

[85] G. R. Lustria, J. Cortese, S. M. Noar, “Computer-tailored health interventions delivered over the Web: review and analysis of key components.” *Patient Education and Counseling*, vol. 74, no. 2, pp. 156–173, 2009.

[86] S. M. Berg-Smith, V. J. Stevens, K. M. Brown, L. Van Horn, N. Gernhofer, E. Peters, R. Greenberg, L. Snetselaar, L. Ahrens, K. Smith, “A brief motivational intervention to improve dietary adherence in adolescents,” *Health Education Research*, vol. 14, no. 3, pp. 399-410, 1999.

[87] N. Hakim, A. Keys, “Architecting a Machine Learning System for Risk,” *AirBnB*, June 2014, Retrieved on 08/20/2015: http://nerds.airbnb.com/architecting-machine-learning-system-risk/

[88] B. Gianluca, “Machine Learning Strategies for Time Series Prediction,” *Machine Learning Summer School (Hammamet, 2013),* 2013. Retrieved on 08/20/2015: http://www.ulb.ac.be/di/map/gbonte/ftp/time_ser.pdf

[89] C. L Lisetti, U. Yasavur, U. Visser, U., N. Rishe, “Toward conducting motivational interviewing with an on-demand clinician avatar for tailored health behavior change interventions,” *Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2011 5th International Conference on*, pp.246-249, May 2011.

[90] R. Herbrich, T. Graepel, C. Campbell, “Bayes point machines,” *The Journal of Machine Learning Research*, *vol. 1,* pp.245-279, 2001.

[91] C. J. Burges, “A tutorial on support vector machines for pattern recognition,” *Data mining and knowledge discovery*, *vol. 2, no. 2, pp.121-167,* 1998.

[92] J. A. Anderson, “An introduction to neural networks,” *MIT press*, 1995.

[93] K. Weinberger, A. Dasgupta, J. Langford, A. Smola, J. Attenberg. "Feature hashing for large scale multitask learning," In *Proceedings of the 26th Annual International Conference on Machine Learning*, pp. 1113-1120, ACM, 2009.

[94] S. Dustdar, H. Gall, "Architectural concerns in distributed and mobile collaborative systems," *Journal of Systems Architecture, vol. 49, no. 10-11*, pp. 457-473, 2003.

[95] L. Bass, P. Clements, R. Kazman, "Software architecture in practice," *Addison-Wesley Longman Publishing Co., Inc., Boston, MA*, 1998.

[96] C. Breazeal, “Toward sociable robots,” *Robotics and autonomous systems*, vol. *42*, no. 3, pp.167-175, 2003.

[97] C. Breazeal, “Jibo”, *https://www.jibo.com/,* n.d.

[98] AT&T Laboratories, *The Database of Faces*, http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html, n.d.

[99] OpenCV, *Cascade Classifier*, http://docs.opencv.org/2.4/doc/tutorials/objdetect/cascade_classifier/cascade_classifier.html#cascade-classifier, n.d.

[100] P. Viola, M. Jones. "Rapid object detection using a boosted cascade of simple features," In *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on*, vol. 1, pp. I-511. IEEE, 2001.

[101] S. Russell, P. Norvig, “Artificial Intelligence – A Modern Approach," *Prentice-Hall, Englewood Cliffs, NJ*, 1995.

[102] S. Marsland, “Machine Learning an Algorithmic Perspective,” *CRC Press*, 2009.

[103] Sprague, Nathan, and Dana Ballard. "Multiple-goal reinforcement learning with modular sarsa (0)." In *IJCAI*, pp. 1445-1447. 2003.

[104] T. Graepel, R. Herbrich, J. Gold. "Learning to fight," In *Proceedings of the International Conference on Computer Games: Artificial Intelligence, Design and Education*, pp. 193-200. 2004.

[105] R. S. Sutton, A. G. Barto, "*Reinforcement Learning: An Introduction*," *MIT Press*, 1998.

[106] IMDB, "Internet Movie Database," *http://www.imdb.com*, n.d.

[107] Facebook, "Using Graph API," *https://developers.facebook.com/docs/graph-api*, n.d.

[108] YouTube, "YouTube API," *https://developers.google.com/youtube/iframe_api_reference*, n.d.

[109] D. Goldberg, D. Nichols, B. Oki, D. Terry. "Using collaborative filtering to weave an information tapestry." *Communications of the ACM*, vol. 35, no. 12, pp. 61-70, 1992.

[110] S. Dooms, T. D. Pessemier, L. Martens. "MovieTweetings: a Movie Rating Dataset Collected From Twitter," *Workshop on Crowdsourcing and Human Computation for Recommender Systems, CrowdRec.* RecSys 2013.

[111] A. E., Hassan, R. C. Holt, "A Reference Architecture for Web Servers," *Reverse Engineering, 2000. Proceedings. Seventh Working Conference*, pp.150-159, 2000.

[112] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, "Proposed Embedded Security Framework for Internet of Things (IoT)," *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference*, pp. 1-5, 2011.

[113] J. M. Seigneur, C. D. Jensen. "Trading Privacy for Trust," *Trust Management, Springer Berlin Heidelberg,* pp. 93-107, 2004.

[114] D. Solove, "Understanding Privacy," *Harvard University Press*, 2008.

[115] W. Itani, A. Kayssim, A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," *DASC '09 Proceedings of the 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp. 711-716, 2009.

[116] W. Lou, K. Ren, "Privacy-enhanced, Attack-resilient Access Control in Pervasive Computing Environments with Optional Context Authentication Capability," *Mobile Networks & Applications*, vol. 12, no. 1, pp. 79, 2007.

[117] Ponemon Institute, Microsoft, "Achieving Data Privacy in the Cloud: United States," *Microsoft – Trustworthy Computing: Cloud Privacy*, pp. 1-16, 2012.

[118] A. Behl, K. Behl, "An Analysis of Cloud Computing Security Issues," *Information and Communication Technologies (WICT), 2012 World Congress on*, pp. 109-114, 2012.

[119] Yale University, "Health Insurance Portability and Accountability Act (HIPAA) Policies, Updates and Reminders," *Yale University*, 2011, Retrieved from http://hipaa.yale.edu/guidance/policy.htm.

[120] P. Mvelase, N. Dlodlo, Q. Williams, M. Adigun, "Custom-made Cloud Enterprise Architecture for Small and Micro Enterprises," 589-601, *Grid and Cloud Computing*, vol. 2, 2012.

[121] J. Zhang; Y. Wang, V. Varadharajan, "Mobile Agent and Web Service Integration Security Architecture," *Service-Oriented Computing and Applications, 2007. SOCA '07. IEEE International Conference on*, pp.172-179, 2007.

[122] L. Xu, C. Jiang, J. Wang, J. Yuan, Y. Ren, "Information Security in Big Data: Privacy and Data Mining," in *Access, IEEE*, vol. 2, pp.1149-1176, 2014.

[123] W. Xu, S. S. Cheung, N. Soares, "Affect-preserving privacy protection of video," *in Image Processing (ICIP), 2015 IEEE International Conference on*, pp.158-162, 27-30 Sept. 2015.

[124] Y. Nakashima, T. Koyama, N. Yokoya, N. Babaguchi, "Facial expression preserving privacy protection using image melding," *in Multimedia and Expo (ICME), 2015 IEEE International Conference on*, pp.1-6, July 3 2015.

[125] A. Dawel, R. O'Kearney, E. McKone, R. Palermo, "Not just fear and sadness: Meta-analytic evidence of pervasive emotion recognition deficits for facial and vocal expressions in psychopathy." *Neuroscience & Biobehavioral Reviews,* vol. 36, no. 10, pp. 2288-2304, 2012.

[126] M. Yamada, J. Decety, "Unconscious affective processing and empathy: an investigation of subliminal priming on the detection of painful facial expressions." *Pain*, vol. 143, no. 1 pp. 71-75, 2009.

[127] P. G. Leon, A. Rao, F. Schaub, A. Marsh, L. F. Cranor, N. Sadeh, "Privacy and Behavioral Advertising: Towards Meeting Users' Preferences." *In Symposium on Usable Privacy and Security (SOUPS).* 2015.

[128] J. Henstridge, "GIMP Python Documentation," *Gimp*, https://www.gimp.org/docs/python/, n.d.

[129] S. Pearson, "Privacy, Security and Trust in Cloud Computing," *HP Laboratories*, pp. 1-58, June 2012, Retrieved from http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf.

[130] S. Pearson, A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," *In: Proc. CloudCom,* 2009.

[131] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, G. J. Sussman, "Information Accountability," *Communications of ACM*, vol. 51, no. 6, pp. 87, June 2008.

[132] Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule, "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research." *Washington (DC), National Academies Press (US),* 2009, Retrieved from http://www.ncbi.nlm.nih.gov/books/NBK9579/.

[133] R. Wenning, W3C, "Platform for Privacy Preferences Project," *P3P Public Overview*, October 2007, Retrieved from http://www.w3.org/P3P/.

[134] L. Jamtgaard, IEF, W3C, "The P3P Implementation Guide," *P3P Toolbox*, December 2005, Retrieved from http://www.p3ptoolbox.org/guide.

[135] J. R Raphael, "The Worst Cloud Outages of 2013," *InfoWorld*, December 2013. Retrieved from http://www.infoworld.com/slideshow/133109/the-worst-cloud -outages-of-2013-part-2-232912.

[136] G. DeCandia, D. Hastorun, M. Jampani, G. Kakulapati, A. Lakshman, A. Pilchin, S. Sivasubramanian, P. Vosshall, W. Vogels, "Dynamo: Amazon's Highly Available Key-value Store," *SOSP*, pp. 205-220, 2007.

[137] Google, "Apps Status Dashboard," *Google Apps*, n. d., Retrieved from http://www.google.com/appsstatus#hl=en&v=status.

[138] P. Mvelase, N. Dlodlo, Q. Williams, M. Adigun, "Custom-made Cloud Enterprise Architecture for Small and Micro Enterprises," 589-601, *Grid and Cloud Computing*, vol. 2, 2012.

[139] C. Weinhardt, A. Anandasivam, B. Blau, J. Stober, "Business Models in the Service World," IEEE Computer, vol. 11, no. 2, pp. 28-33, 2009.

[140] A. E., Hassan, R. C. Holt, "A Reference Architecture for Web Servers," *Reverse Engineering, 2000. Proceedings. Seventh Working Conference*, pp.150-159, 2000.

[141] M. R. Morris, J. Teevan, K. Panovich, "A Comparison of Information Seeking Using Search Engines and Social Networks," *ICWSM*, pp. 23-26, 2010.

[142] T. White, "Hadoop: The Definitive Guide," O'Reilly, 2012.

[143] Wikibon, "Big Data Statistics," *Wikibon*, 2012.

[144] J. Dean, S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," *OSDI*, 2004.

[145] L. Gevelber, "Marketing in the Driver's Seat: Using Analytics to Create Customer Value," *Harvard Business Review*, 2016.

[146] K. Oyama, C. K. Chang, S. Mitra. "Inference of Human Intentions in Smart Home Environments," *International Journal of Robotics Applications and Technologies, IGI Global,* vol. 1, no. 2, pp. 26-42, July-December 2013.

[147] H. A. Simon, "Motivational and emotional controls of cognition," In *Models of Thought,* Yale University Press, New Haven, pp. 29-38, 1979.