Engineering Science and Technology, an International Journal 21 (2018) 574–588

HOSTED BY

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: www.elsevier.com/locate/jestch

Review

Identity and access management in cloud environment: Mechanisms and challenges

I. Indu [a], P.M. Rubesh Anand [a,*], Vidhyacharan Bhaskar [b]

[a] Department of Electronics and Communication Engineering, Hindustan University, Chennai 603103, India
[b] Department of Electrical and Computer Engineering, San Francisco State University, 1600 Holloway Avenue, San Francisco, CA 94132, USA

ARTICLE INFO

Article history:
Received 1 December 2017
Revised 22 March 2018
Accepted 14 May 2018
Available online 23 May 2018

Keywords:
Access management
Authentication
Authorization
Cloud computing
Security
Web services

ABSTRACT

Cloud computing is a complex system with combination of diverse networked devices that supports demanded services. The architecture of cloud computing consists of different kinds of configurable distributed systems with a wide variety of connectivity and usage. The organizations are adapting to cloud networks at a rapid pace due to the benefits like cost-effectiveness, scalability, reliability and flexibility. Though the primary merits of cloud computing are promising facts, cloud networks are vulnerable to various kinds of network attacks and privacy issues. The features like multi tenancy and the third party managed infrastructure in cloud environment necessitates the requirement of identity and access management mechanism. The problems involved in secure access to cloud resources have been addressed by many academicians and industry personnel. In this paper, the issues related to authentication, access management, security and services in cloud environment are surveyed along with the techniques proposed to overcome the same. A detailed comparative study of the existing techniques in the perspective of cloud service providers and cloud users that include identity and access management, security issues and services in the cloud environment are highlighted.

Contents

* Corresponding author.
E-mail address: rubesh.anand@gmail.com (P.M.R. Anand).
Peer review under responsibility of Karabuk University.

https://doi.org/10.1016/j.jestch.2018.05.010
2215-0986/

1. Introduction

Cloud computing is a combination of different configurable computing resources like networks, servers, storages, services, applications that help in providing convenient and on-demand access to the cloud users [1]. Cloud computing is largely mentioned by people and is currently used in many commercial fields. Cloud service providers (CSPs) are responsible for identity and other kinds of management in cloud environment. However, a large number of data leakage incidents are caused due to the vulnerabilities in identity management systems [2]. Identity and access management (IAM) in cloud environment is a crucial concern for the acceptance of cloud-based services. Presently, the mechanism of identity management is mainly CSP-centered, which hardly meets the requirement of users' flexible and fine-grained access control policy.

The cloud environment is generally classified as Private Cloud, Public Cloud and Hybrid/Federated Clouds. A private cloud is designed and dedicated to the needs of a specific organization. In a public cloud environment, infrastructure support to multiple organizations is facilitated and managed by third party provider. Public cloud model is also known as multi-tenant environment which shares the resources among the organizations to bring down the overall service cost. Hybrid or Federated cloud infrastructure is a mix of on-premises, private and public cloud services. Another concept in cloud infrastructure is multi-provider clouds which is an environment that relies on multiple clouds providers and divides the work load among the cloud environment. There are also different cloud environments which is specifically designed to support the service like Internet of Things (IoT) cloud services which are specifically designed to handle and analyse the data from IoT devices and mobile cloud services which uses cloud computing to deliver applications to mobile devices.

Cloud computing is commonly divided into three primary cloud service models, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Cloud is based on service-oriented architecture which has the capability of providing Database-as-a-service (DbaaS), Identity-as-a-service (IDaaS) and Anything-as-a-Service (XaaS) [3]. Cloud computing provides a better way of handling resources in both industry and academia. Cloud system is vibrant in nature by considering numerous users, devices, networks, organizations, and resources that are frequently connected and disconnected to the system. The best option for the cloud service model that has to be implemented is determined through a number of factors. The important factors that are to be considered are flexibility, scalability, interoperability, and control of service [4]. Cloud computing requires extensive authentication and authorization mechanism to secure its data and resources due to the complexity of usage. Lack of efficient mechanism creates multiple challenges in cloud environment which include identity management, risk management, trust management, compliance, data security, privacy, transparency, and data leakage [5]. Another facet of cloud systems is complexity and their associated security challenges. The loss of control and transparency issues are also created while storing and processing user information by Cloud Service Providers (CSPs), or outside the organizational boundaries. Due to these distinctive security challenges, the cloud environment adoption is slow regardless of the assured and attractive features of the cloud. In spite of the aforesaid problems, the organization has a tendency of reluctance in contributing their critical identity information to the cloud [6].

In a cloud system, the storage and processing of data is performed by organizations or with the help of third party vendors. The service provider has to ensure that data and applications stored in cloud are protected as well as the infrastructure is in secure environment. Further, users need to verify that their credentials for authentication is secure [7]. There are many security issues that compromise data in the process of data access and storage in the cloud environment, especially in the case of data storage with the help of third party vendors who themselves may be a malicious attacker. Though standards and best practices are available for overcoming such security problems, cloud service

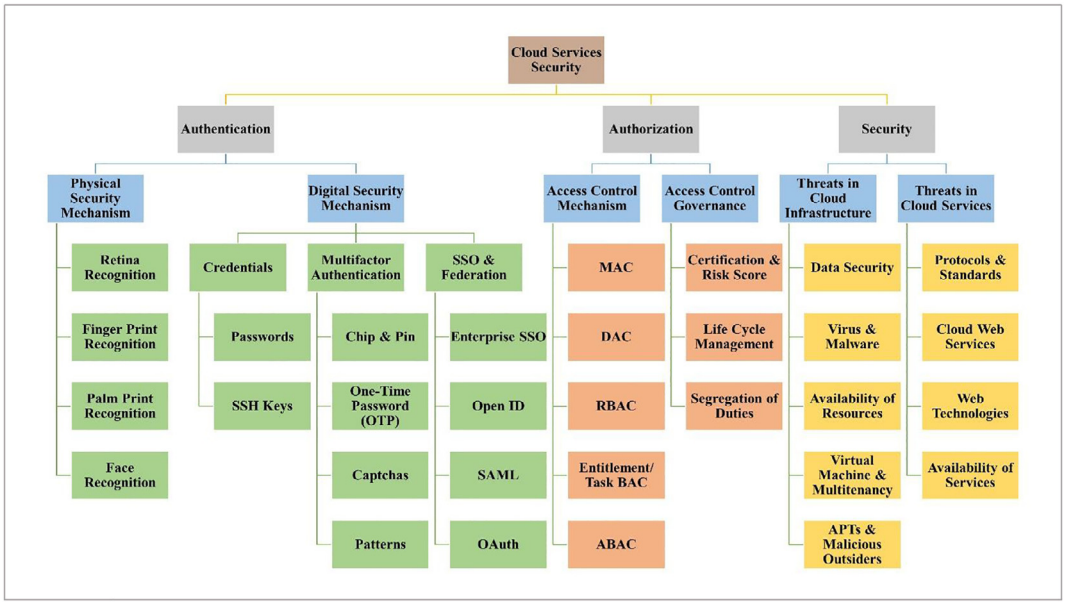

Fig. 1. Taxonomy of cloud services security.

providers are reluctant in securing their network with the updated set of security standards [8]. Identity and access management is one of the best practices to measure on cloud services. Presently, Identity and Access Management (IAM) provides effective security for cloud systems. IAM systems perform different operations for providing security in the cloud environment that include authentication, authorization, and provisioning of storage and verification. IAM system guarantees security of identities and attributes of cloud users by ensuring that the right persons are allowed in the cloud systems. IAM systems also help to manage access rights by checking if the right person with the right privileges are accessing information that are stored in cloud systems [9]. Currently, many organizations use Identity and Access Management systems to provide more security for sensitive information that are stored in the cloud environment. A taxonomy of cloud services security is shown as Fig. 1.

The major contributions of the paper are summarized as follows:

- Comparative analysis of different aspects in identity and access management mechanisms in cloud environment.
- Overview of access governance policies which are least explored area in identity and access governance.
- Overview of market leading identity and access control suite of products and solutions.
- Overview of common security threats in Cloud IAM systems and prevention techniques.
- Recommendations on governance policies and industry best practices.

Further, the rest of the paper is organized in eight sections. The authentication mechanisms that include credentials, SSO and federation are dealt in Section 2. Section 3 deals with access control mechanisms, access control policies and access control delegation. Identity and access management systems are analysed in Section 4. The security threats in cloud computing that include, data security, Virtual Machine (VM) and multi-tenancy are detailed in Section 5. Analysis of security threats in cloud environment is presented in Section 6. Recommendations and industry best practice are discussed in Section 7. The survey is concluded in Section 8.

2. Authentication mechanisms

Authentication is the process of approving an entity through another entity. It is used to ensure whether the person or the application is eligible for accessing or claiming. The authentication process is usually performed by a software or by part of a software [10]. The common authentication methods in a network environment are log-on credentials, multifactor authentication, third-party authentication, simple text passwords, 3D password objects, graphical passwords, biometric authentication and digital device authentication. A cloud system follows any one or combination of the aforesaid authentication mechanisms [11]. Presently, cloud access permission is granted through an identity management system.

2.1. Physical security mechanisms

Physical security mechanisms like, access cards and biometrics ensure security of cloud resources and facilities by denying unauthorized access through authentication. Cloud data centers (CDCs) are the recent attractions of organizations as they provide ease of access to their customers at any time. CDCs centralize all servers, networks and applications so that users access data at any time and from any location. As a part of data center security, access cards and biometric authentication like, iris or retina recognition, fingerprint recognition, face recognition and palm print recognition can be used. In order to prevent the data leakage from insiders or any unauthorized access to data centers, physical security along with certain usage and governance policies are required. Physical security mechanisms presently used are biometric access control and digital devices for authentication [12].

2.2. Digital security mechanisms

2.2.1. Credentials and secure Shell keys

Credentials are the evidence of authority, status, access rights and entitlements. It gives the evidence that the particular user is entitled or deserves to utilize resources and services. The usage of credentials like one-time password, pattern, and captcha is a tra-

ditional way of securing the system from malicious activities. Most commonly used mechanisms to manage access credentials for cloud environment are Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory (AD) technologies. LDAP and AD servers are managed by either third party vendors or within the organizational network in cloud computing [13]. Cloud maintenance overhead increases when multiple applications are deployed on these traditional credential management mechanisms. It is essential to add, disable, modify or remove accounts whenever any employee leaves or enters the organization. In managing the credentials at the provider side, weak credential reset vulnerability is represented when weak password recovery mechanisms are used. The hackers can monitor or manipulate data in the cloud along with malicious redirects whenever the credentials are compromised [14].

Secure Shell (SSH) keys help to identify the SSH server through public-key cryptography or challenge-response authentication. The main advantage of SSH keys is that the authentication to the server is performed without passing the password over the network. This prevents the interception or cracking of the password by hackers. The attempts of guessing credentials through brute force attacks during authentication are eliminated by SSH keys. SSH agents help to establish connection with servers without using separate passwords for each system. SSH key agent stores the private keys and provide them to the SSH client programs. These private keys are encrypted with passphrase and the passphrases are provided during each attempt to connect with the server. In every individual invocation of SSH, the passphrases are needed to decrypt the private key before proceeding to authentication phase. The passphrase is utilized only during the process of adding the private keys to the agent's store. This attempt favours the communicating devices which makes frequent SSH connections. SSH agent runs automatically once the login is initiated and persists for the entire session duration. The main concern of SSH keys is that the security is not better than credentials if the private keys are not well protected. Static credentials and SSH key mechanisms are commonly used for cloud web service authentication.

2.2.2. Multifactor authentication

Multifactor authentication is another method to secure digital assets and transactions over the Internet. Typically, One-Time Password (OTP), Captchas or Patterns are used as the secondary authentication mechanism along with credentials. Multifactor provides additional layer of security over the traditional credential based authentication. Generally, online transactions are authenticated using One-Time Passwords. In the financial transactions through online, server generates a one-time password using specific algorithms based on its configuration and the generated OTP is sent to the user either through a registered mobile number or through email. Another type of OTP is generated with the help of hardware/software token generators which is protected by a Personal Identification Number (PIN). This password can be used once and it has a certain time limit for usage. Captcha is normally used to secure the web applications from attacks by programmatically driven malware. Captcha could be an alphanumeric combination, a mathematical equation or an image and with a provision for a refresh. Patterns are another form of authentication which has different formats. Dotted patterns are widely used in mobile applications while matching image selection is predominantly used in web applications. The usage of security questions is an alternate method of securing digital assets which is a form of shared secret. In this method, the user selects security questions from the predefined list and defines the answer. At the time of authentication, the predefined security questions appear on the login screen and by providing the defined answer along with the credentials allow the user to get authenticated.

2.2.3. Chip & PIN

Chip and Personal Identification Number (PIN) is the conventional method of authentication for financial transactions. This can also be used for authentication to machines/services in a network of an organization. The asymmetric encryption technology uses public and private keys to encrypt and decrypt data used in the chip & PIN mechanism. The microprocessor chip stores the user data and security keys through the creation of unique transaction data to protect against frauds. The communication between the client/terminal with the authentication server is encrypted and signed with the help of security key which is stored in the chip. The server verifies the signature and decrypts the communication with the help of pairing keys which are stored in the server. The PIN is used to authenticate the client/terminal for accessing the user data and keys from the chip.

2.3. SSO & federation

The conventional authentication mechanisms are not always applicable for remote authentication. Authentication for accessing SaaS application needs centralized monitoring to limit software piracy. Multiple services are most likely to be subscribed by the cloud customers, resulting in multiple login requirements [15]. It also creates problem in maintaining a large number of credentials by a single user. The possible solution is the usage of single sign-on techniques. Single Sign-On (SSO) provision helps the cloud users to use one password for all application/service access. It provides secured and uninterrupted services by keeping one credential for each user. The users need not specify their credentials at every time of accessing different cloud web services [16]. Security Assertion Markup Language (SAML), Open Authentication (OAuth) and OpenID provide Single Sign-On (SSO) facility by allowing the Identity Provider (IdP) to share the authentication and authorization information with the Service Providers (SPs) as shown in Fig. 2.

2.3.1. Enterprise SSO

Enterprise Single Sign-On facilitates the storage and transmission of user credentials with the help of encrypted session cookies across web based applications. Once a user is authenticated through a centralized authentication server, SSO generates a browser based encrypted session cookie. While the user navigates from one application to another, the new application checks for a valid session cookie. The user details are read from the valid session cookie and the user is authenticated to the targeted application. Whenever any application is not able to find a valid session, the user is navigated to the centralized authentication mechanism for re-authentication. A new session will be generated for the target application after successful authentication.

2.3.2. OpenID

OpenID is an open standard authentication protocol which allows the user's authentication to the relying parties (RP) with the help of third party identity vendors. A relying party (RP) is a resource provider which could be a website or application that requires the end-user verification. OpenID supports SSO services by allowing single credentials for authenticating to multiple websites and web service accesses. There is no need for the usage of webmasters in OpenID system as it supports decentralized authentication mechanism. OpenID identity provider stores the list of users and with the help of identity provider's list, users create their accounts. The cloud users login into any website which supports OpenID authentication by using their accounts. The latest version of OpenID protocol is OpenID Connect (OIDC) which is built on the top of the OAuth protocol. OpenID Connect supports authentication mechanisms for native and mobile applications. It also pro-

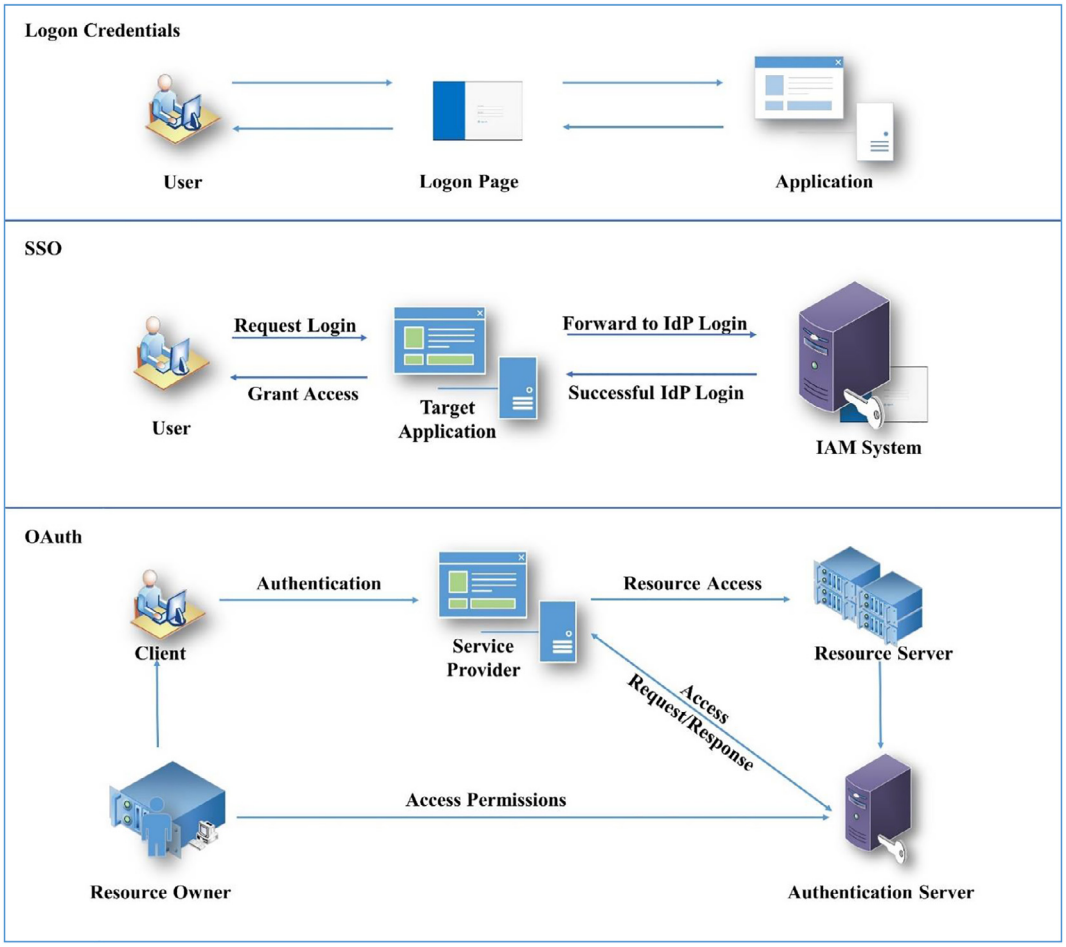

Fig. 2. Comparison of different authentication mechanisms in cloud environment.

vides an option for encrypting and signing the communications between the participants.

2.3.3. OAuth

An alternative method of authentication mechanism is OAuth which offers one-way authentication or mutual authentication for cloud computing [17]. OAuth is an open standard for access delegation which grants access to the user on other website/application without sharing the passwords from an authenticated website/application. The current version of OAuth protocol is OAuth 2.0. The relying parties (RP) need to register with the OAuth token provider to obtain client identifiers and client secrets. When an end user tries to access the relying party, it will be redirected to the identity provider for authentication. Once the user is successfully authenticated, the identity provider shares the OAuth access token along with refresh token, client id and the client secret. The relaying party retrieves the additional user details from the user info end point. The relaying party renews the access token during its expiry with the help of refresh token. The digital signature for the access tokens is not promoted by OAuth2.0.

2.3.4. SAML

Security Assertion Markup Language (SAML) basically works on token-based request and response techniques and it is also an open standard mechanism for communicating between two parties [18]. These two parties are particularly service provider (target application) and identity provider. SAML ensures the authentication of users with target application is secured. SAML tokens do not contain any user credential information. SAML also allows to encrypt and encode data communication between the identity provider and service provider (target application). It ensures that the user is securely authenticated to the target application [19]. SAML provides web browser single sign-on (SSO) and promotes interoperability by specifying and standardizing the web browser SSO profile. The SAML specification involves the roles of user, identity provider and service provider. When a user request for a web service from target application, the target application requests and gets authentication assertions from identity provider. The target application takes decision about the access rights based on the assertion. The social networks use SAML exchanges for providing identity services. Table 1 summarizes the various authentication mechanisms and their associated security issues.

3. Authorization mechanisms

Authorization is the method of permitting or disagreeing access to a particular resource depending on an authenticated user's entitlements. The authorization process decides which user or what applications are allowed to perform on the system and user/application identity information are used for pleasing the decision [20]. Cloud network contains different service providers' environment in which a single user is able to access different kinds of services at the same time while each service is from a different service provider and with different security levels. Sometimes, authorization rights are given by third-party vendors and these third-party applications are authorized to access certain private information as shown in Fig. 3. Such permissions are unsafe since the privacy of

Table 1
Summary of Various Authentication Mechanisms - Security Aspects and Issues.

Topic	Mechanisms	Security Aspects	Issues/Attacks	Reference
Physical Access	Centralized data storage	Physical presence is mandatory and verified using access card or biometrics	Malicious Insiders, Cool Boot Attack	[4,5,12,13]
Credentials	Lightweight Directory Access Protocol (LDAP), Connectors, Database Storage and Microsoft Active Directory (AD)	Individual access rights per application	Weak credential-reset vulnerability, Phishing and malicious redirects	[5,13,15,17–19,22,37,78]
Multifactor	One Time Password, Tokens & Biometrics	Additional authentication layer over the credentials	DoS Attack, Replay Attack, Phishing Attack and Identity Theft	[11,13,14,67,74]
Single Sign-On	SAML, OpenID, OAuth	Single password for all the associated applications Centralized password policies No password sharing to applications	Cross Site Request Forgery, Replay Attack, Cross Site Scripting	[13,15,16,18,19,69]

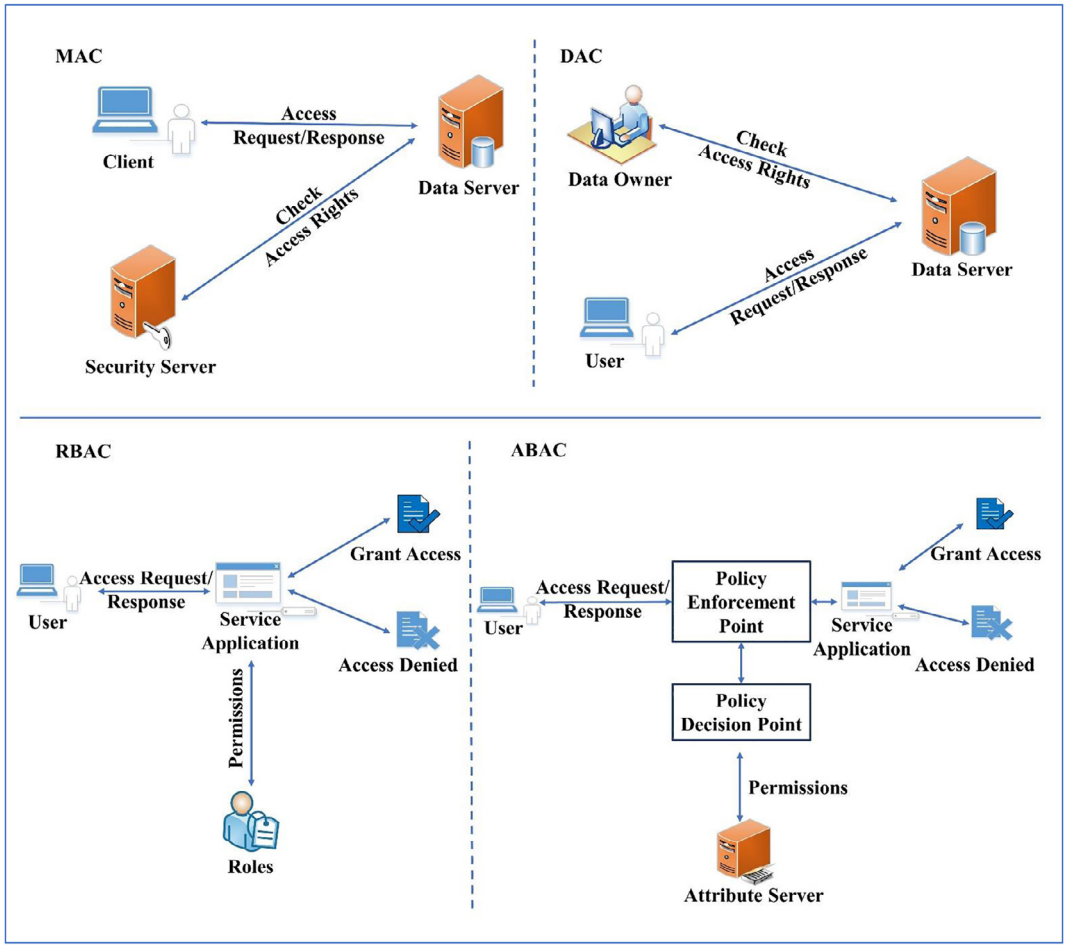

Fig. 3. Comparison of different Access Control Mechanisms in a cloud environment.

the user is involved. For example, in social networks, cloud-based hosted applications are accessed by outside applications whenever the user authorizes that application [21]. In case of malicious activity, it is easier to obtain intelligence on targets. Authorization in a cloud environment is attained by either access control policies or access right delegations. The CSP defines and implements access control policies such that the resources and services are accessed only by the authorized users. Centralized access control mechanisms are advantageous to the organizations in securing sensitive information, reducing several management and security tasks [22].

3.1. Access control mechanisms

3.1.1. Mandatory access control

Mandatory access control (MAC) mechanism is the traditional mechanism to define the access rights of users. MAC gives access

Table 2
Summary of Various Authorization Mechanisms - Security Aspects and Issues.

Topic	Mechanism	Security Aspects	Issues/Attacks	References
Access Control	MAC	Application owns the individual access permissions	Unauthorized access, over classification of data, difficult to implement,	[15,20,23–26,42]
	DAC	Access rights to an application is owned and controlled by another application	Trojan horse susceptibility, Flawed software, Information flaws, Malicious attacks	
	RBAC	Access rights and privileges to multiple applications are bundled as an organizational role	Administrative issues, data abstraction issues, Real-time issues	[15,24–26,28,32,36,37,42]
	ABAC	Access rights and privileges to an application determined based on Subject, Object, Policy and Environmental Attributes	Delegation issues, administration issues, auditability and scalability issues	

permission through the operating system or security kernel. It controls the ability of data owners to grant or deny access rights to clients for the file system. All access control rights are set by the system manager and imposed by the security kernel or operating system. Clients have no rights to alter these access rights. In mandatory access control model, each file system object has a classification label such as, secret, top secret or confidential level. Each device and client is assigned a similar classification and clearance level. The security kernel determines the classification label of clients and resources. The operating system or security kernel checks the credentials of each person or system while accessing a particular resource to determine the access rights of that specific person or device. Even though MAC provides more security in accessing the resources, it needs careful planning and frequent monitoring to keep all the classification labels up-to-date [23]. MAC has less flexible environment to process the access rights.

3.1.2. Discretionary access control

Discretionary access control (DAC) is a security access control mechanism which controls the access permissions through data owner. In DAC, the access rights of each user are performed during authentication by validating the username and password. DACs are discretionary as owner determines the privileges of access. In DAC, file or data has owner and the data access policies are controlled by data owner [24]. DAC provides more flexibility than MAC however, DAC provides less security than MAC. Table 2 summarizes the various authorization mechanisms and their associated security issues in cloud environment.

3.1.3. Entitlement/Task based access control

Entitlement or task based access control is one of the minute level access control mechanism. A specific access permission is required for each task, action or process that is represented by an entitlement or task. This model has capabilities to handle complex access conditions to determine whether the access rights need to be granted or denied. The major concern about entitlement access control model is the maintenance of large number of entitlement sets. The users also need to raise separate request and get the approval for each entitlement. Entitlement or the task based access control model has the ability to represent and implement other hierarchical access control models like role-based access control and attribute based access control.

3.1.4. Role based access control

Role Based Access Control (RBAC) provides access rights based on roles and privileges of the users. User permissions are given by different parameters of RBAC like, user-roles, role permissions and role-role relationships. The roles are classified into two categories as application/technical role and organizational/business role. An application/technical role contains the combination of different application specific entitlements or tasks based permissions and its scope is limited to the specific application. An organizational/business role is generated based on different job functions and access rights assigned to an employee [25]. An organizational/business role is a combination of different application/technical roles. RBAC provides administration security in organizations with large number of users and number of permissions. RBAC contains mainly three rules for assigning permission to a particular user, such as, role assignment, role authorization and permission authorization. The permissions for accessing the data are provided to users based on these rules. RBAC provides a highly secured environment for assigning access permissions. The main limitation of RBAC is that the assigned roles may change from time to time which needs a real-time environment to check and validate the changes.

3.1.5. Attribute based access control

Attribute-based Access Control (ABAC) is a mechanism to control the access permissions. ABAC defines the access control mechanism by the use of policies which determines different sets of attributes to check the access rights of each user. The policies are generated using different types of attributes and based on the policies, the system determines the access permissions. The considered attributes are subject attributes, object attributes, resource attributes and environmental attributes. In the ABAC model, roles and privileges of each user are pre-defined. It resolves many authorization problems, achieves an efficient regulatory compliance and allows flexibility in implementation [26].

3.2. Access control governance

Cloud service providers define policies related to access control in IAM system for ensuring only the valid users are accessing the resources and services. In order to achieve the objectives of each organization, CSPs have to ensure three important characteristics namely, Governance, Risk Management and Compliance (GRC) [27]. Governance is the process of organizations which reflect the complete organizational structure and management mechanisms to achieve their goals. These governance policies are defined and executed by the board of directors of that particular organization. GRC mechanism tries to implement the synchronization of sensitive information and the activities across governance, risk management, compliance for improving the efficiency of operation, effective resource sharing, wasteful overlaps and efficiency of report activities in organizations. Risk management is the process of managing risks associated with resource sharing and access

Table 3
Summary of Various Governance Mechanisms - Security Aspects and Issues.

Topic	Mechanism	Security Aspects	Issues/Attacks	References
Access Control Policies	Governance	Periodic identity and access certification	Cyber-attacks, data and security breaches, transparency issues, segregation of duties	[25,26,29,39,41,63–66,68]
	Risk Management	Risk score calculation, Preventive mechanisms	Data Tampering Attack, Elevation of Privilege & Spoofing Attack	
	Compliance	Organizational policies and implementation	Phishing attacks, loss of control	
Identity and Access management	Credential Synchronization, provisioning & Identity Federation	Right Person, Right Access, Right Resource at Right Time	Synchronization leakage, Identity Theft, Data Tampering Attack & Spoofing Attack	[9,10,19,30,31,70]

permissions to achieve the objectives of organization. Compliance refers to the offering of organizational policies, laws, regulations, and procedures [28].

3.2.1. Certification & risk score

Certification is the process of verifying the links between users, roles and resources to ensure that they are true and correct. Certification enables to review the role hierarchy, user privileges and business rules that are defined in Identity Governance. When a certification is initiated, IAM system automatically invites managers to review and certify the access privileges of the users or resources under their administration. User certification is provided to certify the resources and roles associated with a user. Generally, the privileges of employees are reviewed by the managers. The resources, parent roles, child roles and users linked to each role are certified using role certification. Resource certifications are used to certify the resources and users who are linked to each resource. The roles associated with users are reviewed by administrators of each resource and the access rights of each user with resources are validated. Account certifications are used to certify each account that are linked to users. Each account and its user assignments are typically reviewed by the compliance officer. When a user certifies his own privileges, it is called self-attestation certification. Risk scores are derived based on threat indicators from identity, accounts and entitlements, assets and behavior context. These risk scores are certified by risk score based certification. The user-centric risk score triggers risk-based access certification system. The end result in access certifications provide the most effective, efficient access governance and administration processes.

3.2.2. Life cycle management

Life cycle management is the process by which the process of creation or deletion of accounts, management of accounts, entitlement changes and track policy compliance are performed. The lifecycle management of an individual's identity allows to securely enable access to the right applications. In lifecycle management, user is managed starting from the point of granted access throughout his lifecycle which includes, change of role, entitlement and removal at a point where the relationship concludes.

3.2.3. Segregation of duties

A proper segregation of duties is one of the audit objectives in the organizational framework. Basically, two or more stages of transaction/operation should be controlled by more than one person as per segregation of duties. Organizations need to define the right policies to ensure responsibility assignments and cross checking of duties. Segregation of duty mechanism helps to prevent deliberate frauds as it requires the involvement of two or more people. It also helps in finding out the innocent errors which happens in the process work flow. The duties or responsibilities are broadly classified into four categories, namely, authorization, record keeping, custody and reconciliation. The review and approval of transactions or operations happens in the authorization phase. Record keeping is the phase of creating and maintaining the logs. The custody is the phase of having access or control over a physical or digital asset. Finally, the verification and recording of transactions happens in reconciliation phase. Table 3 summarizes the various access control mechanisms and their associated security issues in cloud environment

4. Identity & access management systems

Identity Management (IdM) is capable of performing functions like, administration, discovery, maintenance, policy enforcement, management, information exchange and authentication. Identity and Access Management (IAM) ratifies that same identity are used and managed for all applications and simultaneously ensures security. It is used to authenticate users, devices or services and to grant or deny rights to access data and other system resources. In the event of the access of any application, the system or service does not require its own identity store or authentication mechanism to authenticate. Instead, the process of identity verification can be configured with the trusted identity provider which indeed reduces the workload of the application. Identity and access management simplifies the management of large-scale distributed systems. Identity and access management are used within an enterprise or outside of an enterprise in a business-to-business relationship or even between a private enterprise and a cloud provider [30]. IAM has an extensive organizational area that deals with identifying cloud objects, entities and controlling access to resources based on pre-established policies [31]. There are a number of operational areas related to identity and access management. The operational areas include identity management and provisioning, authentication management, federated identity management, authorization management and compliance management [32]. These operational areas ensure that the authorized users are securely and effectively incorporated into the cloud. The Service Provisioning Markup Language (SPML) is an XML-based framework that is used for identity management. It exchanges resources, user, and service provisioning information between organizations. One of the shortcomings of SPML is that it uses multiple proprietary protocols from various vendors which leads to a bunch of different Application Peripheral Interfaces (APIs). As the APIs are not of the same vendor, it is difficult to make them interact with each other. The second operational area of IAM is authentication management. This ensures that credentials such as passwords and digital certificates are managed securely [33]. The third operational area of IAM is Federated Identity Management. This identity management authenticates cloud services using the organization's selected identity provider. Federated identity management ensures privacy, integrity and non-repudiation. This also ensures the trust between a web-based application and the identity provider by exchanging Public Key Infrastructure (PKI) certified public keys. The fourth operational area is authorization management. After successful authentication, authorization

management determines whether the authenticated entity is allowed to perform any function within a given application. The last operational area of identity and access management is compliance management. This ensures that an organization's resources are secure and accessed in accordance with the existing policies and regulations [34]. Identity management has an important role in the area of cloud security issues. Privacy and interoperability are the major issues in the existing identity management approaches, especially in public cloud environments [35].

Presently, IAM systems are the efficient mechanisms to reduce risks associated with cloud environment. Many organizations provide IAM system to secure the information by controlling the access permission of each user [38]. The popular IAM system providers are SailPoint, IBM, Oracle, RSA and Core security. SailPoint's identity management solution has capabilities in the areas of password management, compliance control, data access governance, access request, automated provisioning and Single Sign-On [80]. The IBM Identity and access management suite of products provide solutions in web access request, user provisioning, multi-factor authentication, enterprise single sign-on, privileged identity & access control and user activity compliance [81]. Oracle Identity and Access Management provide four major solutions for cloud security. Its products leverage its first solution through the various capabilities in identity administration like, self-service account request, identity life cycle management, password management and enterprise role management. Oracle IAM system provides the second solution for authentication and trust management services like, identity federation, single sign-on and privacy. It also provides the third solution in access control, like fine-grained entitlements, risk-based authorization and web services security. Oracle IAM system provides its fourth solution in identity and access governance like, segregation of duties, audit and compliance reporting, conflict-resolution management, role mining and engineering, attestation, identity & fraud-prevention analytics and directory services (identity virtualization, persistent storage, database-user security, and synchronization) [82]. RSA SecurID Suite [83] offers a comprehensive set of capabilities including authentication, access management, identity governance, risk analytics and lifecycle management. Core Security [84] provides a comprehensive suite of identity management and access governance solutions in the areas of compliance, privileged services, password management and access & identity management. Privileged Identity Management (PIM) specifies the ways in the administration of superuser accounts and the account holder rights. PIM establishes tools and processes such as provisioning tools or specialized PIM products for identity management. The popular PIM system providers are IBM PIM, CyberArk and Oracle PAM.

5. Security threats in cloud environment

Cloud computing is an emerging technology that is currently the most reliable system to store and secure information. Even though cloud based system has numerous benefits, it has some issues associated with security of the stored data. The initial step of removing the risks is to identify the major risks in a cloud environment [39]. Shared and on-demand access are the dominating

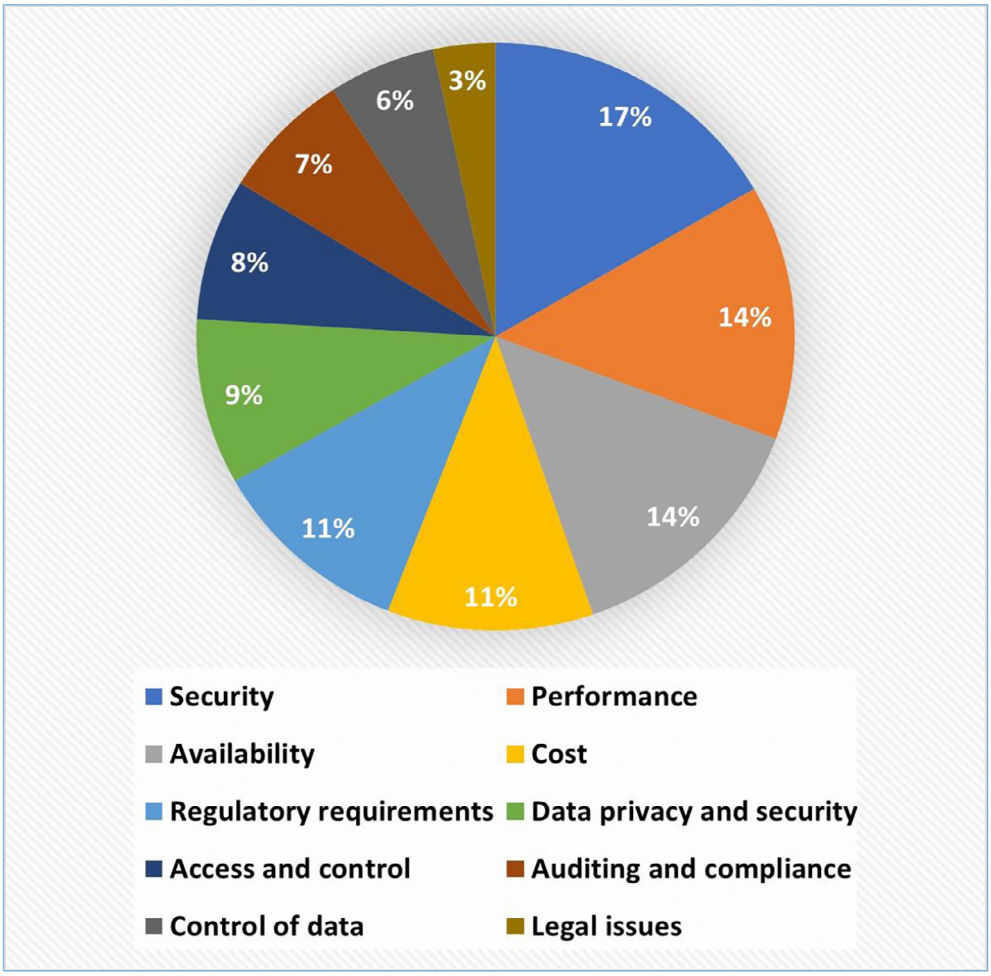

Fig. 4. Analysis of different issues involved in cloud environment.

factors for the newly identified security issues in cloud. The intensity of the growth of cloud computing increases the security threats in multiple dimensions. The identified security issues are data breaches, credential protection, account hijacking, hacked interfaces and APIs, malicious insiders, DoS attacks and shared technology issues [40]. The various areas of threats in cloud environment and their share in the present time are shown in Fig. 4.

5.1. Threats in cloud infrastructure

5.1.1. Data security

Protection of data is essential in cloud environment in terms of availability, integrity and confidentiality. One of the possible data security mechanism is cryptography. Cryptographic mechanisms apply security measures directly to the data. Prime number factorization, intractability of the discrete logarithm, random number generations are some mathematical methods to produce numerical data for cryptography [41]. Two distinguished factors contributed are evolving technology and password cracking methods. As the processing capacity of modern computing devices have increased significantly, search time complexity and huge combinatory key spaces are easily and quickly performed. The most vulnerable attack affect in cryptography is brute-force attack. Data security issues are categorized as security requirements for data in motion and security requirements for data at rest. The security issues for the data at rest arises when a malicious insider misuses or manipulates the user access information through his access rights to the application database or provide unauthorized access privileges to the third party for a particular application [42]. The sensitive data contains the details of the users and their privilege information which has to be secured through appropriate cryptographic suite. In some scenarios sensitive data to be transferred in a large amount from the server to the service requesting target application. In such cases, the data should be protected with the help of SSL certificates.

5.1.2. Virus or malware

Malicious software is referred to as malware that is programmed to interrupt with normal computer operations. It is used to gather sensitive information or gain access to isolated computer systems [43]. Malware has a terrible intent of acting against users' requirements and causing serious damages in the performance of the cloud based systems. The cyber criminals mostly share malwares and insist the users to install the shared software on their computers or mobile devices by giving fake promises. The ultimate goal of these criminals is to gain the control of that particular computer or mobile device. Once such malware is installed, the attackers potentially gain total control of the computer or mobile devices. While the attacked system tries to connect with the cloud server for utilizing cloud services, the malware spreads into the virtual machines of the cloud environment which later spreads to every user who access the cloud. Malware events or attacks occur frequently in organizations aiming to breach the security infrastructure of the organization [44].

5.1.3. Availability of resources

Availability of resources refers to the systems and services that are accessible by an authenticated entity through appropriate authorization. The availability of the cloud means the set of resources that are accessible at any time by authorized entities [45]. Availability is considered as one of the essential security requirements in cloud computing as it ensures the usage of resources at any time and at any place by the cloud users. In some cases, the resources are available in a diverse manner which has to be provided to the cloud users without any interruptions during the cloud service access. In the event of security breach or disaster situation, the ability to continue the business as usual is the primary objective of availability [46]. Generally, cloud services run on multiple virtual machines. Hypervisor controls virtual machines by allowing multiple operating systems to share a single hardware host. Whenever a hypervisor is not working normally, it significantly impacts the availability of the cloud service [47]. The total number of research articles that deal with major concerns of cloud environment is shown in Fig. 5.

5.1.4. Virtual Machine & Multitenancy

Multitenancy is a style in which multiple customers simultaneously use a single instance of a software application. The cloud customer who has the ability to access applications in the cloud environment is called a tenant. Multitenancy represents that more than one tenant share any particular application including its computational services, resources and storage [48]. In multitenancy, resources are shared on the cloud network. It is needed to ensure that the cloud provider is taking appropriate steps in ensuring isolation of network traffic, application instances and virtual machi-

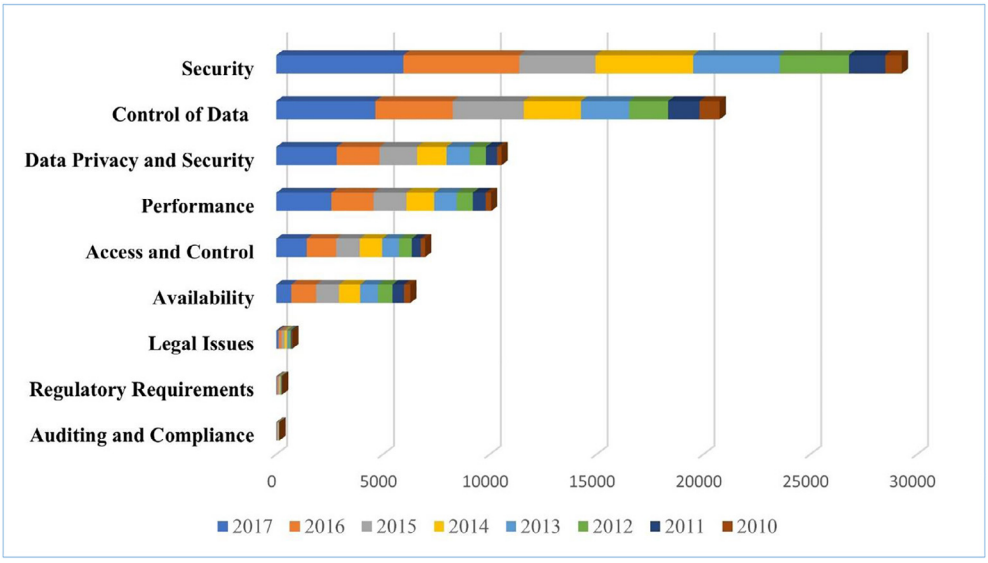

Fig. 5. Research articles in each category of issues in cloud environment.

Table 4
Summary of Various Cloud Mechanisms – Security Aspects and Issues.

Topic	Mechanisms	Security Aspects	Issues/Attacks	Reference
Data Security	Cryptography	Encryption based data protection and privacy	Brute-Force Attack	[40–42,47–50,72,75]
Availability of Resources	Resources Accessibility and usability	Right resource at right time	Bogus resource usage Cloud outages	[13,45–47,71,77]
Multitenancy	Hypervisors, VMM	Shared resources in cloud. Increases the necessity of cyber security	Co-location, co-residence, or co-tenancy attacks, cross-VM attacks, & Side-channel attacks	[8,11,15,18,42,48–50,79]
APTs and Malicious outsiders	Pre-determination of the targets and Persistence	Threat to cyber security	Intelligence gathering, reconnaissance scans, State-sponsored malicious cyber activity, espionage, & Hacktivism	[2,3,5,13,15,34,38,72]

Table 5
Summary of Various Services and their Associated Attacks.

Topic	Issues/Attacks	Mitigations	Reference
Protocols and Standards	Session Hijacking, network based attacks, cookie theft, TLS attack	Usage of secure session, efficient anti-virus, anti-malware software	[1–4,13,29,54,58,73]
Web-Services	Spoofing Attacks, Wrapping attacks	Implementation of strict security policy at receiver and sender side	[1,13,55–58]
Web-Technologies	Web sites growth infection, session attacks, manipulation attacks, malware downloads, browser vulnerabilities	Vulnerability analysis and preventive actions	[1,3,4,58–60]
Availability of Services	Flooding attacks, DNS reflection and amplification attack	Regulating the requests or by implementing a fleet of servers	[3,13,51,60–62,76]

nes (VM). Resource utilization is managed by partitioning a virtualized, shared infrastructure between various customers [49]. In order to achieve the intended flexibility of provisioning the reliable services, cloud networks need high degrees of multitenancy over different platforms of operation. In cloud computing, multitenancy and virtualization are the massive issues. Organization needs to ensure all tenant services are accurately isolated from one another and also ensures that there are no possibilities of data and transaction leakages from the shared resources cloud environment [50].

5.1.5. Apts and malicious outsiders

The Advanced Persistent Threat (APT) is a kind of attack in which an attacker or an unauthorized person gains access to a cloud environment and stays in the network for long period of time without being detected. APT attack aims at stealing the data instead of causing damages to the network or organization. The target organizations of APT attacks are in areas with high sensitive information such as, manufacturing, national defence and financial industry [51]. The information from corporations, governments and individuals are targeted to enable control, modify and future use of data to disrupt performance in the cloud systems [52]. An APT attack model consists of intelligence gathering phase in which an attacker performs more bold reconnaissance scans to map the target network. In threat modelling phase, attacker identifies the target network or server and the best technique for performing the attack. Finally, the attacker exploits the possibly found vulnerabilities and performs the attack [53]. Table 4 shows the summary of various categories of security mechanisms and their associated issues.

5.2. Threats in cloud services

Cloud environment not only contains hardware for data to be stored and processed, but also contains path for transmitting data. Cloud infrastructure uses different standards and protocols that support multiple domains for interoperability and data transmission purposes.

5.2.1. Protocols and standards

The basic communication model on Internet is TCP/IP model and its stacks include different protocols and standards. Cloud standards and protocols that are related to cloud services need international standards to be maintained for cross platform operations. The requirements for the cloud service provider is to plan, establish, operate, implement, review, monitor, improve and maintain as specified by the service management system. The necessity for the fulfillment of the service requirements include, design, delivery, transition and improvement of services. Cloud services are very much related to IT management system as the services provided are IT based [54].

5.2.2. Cloud web services

The cloud environment uses different types of services for integrating web applications. The web services are one of the standardized ways of incorporating web applications. Web services use different protocols for different operations and these collectively perform the services effectively. In case of data tagging, web services use Extensible Markup Language (XML) and for data transferring, Simple Object Access Protocol (SOAP) is utilized. The available web services are showed using Web Services Description Language (WSDL) and the listing of available resources are done by Universal Description Discovery and Integration (UDDI). Web services technology enables organizations to fully utilize the Software as a Service (SaaS). Standard Internet technologies mostly deploy web services. The availability and accessibility of web services in cloud environment are maintained by a dedicated team employed by the vendors [55–58]. Mostly, controlling of access permissions that affects the security of services are done by these dedicated team. In order to reduce these problems, well organized web services access control mechanisms are necessary to be implemented by organizations.

5.2.3. Web technologies

Web technology is an advancing mechanism to allow the interface between web server and subjects for communicating over the network. This technology allows quick, high-speed and convenient

transmission of information over a number of systems and devices [59]. Web technology contains different communication methods to increase the efficiency of operations. The processes involved in web technology are complex and diverse. Computer systems are affected by attacks through networks. Malware attack exploits the weaknesses in a network to infect various network systems. Malicious websites act like genuine websites by hiding their malicious nature. Such websites produce vulnerabilities in the applications provided by web technologies. In order to reduce these hidden attacks, network security is essential while using web technology [60]. The main disadvantage of web technology is that it is not user-friendly. Hence, it is complicated for users who have less experience to track network problems. A well-trained person with specific skills is required to solve these network issues. Table 5 shows the summary of various Internet services and the attacks associated with these services.

5.2.4. Availability of services

Data centers provide huge number of services which are hosted in multiple servers. In order to support these services or a huge amount of data transfer, it requires proper network links with high bandwidth. There are several types of security attacks which affect the availability of a cloud based service like, DoS, DDoS, flooding attacks, DNS reflection and amplification attack. Basically, Denial of Service (DoS) attacks are classified into two categories as direct and indirect attacks. In direct attack, a single malicious request creates the server overloads by exploiting a vulnerability or processing numerous requests. In the indirect attack, the flow of packets fully saturates the network links or intermediate routers with bogus requests which terminates the honest connections while reaching the bandwidth capacity. In order to overcome the impact of DoS attacks, it requires to setup a High Availability (HA) environment which spreads across multiple data centers and also requires a proper Disaster Recovery (DR) plan [61].

6. Security analysis in cloud environment

6.1. Man-in-the-Middle (MITM) attacks

In cloud systems, attacker intercepts the communication between systems and manipulates data without the knowledge of provider and relying party. The attacker mimic the communication between provider and relying party pretending to act like them is termed as man-in-the-middle attack. MITM attack targets to steal personally identifying information such as credentials, account information and financial data including credit card numbers and bank details. The stolen information can be used in identity theft, illicit password changes and unapproved fund transfers. *Mitigation*: The usage of encryption methods could help to avoid the intercepts in the communication. Appropriate SSL (secure socket layer) configuration can reduce the risk of MITM attacks. One time access tokens and encrypted tokens for verifying the identity can reduce the MITM vulnerability.

6.2. Insider attacks

Insider attacks are launched by someone who is inside the security perimeter and compromising the security. The malicious insider is either business partner/contractor of an organization or former/current employee of that organization. These insiders misuse their privileges to access the sensitive resources of the organization which may affect the integrity, confidentiality or availability of that organization. In cloud networks, the insiders may be third party vendors or cloud administrators who uses the cloud resources to carry out attacks against the organizational infrastructure. *Mitigation*: The use of strong authentication and authorization mechanism is needed. The access governance policies of organizations should be suitably defined which could considerably reduce the insider attacks threats.

6.3. Password/Key compromise

In traditional authentication model, an attacker gets access to the web ***s***ervices/server credentials and misuse the cloud services/servers with the acquired access rights. The password/key compromise happens due to malicious insider, malware attack and vulnerability in the system. The other ways of password compromise is through password guessing (weak passwords), brute force attack, phishing attack or spoofing attack. *Mitigation*: The organizations can eliminate the use of static credentials for accessing web-based services by establishing federation/SSO. The cloud servers can be protected with the help of PIM (privileged identity management) solutions.

6.4. Replay attacks

In cloud services, the attacker creates an authentication request from the authentication message which was previously exchanged between an authorized user and the target system. In replay or playback attack, the attacker captures the authentication request through hacking and deliberately mimic it with or without modification to gain access to cloud resources. *Mitigation*: A strong encryption method can help to avoid the intercepts in the communication. The organizations can avoid replay attacks in their cloud environment by defining the expiry and OTPs for the authentication messages.

6.5. Session/Cookie hijacking

Session hijacking occurs when the session id for authentication of the users is not well protected. Typically, the session/cookie stores user details and their credential information. Once a valid session is hijacked, the attacker can use the compromised session id for spoofing attack. The packet sniffing tools are used to gain access of users' session key through capturing of the login sequence. In cookie hijacking, the browser's cookie is stolen to authenticate in other website without the knowledge of the owner. The session/cookie hijacking happens due to malware, vulnerability in system, phishing attack and sniffing tools. *Mitigation*: The usage of secure session can help to prevent session hijacking attacks from client websites. It is also recommended to use efficient antivirus, anti-malware software and software should be kept up-to-date. Session hijacking attack can be prevented by encrypting entire communication through channels.

6.6. Guessing attacks

In guessing attacks, attacker regenerates the passwords of users who use passwords as a simple patterns or make it to remember easily. The attackers collect some vital information about the valid users and try to guess their password by multiple attempts to login until they get the access. In offline cases, there is a high chance of getting the correct password by guessing it as there is no restriction on the number of attempts. *Mitigation*: The usage of strong passwords and blocks the user after a certain number of login attempts can prevent the system from different types of guessing attacks.

6.7. Denial-of-Service attacks (DoS/DDoS)

In Denial of Service (DoS) attack, the target server is overloaded with fake service requests which ultimately prevents the system from responding to the genuine requests. Once the target server is unable to handle the continuous service requests by its own, it delegates the requests to similar server instance in the load balancing system which ultimately leads to the flooding attacks. Distributed Denial of Service (DDoS) attacks are initiated by bots or malware from thousands of infected hosts. The servers in cloud environment are vulnerable to DoS/DDoS attacks as they support IaaS, SaaS models. *Mitigation:* The usage of firewalls to allow or deny access to ports, protocols or IP addresses. The impact due to DoS attacks on cloud services can be minimized by programmatically limiting and regulating (Products like, *DataPower Gateway* for limiting the allocation of network bandwidth) the hits count from each requesting organization channels.

7. Recommendations and best practices

The different identity and access control models are compared and the security aspects of each model are analysed in depth to provide comprehensive overview on IAM systems for academicians and industry personnel. The following recommendations are suggested on the authentication and authorization models for different scenarios.

- As a best practice, any of the multifactor authentication mechanism in association with the traditional credential based and SSH key based authentication must be used. The implementation of another level of security over the normal credential-based authentication helps the organizations to avoid the insider threats. The usage of chip & pin combination over the traditional chip/magnetic tapes mechanisms is also recommended for the same purpose.
- OpenID Connect framework which offer encrypted communication between the relying parties is recommended for federating a native application from a mobile or computer.
- In web based SSO scenarios, encrypted and signed SAML communication is strongly recommended to prevent vulnerabilities such as man in middle attacks and replay attacks.
- Role based access control is recommended as an authorization mechanism for organizations. The RBAC model ensures quick on-boarding of employees/contractors to the organization structure which saves on-boarding cost and time.
- ABAC model authorization mechanism is recommended for multi-party cloud infrastructure sharing as it offers flexible and dynamic operations.
- As an industry best practice, the access governance recommendations such as identity & account certification, life cycle management and segregation of duties to be followed for ensuring secured cloud services.

8. Conclusions

Cloud service is an important paradigm for digital solutions as it brings down the capital expenditure and operational expenditure of an organization. Security risks and vulnerabilities are the major concern of this technology due to its nature of multi tenancy and the third-party delegation for the cloud environment maintenance. This paper analysed and summarized the current security aspects, potential threats and mitigations involved in cloud services with emphasis on identity management, access management, security and services. This research compares different topics with their commonly used mechanisms, major issues associated with each mechanism, recommendations and best practices from academia and industry perspectives. The survey of different identity and access management mechanisms along with the different services offered by cloud technology highlights the necessity to enhance the existing identity and access management frameworks which indeed shows the direction for future research and development of appropriate methodologies.

Acknowledgements

The authors would like to thank the anonymous reviewers for their helpful suggestions that greatly contributed in improving the quality of the paper. The authors also thank **Rejeesh Ranganathan**, Solution Architect, Enterprise Risk and Security Services, Cognizant Technology Solutions and **Ravi Sundar**, Manager-Projects, Cognizant Technology Solutions for their valuable discussions on the various aspects of Cloud IAM systems.

References

[1] CSA, Security Guidance Critical Areas of Focus for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance, No. 1, pp. 1–76, 2009. [Online] https://cloudsecurityalliance.org/csaguide.pdf.
[2] S. Eludiora, A user identity management protocol for cloud computing paradigm, Int. J. Commun. Netw. Syst. Sci. 4 (2011) 152–163, https://doi.org/10.4236/ijcns.2011.43019.
[3] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (2011) 1–11, https://doi.org/10.1016/j.jnca.2010.07.006.
[4] Wayne Jansen and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication, pp. 800-144, 2011. [Online] http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.
[5] S. Singh, Y.S. Jeong, J.H. Park, A survey on cloud computing security: issues, threats, and solutions, J. Netw. Comput. Appl. 75 (2016) 200–222, https://doi.org/10.1016/j.jnca.2016.09.002.
[6] A. Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, X. Huang, Hierarchical and shared access control, IEEE Trans. Inf. Forensics Secur. 11 (2016) 850–865, https://doi.org/10.1109/TIFS.2015.2512533.
[7] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, K. Sakurai, Authentication in mobile cloud computing: a survey, J. Netw. Comput. Appl. 61 (2016) 59–80, https://doi.org/10.1016/j.jnca.2015.10.005.
[8] Z. Liu, J. Luo, L. Xu, A fine-grained attribute-based authentication for sensitive data stored in cloud computing, Int. J. Grid Util. Comput. 7 (2016) 237–244, https://doi.org/10.1504/IJGUC.2016.10001940.
[9] D.H. Sharma, C.A. Dhote, M.M. Potey, Identity and access management as security-as-a-service from clouds, Procedia Comput. Sci. 79 (2016) 170–174, https://doi.org/10.1016/j.procs.2016.03.117.
[10] A. Singh, K. Chatterjee, Identity Management in Cloud Computing through Claim-Based Solution, in: 2015 Fifth Int. Conf. Adv. Comput. Commun. Technol., IEEE, 2015. doi:10.1109/acct.2015.89.
[11] I. Butun, M. Erol-Kantarci, B. Kantarci, H. Song, Cloud-centric multi-level authentication as a service for secure public safety device networks, IEEE Commun. Mag. 54 (2016) 47–53, https://doi.org/10.1109/mcom.2016.7452265.
[12] H. Saevanee, N. Clarke, S. Furnell, V. Biscione, Continuous user authentication using multi-modal biometrics, Comput. Secur. 53 (2015) 234–246, https://doi.org/10.1016/j.cose.2015.06.001.
[13] D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M. Freire, P.R.M. Inácio, Security issues in cloud environments: a survey, Int. J. Inf. Secur. 13 (2014) 113–170, https://doi.org/10.1007/s10207-013-0208-7.
[14] B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Secur. Priv. 9 (2011) 50–57, https://doi.org/10.1109/MSP.2010.115.
[15] A. Khalil, M. Khreishah Azeem, Consolidated Identity Management System for secure mobile cloud computing, Comput. Networks. 65 (2014) 99–110, https://doi.org/10.1016/j.comnet.2014.03.015.
[16] A.P. Méndez, R.M. López, G.L. Millán, Providing efficient SSO to cloud service access in AAA-based identity federations, Futur. Gener. Comput. Syst. 58 (2016) 13–28, https://doi.org/10.1016/j.future.2015.12.002.
[17] J.F. González, M.C. Rodriguez, M.L. Nistal, L.A. Rifón, Reverse OAuth: a solution to achieve delegated authorizations in single sign-on e-learning systems, Comput. Secur. 28 (2009) 843–856, https://doi.org/10.1016/j.cose.2009.06.002.
[18] U. Habiba, R. Masood, M.A. Shibli, M.A. Niazi, Cloud identity management security issues & solutions: a taxonomy, Complex Adapt. Syst. Model. 2 (2014), https://doi.org/10.1186/s40294-014-0005-9.
[19] I. Indu, P.M. Rubesh Anand, V. Bhaskar, Encrypted token based authentication with adapted SAML technology for cloud web services, J. Netw. Comput. Appl. 99 (2017) 131–145, https://doi.org/10.1016/j.jnca.2017.10.001.

[20] A.N. Khan, M.L.M. Kiah, S.A. Madani, M. Ali, A.U.R. Khan, S. Shamshirband, Incremental proxy re-encryption scheme for mobile cloud computing environment, J. Supercomput. 68 (2014) 624–651, https://doi.org/10.1007/s11227-013-1055-z.
[21] I. Indu, P.M. Rubesh Anand, S.P. Shaji, Secure file sharing mechanism and key management for mobile cloud computing environment, Indian J. Sci. Technol. 9 (2016), https://doi.org/10.17485/ijst/2016/v9i48/89496.
[22] M.A. Khan, A survey of security issues for cloud computing, J. Netw. Comput. Appl. 71 (2016) 11–29, https://doi.org/10.1016/j.jnca.2016.05.010.
[23] R. Jiang, X. Wu, B. Bhargava, SDSS-MAC: secure data sharing scheme in multi-authority cloud storage systems, Comput. Secur. 62 (2016) 193–212, https://doi.org/10.1016/j.cose.2016.07.007.
[24] S. Wang, J. Zhou, J.K. Liu, J. Yu, J. Chen, W. Xie, An efficient file hierarchy attribute-based encryption scheme in cloud computing, IEEE Trans. Inf. Forensics Secur. 11 (2016) 1265–1277, https://doi.org/10.1109/tifs.2016.2523941.
[25] Y. Zhu, D. Huang, C.-J. Hu, X. Wang, From RBAC to ABAC: constructing flexible data access control for cloud storage services, IEEE Trans. Serv. Comput. 8 (2015) 601–616, https://doi.org/10.1109/tsc.2014.2363474.
[26] J. Shen, T. Zhou, X. Chen, J. Li, W. Susilo, Anonymous and traceable group data sharing in cloud computing, IEEE Trans. Inf. Forensics Secur. 13 (2018) 912–925, https://doi.org/10.1109/TIFS.2017.2774439.
[27] Y. Zhang, D. Zheng, Q. Li, J. Li, H. Li, Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing, Secur. Commun. Networks. 9 (2016), https://doi.org/10.1002/sec.1574.
[28] N. Saxena, B.J. Choi, R. Lu, Authentication and authorization scheme for various user roles and devices in smart grid, IEEE Trans. Inf. Forensics Secur. 11 (2016) 907–921, https://doi.org/10.1109/tifs.2015.2512525.
[29] H. Wang, D. He, S. Tang, Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud, IEEE Trans. Inf. Forensics Secur. 11 (2016) 1165–1176, https://doi.org/10.1109/tifs.2016.2520886.
[30] I. Indu, P.M. Rubesh Anand, Identity and access management for cloud web services, IEEE Recent Adv. Intell. Comput. Syst. (2015), https://doi.org/10.1109/RAICS.2015.7488450.
[31] P.M. Rubesh Anand, V. Bhaskar, A unified trust management strategy for content sharing in Peer-to-Peer networks, Appl. Math. Model. 37 (2013) 1992–2007, https://doi.org/10.1016/j.apm.2012.04.050.
[32] Z. Wang, D. Huang, Y. Zhu, B. Li, C.J. Chung, Efficient attribute-based comparable data access control, IEEE Trans. Comput. 64 (2015) 3430–3443, https://doi.org/10.1109/TC.2015.2401033.
[33] H. Nicanfar, S. Member, P. Jokar, S. Member, K. Beznosov, V.C.M. Leung, Efficient authentication and key management mechanisms for smart grid communications, IEEE Sys. Jou. 8 (2014) 629–640.
[34] J. Li, X. Huang, J. Li, X. Chen, Y. Xiang, Securely outsourcing attribute-based encryption with checkability, IEEE Trans. Parallel Distrib. Syst. 25 (2014) 2201–2210, https://doi.org/10.1109/TPDS.2013.271.
[35] Z. Yan, M. Wang, Y. Li, Encrypted data management with deduplication in cloud computing, IEEE Cloud Comput. (2016) 28–35.
[36] L. Zhou, V. Varadharajan, M. Hitchens, Trust enhanced cryptographic role-based access control for secure cloud data storage, IEEE Trans. Inf. Forensics Secur. 10 (2015) 2381–2395, https://doi.org/10.1109/TIFS.2015.2455952.
[37] X. Yao, H. Liu, H. Ning, L.T. Yang, Y. Xiang, Anonymous credential-based access control scheme for clouds, IEEE Cloud Comput. 2 (2015) 34–43, https://doi.org/10.1109/MCC.2015.79.
[38] Q. Liu, G. Wang, J. Wu, Secure and privacy preserving keyword searching for cloud storage services, J. Netw. Comput. Appl. 35 (2012) 927–933, https://doi.org/10.1016/j.jnca.2011.03.010.
[39] D.R. dos Santos, R. Marinho, G.R. Schmitt, C.M. Westphall, C.B. Westphall, A framework and risk assessment approaches for risk-based access control in the cloud, J. Netw. Comput. Appl. 74 (2016) 86–97, https://doi.org/10.1016/j.jnca.2016.08.013.
[40] N. Garg, S. Bawa, Comparative analysis of cloud data integrity auditing protocols, J. Netw. Comput. Appl. 66 (2016) 17–32, https://doi.org/10.1016/j.jnca.2016.03.010.
[41] S.K. Sood, A combined approach to ensure data security in cloud computing, J. Netw. Comput. Appl. 35 (2012) 1831–1838, https://doi.org/10.1016/j.jnca.2012.07.007.
[42] I. Indu, P.M.R. Anand, Hybrid authentication and authorization model for web based applications, in: Proc. 2016 IEEE Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2016, (2016). doi:10.1109/WiSPNET.2016.7566324.
[43] F. Chen, T. Xiang, Y. Yang, S.S.M. Chow, Secure cloud storage meets with secure network coding, IEEE Trans. on Comput. 65 (2016) 1936–1948.
[44] F. Zhang, S. Member, K. Hwang, L. Fellow, S.U. Khan, S. Member, Q.M. Malluhi, Skyline discovery and composition of multi-cloud mashup services, IEEE Trans. Serv. Comput. 9 (2016) 72–83.
[45] S. Lin, R. Zhang, H. Ma, M. Wang, Revisiting attribute-based encryption with verifiable outsourced decryption, IEEE Trans. Inf. Forensics Secur. 10 (2015) 2119–2130, https://doi.org/10.1109/TIFS.2015.2449264.
[46] A.A. Almutairi, A. Ghafoor, Risk-aware virtual resource management for multitenant cloud datacenters, IEEE Cloud Comput. 1 (2014) 34–44, https://doi.org/10.1109/MCC.2014.63.
[47] Z. Zhu, R. Jiang, A secure anti-collusion data sharing scheme for dynamic groups in the cloud, IEEE Trans. Parallel Distrib. Syst. 27 (2016) 40–50, https://doi.org/10.1109/TPDS.2015.2388446.
[48] H. He, R. Li, X. Dong, Z. Zhang, Secure, efficient and fine-grained data access control mechanism for P2P storage cloud, IEEE Trans. Cloud Comput. 2 (2014) 471–484, https://doi.org/10.1109/TCC.2014.2378788.
[49] H. Wang, Identity-based distributed provable data possession in multicloud storage, IEEE Trans. Serv. Comput. 8 (2015) 328–340, https://doi.org/10.1109/TSC.2014.1.
[50] Z. Liu, X. Chen, J. Yang, C. Jia, I. You, New order preserving encryption model for outsourced databases in cloud environments, J. Netw. Comput. Appl. 59 (2016) 198–207, https://doi.org/10.1016/j.jnca.2014.07.001.
[51] S.S. Manvi, G. Krishna Shyam, Resource management for Infrastructure as a Service (IaaS) in cloud computing: a survey, J. Netw. Comput. Appl. 41 (2014) 424–440, https://doi.org/10.1016/j.jnca.2013.10.004.
[52] S. Iqbal, M.L. Mat Kiah, B. Dhaghighi, M. Hussain, S. Khan, M.K. Khan, K.K. Raymond Choo, On cloud security attacks: a taxonomy and intrusion detection and prevention as a service, J. Netw. Comput. Appl. 74 (2016) 98–120, https://doi.org/10.1016/j.jnca.2016.08.016.
[53] B. Dong, Q. Zheng, F. Tian, K.M. Chao, R. Ma, R. Anane, An optimized approach for storing and accessing small files on cloud storage, J. Netw. Comput. Appl. 35 (2012) 1847–1862, https://doi.org/10.1016/j.jnca.2012.07.009.
[54] H. Liu, H. Ning, Q. Xiong, L.T. Yang, Shared authority based privacy-preserving authentication protocol in cloud computing, IEEE Trans. Parallel Distrib. Syst. 26 (2015) 241–251, https://doi.org/10.1109/TPDS.2014.2308218.
[55] C.A. Atwood, R.C. Goebbert, J.A. Calahan, T.V. Hromadka, T.M. Proue, W. Monceaux, J. Hirata, Secure web-based access for productive supercomputing, Comput. Sci. Eng. 18 (2016) 63–72, https://doi.org/10.1109/MCSE.2015.134.
[56] J. Liu, M. Au, X. Huang, R. Lu, J. Li, Fine-grained two-factor access control for web-based cloud computing services, IEEE Trans. Inf. Forensics Secur. 6013 (2015) 1, https://doi.org/10.1109/TIFS.2015.2493983.
[57] V. Chang, M. Ramachandran, Towards achieving data security with the cloud computing adoption framework, IEEE Trans. Serv. Comput. 9 (2016) 138–151.
[58] C.A. Lee, Cloud federation management and beyond: requirements, relevant standards, and gaps, IEEE Cloud Comput. 3 (2016) 42–49, https://doi.org/10.1109/MCC.2016.15.
[59] Yuanchao Shu, Y.J. Gu, Jiming Chen, Y. Shu, J. Chen, Dynamic authentication with sensory information for the access control systems, IEEE Trans. Parallel Distrib. Syst. 25 (2014) 427–436, https://doi.org/10.1109/TPDS.2013.153.
[60] C. Lyu, S.F. Sun, Y. Zhang, A. Pande, H. Lu, D. Gu, Privacy-preserving data sharing scheme over cloud for social applications, J. Netw. Comput. Appl. 74 (2016) 44–55, https://doi.org/10.1016/j.jnca.2016.08.006.
[61] A. Waqar, A. Raza, H. Abbas, M. Khurram Khan, A framework for preservation of cloud users data privacy using dynamic reconstruction of metadata, J. Netw. Comput. Appl. 36 (2013) 235–248, https://doi.org/10.1016/j.jnca.2012.09.001.
[62] Z. Yang, X. Liu, X.S. Jia Shen, Time-domain attribute-based access control for cloud-based video content sharing: a cryptographic approach, IEEE Trans. Multimed. 18 (2016) 940–950, https://doi.org/10.1109/TMM.2016.2535728.
[63] J. Zhang, H. Huang, X. Wang, Resource provision algorithms in cloud computing: a survey, J. Netw. Comput. Appl. 64 (2016) 23–42, https://doi.org/10.1016/j.jnca.2015.12.018.
[64] S. Masdari, Z. ValiKardan, S.I. Shahi Azar, Towards workflow scheduling in cloud computing: a comprehensive analysis, J. Netw. Comput. Appl. 66 (2016) 64–82, https://doi.org/10.1016/j.jnca.2016.01.018.
[65] A. Siddiqa, I.A.T. Hashem, I. Yaqoob, M. Marjani, S. Shamshirband, A. Gani, F. Nasaruddin, A survey of big data management: taxonomy and state-of-the-art, J. Netw. Comput. Appl. 71 (2016) 151–166, https://doi.org/10.1016/j.jnca.2016.04.008.
[66] J. Li, X. Chen, M. Li, J. Li, P.P.C. Lee, W. Lou, Secure deduplication with efficient and reliable convergent key management, IEEE Trans. Parallel Distrib. Syst. 25 (2014) 1615–1625, https://doi.org/10.1109/TPDS.2013.284.
[67] S.A.H. Tabatabaei, O. Ur-rehman, N. Zivic, C. Ruland, Secure and robust two-phase image authentication, IEEE Trans. Multimed. 17 (2015) 945–956, https://doi.org/10.1109/TMM.2015.2432672.
[68] J. Xu, Q. Wen, W. Li, Z. Jin, Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing, IEEE Trans. Parallel Distrib. Syst. 27 (2016) 119–129, https://doi.org/10.1109/TPDS.2015.2392752.
[69] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, G. Ferrari, S. Member, IoT-OAS: an OAuth-based authorization service architecture for secure services in IoT scenarios, IEEE Sens. Jou. 15 (2015) 1224–1234.
[70] W. Sun, S. Member, S. Yu, Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud, IEEE Trans. Para. Dist. Syst. 27 (2016) 1187–1198.
[71] A. Gani, A. Siddiqa, S. Shamshirband, F. Hanum, A survey on indexing techniques for big data: taxonomy and performance evaluation, Knowl. Inf. Syst. 46 (2016) 241–284, https://doi.org/10.1007/s10115-015-0830-y.
[72] J. Shuja, A. Gani, S. Shamshirband, R.W. Ahmad, K. Bilal, Sustainable Cloud Data Centers: a survey of enabling techniques and technologies, Renew. Sustain. Energy Rev. 62 (2016) 195–214, https://doi.org/10.1016/j.rser.2016.04.034.
[73] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, S. Shamshirband, Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications, Egypt. Inf. J. 18 (2017) 113–122, https://doi.org/10.1016/j.eij.2016.11.001.
[74] A.N. Khan, M.L. Mat Kiah, M. Ali, S. Shamshirband, A. Ur R. Khan, A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach, J. Grid Comput. 13 (2015) 651–675, https://doi.org/10.1007/s10723-015-9352-9.
[75] A.N. Khan, M.L.M. Kiah, M. Ali, S.A. Madani, A. Ur R. Khan, S. Shamshirband, BSS: block-based sharing scheme for secure data storage services in mobile cloud environment, J. Supercomput. 70 (2014) 946–976, https://doi.org/10.1007/s11227-014-1269-8.

[76] O.M. Achim, F. Pop, V. Cristea, Reputation based selection for services in cloud environments, in: Proc. - 2011 Int. Conf. Network-Based Inf. Syst. NBiS 2011, 2011: pp. 268–273. doi:10.1109/NBiS.2011.46.
[77] D. Ionică, N. Popescu, D. Popescu, F. Pop, Cyber Defence Capabilities in Complex Networks, in: Internet of Everything, Springer, Singapore, 2018, pp. 217–231.
[78] H. Wang, Z. Zheng, Y. Wang, Cloud-aided online/offline ciphertext-policy attribute-based encryption in the standard model, Int. J. Grid Util. Comput. 8 (2017) 211–221, https://doi.org/10.1504/IJGUC.2017.10008770.
[79] D.C. Mansour Christopher, Security challenges in the internet of things, Int. J. Space-Based Situated Comput. 5 (2015) 141–149, https://doi.org/10.1504/IJSSC.2015.070945.
[80] Sailpoint IDM. [Online] https://www.sailpoint.com/identity-management-solutions/.
[81] IBM Cloud Services. [Online] https://www.ibm.com/cloud-computing/in-en/services/cloud-managed-services/.
[82] Oracle Cloud Services. [Online] https://www.oracle.com/cloud/index.html.
[83] RSA Security Suite. [Online] https://www.rsa.com/en-us/products/rsa-securid-suite.html.
[84] Coresecurity IAM. [Online] https://www.coresecurity.com/iam-products.