



Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing

Amjad Alsirhani, Mohamed Ezz and Ayman Mohamed Mostafa*

College of Computer and Information Sciences, Jouf University, Sakaka, 72314, Saudi Arabia *Corresponding Author: Ayman Mohamed Mostafa. Email: amhassane@ju.edu.sa Received: 02 November 2021; Accepted: 03 December 2021

Abstract: Identity management is based on the creation and management of user identities for granting access to the cloud resources based on the user attributes. The cloud identity and access management (IAM) grants the authorization to the end-users to perform different actions on the specified cloud resources. The authorizations in the IAM are grouped into roles instead of granting them directly to the end-users. Due to the multiplicity of cloud locations where data resides and due to the lack of a centralized user authority for granting or denying cloud user requests, there must be several security strategies and models to overcome these issues. Another major concern in IAM services is the excessive or the lack of access level to different users with previously granted authorizations. This paper proposes a comprehensive review of security services and threats. Based on the presented services and threats, advanced frameworks for IAM that provide authentication mechanisms in public and private cloud platforms. A threat model has been applied to validate the proposed authentication frameworks with different security threats. The proposed models proved high efficiency in protecting cloud platforms from insider attacks, single sign-on failure, brute force attacks, denial of service, user privacy threats, and data privacy threats.

Keywords: Identity management; cloud computing; security threats and authentication mechanisms

1 Introduction

Cloud Computing is considered the most commonly used method for sharing information, resources, data, networks, and services for multiple users. The main objective of cloud computing is to build a service environment with authentication capabilities and low-cost facilities based on different deployment models such as infrastructure, platform, and software as a service [1]. Authentication mechanisms in cloud services are divided into physical security and digital security mechanisms [2]. Physical security mechanisms rely on the nature of using biometric authentication, such as face recognition, fingerprint recognition, and iris detection. Digital security mechanisms are based on passwords credentials, single sign-on (SSO), and multifactor authentication that is considered the most commonly used authentication method for access management in cloud computing. Different security standards such as access control



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

mechanisms and access control governance are applied to overcome cloud security problems [3]. Identity and access management (IAM) is considered the best method for measuring the security of cloud services. As presented in [4], a two-factor authentication framework for authenticating users accessing private cloud services is improved. The framework aims to send a secret QR code for each user using the Open Stack tool. Another method for improving the authentications levels in cloud computing is proposed in [5], where different security layers are applied using simple password, graphical password and biometrics method.

These methods lack integration and harmony between each other. Authentication methods must ensure flexibility and efficiency while ensuring the security of cloud computing services. Building cloud authentication frameworks for maintaining identity and access management (IAM) with high flexibility and efficiency is considered a challenging task. The contribution of our paper is as follows:

- Providing a comprehensive comparison of current cloud security services with their corresponding security threats.
- Providing an identity-as-a-service (IdaaS) authentication algorithm based on a unified framework using single sign-on (SSO) and OAuth2 security mechanisms.
- Applying a multi-layer security mechanism using cryptography, hash functions and SSO between cloud provider (CP) and directory provider (DP).
- Based on the proposed IdaaS, two authentication frameworks are applied for public and private clouds to authenticate and validate user identities.
- Proposing a comparative analysis between the presented cloud frameworks and other cloud deployment models.
- Providing a threat model for validating the proposed IAM frameworks by comparing recent cloud security models with proposed frameworks.

The organization of the paper is as follows: Section 2 presents literature review. Section 3 proposes advanced Identity-as-a-Service (IdaaS) authentication algorithm. Section 4 presents cloud authentication frameworks for public and private clouds. Section 5 proposes a threat model for validating proposed IAM frameworks with current security threats and attacks. The paper is concluded in Section 6.

2 Literature Review

The primary component of IAM system is based on the authentication and authorization processes. The authentication process is used to ensure that the end-users are authentic, while the authorization process is based on granting or denying cloud resources based on the user authorities. As presented in [6], an overall evaluation for IAM was proposed with different evaluation.

The proposed work started that different identity management characteristics must be provided to ensure the efficiency of IAM. As presented in [7], various techniques of identity management system on cloud are described and analyzed. The authors made a comparison that presented advantages and disadvantages for each presented authentication technique. Identity management in a hybrid cloud was presented in [8]. The paper is based on sharing data and information for different users between different servers in the same network. Security risks, authentication, and critical management of cloud computing are evaluated. The remaining related works focus on presenting recent security models for identity and access management (IAM) along with their security architectures and security issues. A comprehensive comparison of current cloud security services with their corresponding security threats are proposed.

2.1 IAM Service Models

Different IAM service models have been deployed and proposed to evaluate the identity and access management performance based data storage, storage services, and privacy of stored data. The data storage of cloud computing user identities is proposed in [9]. An identity-based proxy re-encryption is used to manage files. There are many drawbacks where the central authority is responsible for granting access to data. Moreover, the proposed schemes are insecure against some types of closure attacks. Organizational requirements of the present century are fulfilled by cloud computing. IaaS, PaaS, SaaS, and multi-tenancy models are used to assist in the availability of cost of cloud computing. However, the flaw in these models is privacy and security risks. To cope up with these flaws, identity and access management is designed to minimize the risks. This paper proposes an integrated identity system and attribute-based access management system for cloud computing. Authentication and attribute-based control are used as improved security for cloud web services [10].

Based on the stored data on cloud, several methods are applied to monitor the integrity of users' profiles. As shown in [11], a database-auditing model was proposed to ensure and verify cloud service providers for maintaining the integrity and privacy of cloud storage systems. Many organizations shifted their services to the cloud platform in recent years. Adopting a cloud platform for storage raise question regarding user privacy control. The traditional method is based on using privacy control such as username and password that cannot protect the users from virtualization attacks, sniffing, and phishing attacks. As presented in [12], a method was proposed to extend the existing claim-based identity management system for providing a more secure way to access cloud services.

2.2 IAM Architectures

The IAM architectures provide a set of policies, standards, procedures, and activities that can clarify the goals and objectives of the cloud identity services. Different workflows are defined with security issues to maintain the privacy of cloud data services. An Open ID intrusion tolerant identity provider was presented in [13] with a proposed architecture implemented to share communication and memory between services and proxies on the level of Hypervisor. The proposed model translates the intrusion to actions and keeps the user information in separate compartments. A cloud identity management of Open Stack platform was proposed in [14] to authenticate users and ensure that the transmitted usernames, passwords are in encrypted form over the network. As shown in [15], a multi-tier infrastructure was presented with a centralized identity and access management. The first step is to identify the crucial requirements, then propose a feasible solution accordingly and finally, the infrastructure addresses the required outputs.

Dealing with the security issues in the cloud identity and access management is considered a crucial factor. As presented in [16], a complete strategy was proposed to solve issues in the cloud regarding user information. This strategy uses the service technology to have a standardized output. The study is beneficial in providing scalability, autonomy, standardization, and a systematic approach. The primary issue is that if the user's data is kept secure, it can be encrypted for processing. User Authentication is considered another major significant problem in cloud service architectures. If there are any defects or errors in the design of the cloud architecture, there will be high probability for losing sensitive data. A cloud user identity management protocol is proposed in [17] based on the block-chain technology. The protocol is considered an improved version of consolidation identity management (CIDM) that depends on third-party policies.

2.3 IAM Security Issues

The IAM security procedures provide different policies and roles for managing digital user identities for accessing data, resources, and systems whether on public, private, or hybrid clouds. Based on the IAM policies, organizations can mitigate risks and threats with the ability to improve the privacy of cloud data resources. As presented in [18], a comprehensive review on cloud computing security, challenges, threats, and proposed solutions has been proposed. The study focuses on three types of cloud computing challenges, including authentication, authorization, and integrity with data storage issues and virtualization security issues. The trust management in cloud computing has been presented in [19] to deal with suspicious user comments in order to measure the impact of these comments on the level of trust.

As presented in [20], different protocols have been proposed to handle the secrecy, integrity and availability in cloud resources. A two-layer method was applied using authentication and cryptography in order to conceal user identities on the cloud server. Protecting user digital identities is considered another major concern in securing cloud frameworks. As proposed in [21], cross-border data using different approaches from US, Europe, and Australia have been used to improve the protection of user identities. Another model for maintaining the privacy of identity management was presented in [22]. The proposed model helps in enhancing the cloud services with regard to different evaluation criteria such as user-friendly, obfuscation, trust, data quality, and transparency.

Securing identity management in Mobile cloud computing is considered a high security concern due to the wide use of Mobile applications in accessing cloud computing services. As presented in [23], a new IAM model has been proposed to fix the major risks and vulnerabilities in cloud identity management. The proposed model was evaluated with the existing model by comparing the ability of both models to avoid vulnerabilities caused by server penetrations. As presented in [24], a secure IAM was applied for protecting mobile cloud computing from attacks using authentication steps where a token is generated for every user request by giving the username. A security question will be sent to the user by the Cloud Service Provider (CSP) to validate the token. Therefore, the token is used to validate the user instead of using passwords. Another scheme for protecting the privacy of identity management was presented in [25] where an authentication method using a one-time password and ZKP is used. The drawback in this scheme is that a single credential is used for all cloud services that may cause penetration from attackers.

As presented in [26], a security framework is applied as a service for IAM based on the major security parameters: secrecy, integrity, and availability. The authors implemented the framework as a collection of virtual machines in the cloud. Another model for securing and managing user identities was presented in [27] where a single sign-on (SSO) model was implemented to allow a single user to access several resources using the same password. An evaluation of a single sign-on security failure was presented in [28] where service failures occur due to the limitation in protecting information. Cloud computing helps in optimizing the data and privacy of the owner who assess security risks. The paper focuses on the authorization of SSO and how it affects the security, risks and privacy in cloud computing. Another methodology for securing identity management was presented in [29] where a user authentication model was proposed based on a set of policies.

One of the recent models for evaluating risk management in IAM was presented in [30]. The authors proposed a platform that focuses on auditing user identities. The authors implemented the platform using Oracle identity and access management tool that is used after authenticating and authorizing users. Encryption techniques are also considered major significant methods for protecting the secrecy of user identities. Different research papers highlighted the role of cryptography in protecting and maintaining user identities. As presented in [31], an identity-based encryption scheme was implemented to secure user data and reduce the computation cost in searching over the encrypted data on the cloud server. As shown in [32], an encryption tool was implemented by combining public-key encryption with identity-based encryption to create a new authentic encryption technique. As proposed in [33], a checking protocol for cloud data integrity was implemented to enhance the checking mechanism by eliminating the complexity in certificate management. A prototype was applied to measure the performance of the proposed protocol and prove its practicability.

One of the recent ways for maintaining the cloud data profiles was presented in [34] where encryption techniques are applied to the cloud data to maintain its privacy and integrity. Based on this method, the sharing of data among multiple users can be more secure. Another recent model for auditing stored data on the cloud was presented in [35]. In the proposed model, the revoking process of user authorizations can cause overhead on cloud servers. Therefore, an identity-based encryption technique was applied to distinguish between revoked and non-revoked users. As shown in [36], another auditing mechanism was

applied to preserve the privacy of cloud-stored data by authorizing users using encryption techniques. The new model used public-key certificate to identify users on the cloud.

Blockchain is considered a revolutionary technology in protecting data based on a decentralized manner. As shown in [37,38], the Blockchain technology played a vital role in analyzing and securing identity management systems. As proposed in [37], an evaluation for identifying the best identity management solution using Blockchain was applied. Different open source tools of Blockchain are used to analyze user identity profiles. In [38], the authors concentrated on the role of Blockchain in protecting the user identities on cloud where the Blockchain can be applied to IAM, data storage and processing tasks. As presented in Tab. 1, a comparative analysis for the previous literature review has been applied. The objectives, cloud security services, and major threats for each research are highlighted to provide a complete view of most of the breaches and threats that can affect the security of cloud computing.

Table 1: Summary	v of cloud	security	services	and threats
------------------	------------	----------	----------	-------------

• .

.

1.1

0 1 1

Ref#	Objective	Security service	Security threat
[6]	Review of privacy issues in cloud identity management	 Single sign-on (SSO) Security assertion markup language Authentication Authorization 	 Lack of confidentiality Distributed denial of service Malicious attacks Injection attacks
[7]	Federated identity management for implementing OpenStack cloud	• Multi-layer security Service	Malicious cloud serverThird party verifier
[8]	Revising security risks in cloud environment	CryptographyDigital signature	• Single sign-on overhead
[<mark>9</mark>]	Providing attribute and access management for cloud services	 Integrated identity management 	 Privacy risks Security risks
[10]	Identity-based data storage in cloud computing	• Re-encryption model	• Inside and outside cloud attacks
[11]	Maintaining the integrity and privacy of cloud storage systems	CryptographyAuditing	• Sensitive data threats
[12]	Applying a claim-based model for identity management	• Security assertion markup language (SAML)	Virtualization attacksPhishing attacks
[13]	Providing intrusion tolerant framework for identity management	 Hypervisor Authentication and authorization controls Open ID 	 Distributed denial of service (DDoS) Malicious attacks Injection attacks
[14]	Proposing open stack model for authentication in identity management	 Host-based access control (HBAC) Role-based access control (RBAC) Kerberos 	 Vulnerabilities during transmission Eavesdropping on certification information Denial of service (DoS)

Ref#	Objective	Security service	Security threat
[15]	Managing identities in multi-tier cloud infrastructure	AuthenticationAccess management	• Access violations
[16]	Exploring security issues for accessing cloud resources	AuthenticationAuthorization	• Data loss
[17]	Providing a cloud framework for identity management.	• JSON web token (JWT) in OAuth 2.0	• User identity authentication
[18]	Comprehensive review on identity management challenges, issues, threats and solutions	• Cryptography and other security issues	User privacy threatUser information theftMisuse
[19]	Proposing a trust management architecture for validating cloud providers	 Cryptography Intrusion detection systems Authentication Authorization Policies and audit 	 Distributed denial of service Malicious rater Malicious participants attack Vulnerabilities and fraud
[20]	Handling CIA in cloud resources for concealing cloud user identities	AuthenticationCryptography	• Denial of service (DoS) attacks
[21]	Dealing with cross border data in cloud computing	• Authentication	Information disclosure
[22]	Providing a model for maintaining the privacy of personal information	PoliciesCryptography	• Sensitive data threats
[23]	Providing a third part identity management system	CryptographyAccess control	Server compromiseMobile compromiseTraffic interception
[24]	Securing identity management based on authentication and privacy	 Zero knowledge proof (ZKP) Token verification 	Server compromise
[25]	Authenticating users based on their attributes	 Authentication Zero knowledge proof (ZKP) One-time password 	• Sensitive data threat
[26]	Providing identity management for security as a service cloud	AuthenticationAuthorization	• Sensitive data threat
[27]	Proposing a model for managing user identities using multi-agent systems	AuthenticationAuthorizationCryptography	 Distributed denial of service Injection attacks Vulnerabilities and fraud

(Continued)

Ref#	Objective	Security service	Security threat
[28]	Evaluating single sign-on authorization	 Security token 	• Single sign-on failure
[29]	Providing an authentication model for controlling cloud user identities	PolicyAuthentication	• User privacy threat
[30]	Providing a multi-layer approach for risk management	AuthenticationAuthorization	• User privacy threat
[31]	Implementing a secured model for efficient search on cloud data	• Cryptography	 Chosen identity attack Chosen cipher text attack
[32]	Providing identity based encryption for cloud data	 Cryptography 	 User privacy threat
[33]	Proposing a cloud auditing model for verifying user integrity data	• Cryptography	• User privacy threat
[34]	Maintaining user profiles using encryption techniques	• Cryptography	• User privacy threat
[35]	Providing an identity-based encryption technique to distinguish between revoked and non-revoked users	• Cryptography	User privacy threatSensitive data threats
[36]	Preserving the privacy of cloud stored data using encryption techniques	• Cryptography	 User identity disclosure Denial of service attack Single-manager abuse
[37]	Analyzing IAM systems using blockchain	Blockchain	• User privacy threat
[38]	Protecting and controlling identities using blockchain	• Blockchain	• User identity information misuse

3 Advanced Identity-as-a-Service (IdaaS) Authentication Algorithm

Due to the multiplicity of cloud locations where data resides and due to the lack of a centralized user authority for granting or denying cloud user requests, there must be several security strategies and models to overcome these issues. Another major concern in IAM services is the excessive or the lack of access level to different users with previously granted authorizations. Based on the information extracted from Tab. 1, the most common security threats in cloud computing applications are data privacy threats, malicious participants' threats, user information theft, denial of service, and sensitive data threats. These threats aim to compromise sensitive information from cloud providers' resources to modify user identity profiles. In addition to the previous threats, maintaining the authentication and privacy of user identities is considered one of the most important security trends in cloud computing [39].

Recent authentication mechanisms in a cloud environment are based on single-sign-on (SSO) and OAuth [1]. In single-sign-on (SSO), the user requests access to the target application that directs the request to the identity provider (IdP). The IAM systems grant/deny the request and direct it to the target application again.

When the user navigates from one cloud application to another, the IdP verifies the user to the new application. The OAuth and its new version OAuth2 are based on a one-way authentication method into which the user sends a request to the service provider. The service provider directs the request to an authentication server that authenticates the user and sends the request back to the service providing for granting or denying the user request. The objective of the proposed IAM framework and algorithm is to facilitate and enhance the authentication of user identities in cloud computing applications by merging the SSO and OAuth2 features on a unified framework. The enhanced framework is based on an identity-as-a-service methodology with an enhanced algorithm for authenticating user identities between directory provider (DP), cloud provider (CP), and identity-as-a-service (IdaaS) provider that are belonging to the same organization. As presented in Fig. 1, an enhanced framework is proposed for maintaining the authenticity of users, eliminating malicious participants' threats, and obtaining the privacy of data.

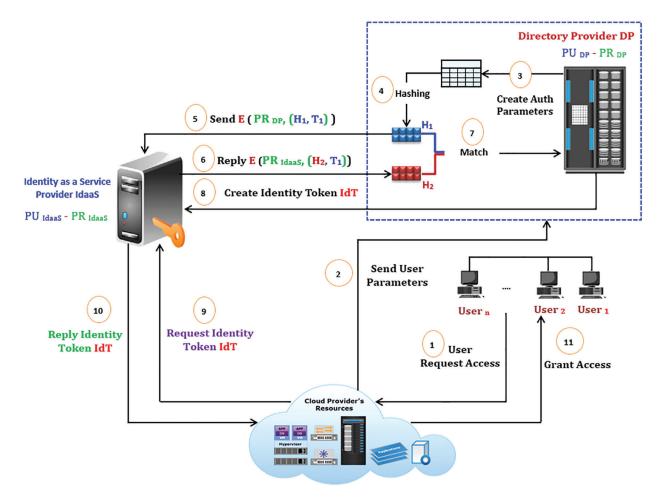


Figure 1: Identity-as-a-service authentication framework

The framework authenticates and handles the user registration using a single-sign-on (SSO) in cloud provider's resources through a directory provider (DP) and identity-as-a-service (IdaaS) provider. The role of each participating entities is as follows:

• Directory provider (DP): is considered the central authority for storing user parameters, creating authentication parameters and generating identity tokens for cloud users.

- Identity as a-service (IdaaS) provider: is considered the verification authority that validates the user identity, credentials and finally sends them to the cloud service provider (CP).
- Cloud Provider (CP): is considered the resources' provider to cloud users for different computing resources.

Once the user performs a single-sign on (SSO) to the cloud resource, an interaction between the triple: DP, IdaaS, and cloud provider's resources is established to authenticate the user and maintain the privacy of data. As presented in Fig. 1, the users who request access to the cloud provider (CP) are already registered users where their parameters are stored in the directory provider (DP). The role of the DP is to create authentication parameter for each user. The DP has its own public and private keys (PU_{DP} , PR_{DP}) where the CP encrypts the user parameters using the public key of the DP (PU_{DP}). Once the DP received the message, a decryption process using (PR_{DP}) is applied to match the decrypted user parameters with the stored ones. If both parameters are matched, the DP creates the authentication parameter for each user.

In addition, an authentication between both DP and IdaaS is applied to overcome the man-in-the-middle attack problem that may compromise the transmission between DP and IdaaS. The overall mechanism of the framework is presented in Algorithm 1, where several security measures are established to authenticate the user.

Algorithm 1: Id-as-a-Service Authentication
Initialize IdaaS Provider
Initialize Directory Provider DP
Generate PU _{DP} -PR _{DP}
Initialize Cloud Provider CP
Initialize Registration Phase
User i ← Register User i Attributes
DP ← Generate User i Auth Parameters
DP \leftarrow Perform Hashing H ₁
Encrypt (PR $_{DP}$, (H ₁ , T ₁))
IdaaS \leftarrow Perform Hashing H ₂
Decrypt (PU $_{DP}$, (H ₂ , T ₁))
DP ← Apply Matching Process
If $If H_1 \neq H_2$ Then
Raise Alarm
Discard H ₁ , H ₂
Else
DP \leftarrow Generate IdT
IdaaS ← Receive IdT
User $_{i}$ \leftarrow Send Access Request
$CP \leftarrow Receive Access Request$
$\mathbf{CP} \leftarrow \text{Request } \mathbf{IdT}$
IdaaS \leftarrow Reply IdT
CP ← Grant User i Access

The overall algorithm is divided into three main phases as follows:

Phase I: Initialization Phase

- Identity as-a-Service Provider (IdaaS): The IdaaS is initialized to communicate with the directory provider (DP) for creating the identity token (IdT) for registered users. The IdT is considered the second authentication factor for verifying user on the cloud and maintaining the privacy of cloud resources.
- **Directory Provider (DP)**: The DP is initialized by generating public and private keys PU_{DP} , PR_{DP} where the public key PU_{DP} is sent to the IdaaS for authenticating user identity. The DP is responsible for creating and storing authentication parameters and the identity token (IdT).
- Cloud Provider (CP): The CP is initialized to serve as an interoperability layer between the IdaaS and the users. The CP is responsible for providing cloud services and resources to the users.
- User Access: The user accesses to the cloud provider resources using his/her secret attributes. The cloud provider directs the user attributes to the DP that is considered as the central authority for handling users' profiles.

Phase II: Encryption and Authentication Phase

• Creating Authentication Parameters: Once the data is transmitted to the DP, the authentication parameters are created and hashed based on the following equation:

 $E(PR_{DP}, (H_1, T_1))$

where H_1 is the hash of the authentication parameters, T_1 is the timestamp of the message sent from the DP to the IdaaS. The overall message is encrypted using the DP private key PR _{DP} to prove the authentication of the sender.

• Generating H₂: The IdaaS validating the received message by decrypting the message using the DP public key PU _{DP} to obtain H₁. The decryption process is performed based on the following equation:

 $D(PU_{DP}, (H_1, T_1))$

The IdaaS creates H_2 and encrypts it with the private key PR_{IdaaS} . The hash H_2 is sent to the DP with the original timestamp T_1 to prove that the original message was not delayed. The encryption process is performed based on the following equation:

 $E(PR_{IdaaS}, (H_2, T_1))$

(3)

(2)

(1)

• Matching Process: the DP performs a matching process between both H₁ and H₂. If no match exists, an alarm will be raised and both H₁ and H₂ will be discarded as an evidence of an attack during transmission. Otherwise, the DP will create the user identity token (IdT). The generated identity token (IdT) is considered a one-time token that is used to login into the CP resources only once. Once the user finished executing his transactions on the CP services, the token is discarded. For every user request to the CP, a new unique token is generated. This can increase and maintain the secrecy and privacy on the cloud resources.

Phase III: Granting Access Phase

- Creating IdT: once the matching process is validated, the IdT is sent from the DP to the IdaaS that will be the leading layer for granting or denying the user request.
- User Request: the *user_i* performs a single sign-on (SSO) to the cloud provider (CP) for accessing cloud resources.

- **Request IdT:** The CP requests the IdT for *user_i* from the IdaaS.
- **Reply IdT:** The IdaaS replies the message by sending the IdT for *user_i* to the CP.
- Granting Access: The CP grants access to the user

4 Cloud Authentication Frameworks

Based on the IdaaS algorithm that has been presented, two authentication frameworks for public and private cloud are proposed to authenticate and validate user identities. The proposed frameworks are based on generating authentication or security token that can ensure the identity of the logging user.

4.1 Public Cloud Authentication Framework

In public cloud, the cloud infrastructure is applied for open user where data resides on the premises of the cloud provider. The public cloud can be managed and operated by businesses, governmental, or academic institutions [40]. Although public cloud can provide availability, flexibility, security with the addition of cost-reduction in storing and maintaining end users' data; there still several inadequate security requirements that can violate the transfer of resources to the public cloud. These security requirements are based on traditional methods such as access control and intrusion detection systems (IDSs) [41]. As presented in Fig. 2, an authentication framework for public cloud infrastructure is proposed based on the four components: identity provider (IdP), directory provider (DP), cloud service provider, and user. This framework verifies the identity of the user logging on to the cloud by generating an authentication token between the IdP and cloud service provider. The overall mechanism starts by sending the user a request to the cloud provider resources that directs the user credentials [*UID_i*, *UN_i*, *PW_i*] to the IdP. The verification procedure is executed as follows:

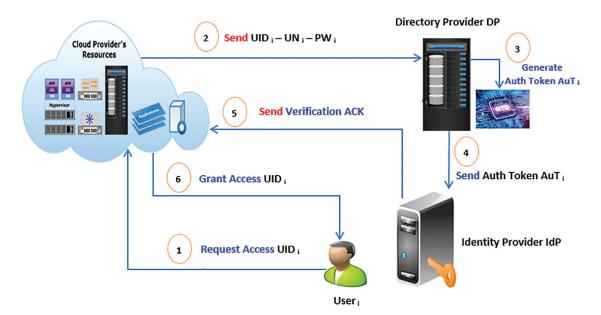


Figure 2: Public cloud authentication framework

- The DP generates an authentication token AuT_i for $user_i$ based on user attributes.
- The DP transmits the authentication token AuT_i to the IdP for verifying the logging user.
- The IdP sends a verification acknowledgement to the cloud service provider.

- The verification process between both IdP and cloud service provider is handled based on the authentication mechanisms presented between the IdaaS and DP in Algorithm 1. The secrecy and authentication between both IdP and cloud service provider must be maintained to eliminate security breaches during transmission.
- When the *user*_i requests access to the cloud resources using user attributes, the cloud service provider grants access to the user. If a *user*_k requests access to the cloud resources, there must be both security attributes $[UID_k, UN_k, PW_k]$ and authentication token AuT_k . If both parameters exist, the user is granted access; otherwise, access denied is raised.

4.2 Private Cloud Authentication Framework

Private cloud is directed for exclusive use of single organization where data can be managed and maintained on or off the organization premises. The security of private cloud is strongly dependent on daily interactions that must be monitored using intrusion detection systems (IDSs) and firewalls. The private cloud security mechanisms have an advantage over public cloud where public cloud forces user operations to a set of protocols and security rules that may affect the performance of the cloud. The private cloud can depend on a set of security countermeasures for maintaining both security and efficiency such as application security, auditing and identity management [42]. IAM provides effective security solutions for cloud systems using authentication, authorization, and automatic provisioning to guarantee that authorized users are allowed to access cloud systems [1]. As presented in Fig. 3, an authentication framework for private cloud is applied into which the user requests access to the resources of cloud service provider that directs the user attributes [*UID_i*, *UN_i*, *PW_i*] to the security token service (STS). The STS is similar to the directory provider (DP) in addition to the ability for identifying the lifetime of each identity token *IDT_k*. The verification procedure is executed as follows:

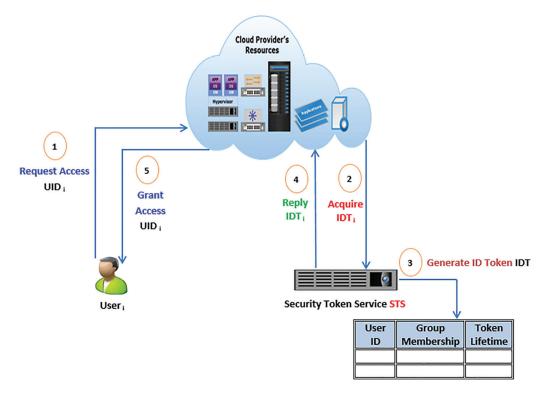


Figure 3: Private cloud authentication framework

- The cloud service provider requests the identity token *IDT_i* for the *user_i*.
- The STS generates an identity token IDT_i for $user_i$ based on the user attributes.
- The IDT_i is defined based on the following parameters:

- The user identity is stored based on the identity directed from the cloud provider.

- The lifetime of IDT_i is defined to determine the allowed validation time for the user to log into the cloud using the authentic token.

- The group membership identifies the allowed authorizations for the user to access cloud resources.

- The STS transmits the IDT_i to the cloud service provider for verifying the logging user.
- The verification process between both STS and cloud service provider is handled based on the authentication mechanisms presented between the IdaaS and DP in Algorithm 1.
- When the *user*_i requests access to the cloud resources using user attributes, the cloud service provider grants access to the user. If a *user*_k requests access to the cloud resources, there must be both security attributes $[UID_k, UN_k, PW_k]$ and authentication token IDT_k . If both parameters exist, the user is granted access; otherwise, access denied is raised.

Based on the proposed frameworks for maintaining identity management of the users, a comparative analysis is applied to compare the IAM of the proposed frameworks with independent, centralized, and federated clouds. As presented in [39], IAM architectures have been analyzed based on their complexity, design, scalability, SSO, and user resources. These standards have been analyzed in independent, centralized, and federated clouds to explain and measure the efficiency of each architecture to each standard. In IAM of independent cloud, the service provider has its identity data. Therefore, the structure is simple but it is not scalable due to the difficulty for increasing the number of service providers. As presented in Tab. 2, a comparative analysis for the proposed IAM frameworks with other cloud architectures is provided as follows:

Criteria		Overall cloud frameworks				
	Independent Centralized Federated		Proposed frameworks			
Complexity	Low	Medium	High	High		
Design	Simple	Medium	Hard	Simple		
Scalability	Low	Medium	High	High		
Single-sign-on	No	Yes	Yes	Yes		
User resources	High	Low	Medium	High		

Table 2: Comparative analysis of proposed authentication frameworks

- **Complexity**: the proposed IAM introduces high complexity in securing user identities due to the efficient security features that are applied for securing the DP, IdaaS, cloud resource providers and users.
- **Design**: the design of the proposed IAM is more flexible in dealing with different cloud deployment models such as private and public clouds.
- **Scalability**: as the proposed IAM frameworks are enhanced for both public and private clouds, they are more scalable to be applied in different cloud architectures.

- Single Sign-On: the SSO process is highly effective in the IAM frameworks due to the ability of the users to access the public or private clouds with a single sign procedure while AuT_i or IDT_i are applied to authenticate the users that are signing to the cloud provider resources.
- User Resources: as the public cloud can obtain multiple service providers then users' identities can be validated from other service providers.

5 Threat Model

In cloud computing environment, the goal of the intruders or insiders is to compromise user identities to utilize cloud resources or disclose confidential information. Based on the cloud security threats that have been addressed in Tab. 1, the following are the most common assumptions for the capabilities of an attacker that may perform to penetrate cloud resources.

- **Insider Attacks:** this kind of attack is related to an insider user who tries to exceed his predefined privileges to disclose cloud data.
- Data Privacy Threats: occurs when the adversary discloses sensitive data attributes from the cloud resources.
- User Privacy Threats: occurs when the adversary intercepts the credentials of an authorized user.
- Brute Force Attacks: this attack is similar to malicious attack where the attacker tries every possible key for disclosing user privacy information.
- Single Sign on (SSO) Failure: this error occurs when there is a verification failure between the identity provider and cloud provider due to an interception between the directory provider and identity as a Service Provider
- **Denial of Service:** this type of attack occurs when there is an attempt to disrupt the service of the cloud service provider.

Tab. 3 summarizes the major security threats of cloud computing. Each one of the explained papers is checked whether it can defend against the presented threats and attacks or not.

Reference	Insider attacks	Data privacy threats	User privacy threats	Brute force attack	Single sign-on failure	Denial of service
[6]		х	Х	Х	\checkmark	х
[7]	\checkmark	Х	Х	Х	\checkmark	Х
[8]	\checkmark	\checkmark	\checkmark	Х	Х	Х
[9]	X	Х	Х	Х	\checkmark	\checkmark
[10]	X	х	х	Х	Х	\checkmark
[11]	\checkmark	х	х	Х	X	\checkmark
[12]	Х	х	х	Х	\checkmark	Х
[13]	\checkmark	х	х	Х	\checkmark	Х
[14]	\checkmark	х	х	Х	X	Х
[15]	\checkmark	х	\checkmark	Х	X	х
[16]	\checkmark	х	\checkmark	Х	X	х
[17]	Х		Х	х	X	Х

Table 3: Evaluation of recent security threats in IAM

(Continued)

Table 3 (continued)						
Reference	Insider attacks	Data privacy threats	User privacy threats	Brute force attack	Single sign-on failure	Denial of service
[18]	\checkmark	Х	X	X	\checkmark	
[19]	\checkmark	\checkmark	х	Х	X	X
[20]	\checkmark	\checkmark	\checkmark	\checkmark	Х	х
[21]	\checkmark	Х	х	Х	X	Х
[22]	\checkmark	Х	х	Х	X	Х
[23]	Х	\checkmark	\checkmark	Х	X	Х
[24]	\checkmark	\checkmark	\checkmark	Х	X	Х
[25]	\checkmark	Х	\checkmark		X	Х
[26]	\checkmark	х	\checkmark	\checkmark	X	Х
[27]	\checkmark	\checkmark	х	Х	\checkmark	Х
[28]	\checkmark	х	х	\checkmark	\checkmark	Х
[29]	\checkmark	\checkmark	х	Х	X	Х
[30]	\checkmark	\checkmark	х	Х	\checkmark	х
[31]	Х	\checkmark	х	Х	X	Х
[32]	Х	\checkmark	х	Х	X	Х
[33]	Х	\checkmark	х	Х	X	Х
[34]	Х	\checkmark	х	Х	X	Х
[35]	X	х	х	Х	X	Х
[36]	X	Х	х	\checkmark	X	Х
[37]	X	\checkmark	х	\checkmark	\checkmark	Х
[38]	X	\checkmark	х	\checkmark	\checkmark	Х
Proposed mechanisms	\checkmark	\checkmark		\checkmark	\checkmark	\checkmark

Based on the IAM security threats presented in Tab. 3, the proposed IAM frameworks for authenticating and validating users' identities are effective against aforementioned attacks as discussed below:

- **Insider Attacks:** This type of attack is eliminated due to the predefined privileges given to the user in both public and private clouds where the user parameter during the authentication process determines the authorization limit for each user.
- **Data Privacy Threats:** the proposed IAM frameworks protect data privacy in both public and private clouds by generating *AuT_i* and *IDT_i* respectively that can limit access to only authorized users.
- User Privacy Threats: the proposed IAM frameworks can maintain the privacy of users where the IdaaS allows only authorized users to access the cloud provider resources.
- Malicious Attacks: the proposed IAM algorithm and frameworks are effective due to the complexity in obtaining the identity token (IdT) for the authorized user.

- Single Sign On Failure: The verification is maintained due to the asymmetric authentication between the DP and IdaaS where the PU_{DP} and PR_{DP} keys are used to verify the sender and receiver of the Identity Token (IdT).
- **Denial of Service:** using the IAM framework, the cloud service provider does not contain the user identity. Instead, the Identity Token (IdT) for the user is generated on the DP and is verified using IdaaS then the Identity Token (IdT) is sent to the cloud service provider for authenticating the user.

6 Conclusion

Cloud computing is based on a set of different configurable resources like data centers, storage, networks, operating systems, applications and database. It can present a convenient access to cloud users based on their authorizations and privileges into which cloud service providers are responsible for granting access to different cloud resources and services based on user identity. Due to the increasing number of users on cloud services, security threats can cause different vulnerabilities in identity and access management processes. This paper proposed a comprehensive comparison for current cloud security services with their security threats and attacks in order to identify the major vulnerabilities and the proposed solutions in cloud identity management. An identity-as-a-service (IdaaS) algorithm and framework are presented based on a unified security mechanism of SSO and OAuth2 features. An encryptions techniques and access control mechanisms are implemented to provide a secured interaction between cloud provider and directory provider. Based on the proposed IdaaS, advanced frameworks for public and private clouds are explored to validate authentications of user identities. Furthermore, an evaluation of recent security threats on identity and access management (IAM) has been proposed to determine the efficiency of each model against a set of security attacks and threats. The proposed IdaaS achieved effective security countermeasure against different security attacks. Finally, a threat model is applied for exploring and validating the proposed IdaaS and cloud frameworks. Future directions on this paper will focus on implementing proposed frameworks and algorithm using Microsoft Azure solutions for providing a monitoring strategy and applying action alerts. The IAM will be implemented using Azure identity solutions that will apply active directory for implementing access management between Directory Provider (DP), Identity as-a-Service Provider (IdaaS), Cloud Provider (CP), and the user.

Funding Statement: This work was funded by the Deanship of Scientific Research at Jouf University under Grant No. (DSR-2021-02-0303).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] D. Patil and N. Mahajan, "An analytical survey for improving authentication levels in cloud computing," in *IEEE Int. Conf. on Advance Computing and Innovative Technologies in Engineering*, India, pp. 6–8, 2021.
- [2] I. Indu, P. M. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *International Journal of Engineering Science and Technology*, Elsevier, vol. 21, no. 4, pp. 574–588, 2018.
- [3] Z. Liu, J. Luo and L. Xu, "A Fine-grained attribute-based authentication for sensitive data stored in cloud computing," *ACM International Journal of Grid and Utility Computing*, vol. 7, no. 4, pp. 237–244, 2016.
- [4] I. Gordin, A. Graur and A. Potorac, "Two-factor authentication framework for private cloud," in *IEEE Int. Conf.* on System Theory, Control and Computing (ICSTCC), Romania, pp. 255–259, 2019.
- [5] A. P. Méndez, R. M. López and G. L. Millán, "Providing efficient SSO to cloud service access in AAA-based identity federations," *Future Generation Computer Systems*, Elsevier, vol. 58, pp. 13–28, 2016.

- [6] J. Werner, C. Merkle and C. Westphall, "Cloud identity management: A survey on privacy strategies," *Computer Networks*, Elsevier, vol. 122, pp. 29–42, 2017.
- [7] R. Shere, S. Srivastava and R. K. Pateriya, "A review of federated identity management of openstack cloud," in *IEEE Int. Conf. on Recent Innovations in Signal Processing and Embedded Systems (RISE)*, India, 2017.
- [8] A. Goel, G. Gupta, M. Bhushan and N. Nirwal, "Identity management in hybrid cloud," in *IEEE Int. Conf. on Green Computing and Internet of Things (ICGCIoT)*, India, pp. 1096–1100, 2015.
- [9] I. Indu and P. Anand, "Identity and access management for cloud web services," in *IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, India, pp. 406–410, 2015.
- [10] J. Han, W. Susilo and Y. Mu, "Identity-based data storage in cloud computing," *Future Generation Computer Systems*, Elsevier, vol. 29, pp. 673–681, 2013.
- [11] L. Deng, B. Yang and X. Wang, "A lightweight identity-based remote data auditing scheme for cloud storage," *IEEE Access*, vol. 8, pp. 206396–206405, 2020.
- [12] A. Singh and K. Chatterjee, "Identity management in cloud computing through claim-based solution," in *IEEE Int. Conf. on Advanced Computing & Communication Technologies*, India, pp. 524–529, 2015.
- [13] L. Barreto, F. Siqueira, J. Fraga and E. Feitosa, "An intrusion tolerant identity management infrastructure for cloud computing services," in *IEEE Int. Conf. on Web Services*, United States, pp. 155–162, 2013.
- [14] Y. Chi, G. Li, Y. Chen and X. Fan, "Design and implementation of open stack cloud platform identity management scheme," in *IEEE Int. Conf. on Computer, Information and Telecommunication Systems (CITS)*, France, pp. 1–5, 2018.
- [15] M. Faraji, J. Kang, H. Bannazadeh and A. Leon-Garcia, "Identity access management for multi-tier cloud infrastructures," in *IEEE Network Operations and Management Symp. (NOMS)*, Poland, pp. 1–9, 2014.
- [16] Y. Yang, X. Chen, G. Wang and L. Cao, "An identity and access management architecture in cloud," in *IEEE Int. Symp. on Computational Intelligence and Design*, China, pp. 200–203, 2015.
- [17] S. Wang, R. Pei and Y. Zhang, "EIDM: Ethereum-based cloud user identity management protocol," *IEEE Access*, vol. 7, pp. 115281–115291, 2019.
- [18] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, Elsevier, vol. 79, pp. 88–115, 2017.
- [19] S. Chong, M. Ahmad, I. Hamid and J. Abawajy, "Enhancing trust management in cloud environment," *Procedia-Social and Behavioral Sciences*, Elsevier, vol. 129, pp. 314–321, 2014.
- [20] A. Sharma and S. Mathur, "Concealing the user identity in cloud services," in IEEE Int. Conf. on Electronics, Communication and Aerospace Technology (ICECA), India, pp. 372–376, 2019.
- [21] C. Sullivan, "Protecting digital identity in the cloud: Regulating cross border data disclosure," Computer Law and Security Review, vol. 30, pp. 137–152, 2014.
- [22] J. Werner and C. Westphall, "A model for identity management with privacy in the cloud," in *IEEE Symp. on Computers and Communication (ISCC)*, Italy, pp. 1–6, 2016.
- [23] I. Khalil, A. Khreishah and M. Azeem, "Consolidated identity management system for secure mobile cloud computing," *Computer Networks*, Elsevier, vol. 65, pp. 99–110, 2014.
- [24] M. Suguna, R. Anusia, S. Shalinie and S. Deepti, "Secure identity management in mobile cloud computing," in IEEE Int. Conf. on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), India, pp. 42–45, 2017.
- [25] D. Soni and H. Patel, "Privacy preservation using novel identity management scheme in cloud computing," in IEEE Int. Conf. on Communication Systems and Network Technologies, India, pp. 714–719, 2015.
- [26] D. Sharma, C. Dhote and M. Potey, "Identity and access management as security-as-a-service from clouds," *Procedia Computer Science*, Elsevier, vol. 79, pp. 170–174, 2016.
- [27] A. Rasim and A. Fargana, "Identity management based security architecture of cloud computing on multi-agent systems," in *IEEE Int. Conf. on Innovative Computing Technology*, London, UK, pp. 232–235, 2013.
- [28] B. Cusack and E. Zadeh, "Evaluating single sign on security failure in cloud services," *Business Horizon*, Elsevier, vol. 59, no. 6, pp. 605–614, 2016.
- [29] F. Moghaddam, P. Wieder and R. Yahyapour, "A Policy-based identity management schema for managing accesses in clouds," in *IEEE Int. Conf. on the Network of the Future (NOF)*, London, UK, pp. 91–98, 2017.

- [30] J. Petrovska, A. Memeti and F. Imeri, "SOA Approach-identity and access management for the risk management platform," *IEEE Mediterranean Conf. on Embedded Computing (MECO)*, Montenegro, pp. 1–4, 2019.
- [31] L. Wu, Y. Zhang, K. Choo and D. He, "Efficient and secure identity-based encryption scheme with equality test in cloud computing," *Future Generation Computer Systems*, Elsevier, vol. 73, pp. 22–31, 2017.
- [32] S. Ma, "Identity-based encryption with outsourced equality test in cloud computing," *Information Sciences*, Elsevier, vol. 328, pp. 389–402, 2016.
- [33] Y. Yu, L. Xue, M. Au, W. Susilo, J. Ni et al., "Cloud data integrity checking with an identity-based auditing mechanism from RSA," *Future Generation Computer Systems*, Elsevier, vol. 62, pp. 85–91, 2016.
- [34] H. Deng, Z. Qin, Q. Wu, Z. Guan, R. Deng et al., "Identity-based encryption transformation for flexible sharing of encrypted data in public cloud," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3168– 3180, 2020.
- [35] Y. Zhang, J. Yu, R. Hao, C. Wang and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, pp. 6089–619, 2020.
- [36] X. Yang, M. Wang, T. Li, R. Liu and C. Wang, "Privacy-preserving cloud auditing for multiple users scheme with authorization and traceability," *IEEE Access*, vol. 8, pp. 130866–130877, 2020.
- [37] S. El Haddouti and M. El Kettani, "Analysis of identity management systems using blockchain technology," in *IEEE Int. Conf. on Advanced Communication Technologies and Networking (CommNet)*, Morocco, pp. 1–7, 2019.
- [38] W. Sim, H. Chua and M. Tahir, "Blockchain for identity management: The implications to personal data protection," in *IEEE Conf. on Application, Information and Network Security (AINS)*, Malaysia, pp. 30–35, 2020.
- [39] Y. Liu, D. He, M. Obaidat, N. Kumar, M. Khan et al., "Blockchain-based identity management systems: A review," *Journal of Network and Computer Application*, vol. 166, pp. 1–11, 2020.
- [40] W. Wu, Q. Zhang and Y. Wang, "Public cloud security protection research," in *IEEE Int. Conf. on Signal Processing, Communications and Computing (ICSPCC)*, China, pp. 1–4, 2019.
- [41] M. Hawedi, C. Talhi and H. Boucheneb, "Security as a service for public cloud tenants (SaaS)," in *Int. Symp. on Frontiers in Ambient and Mobile Systems*, Elsevier, Canada, vol. 130, pp. 1025–1030, 2018.
- [42] C. Zaraket, Kh. Hariss, M. Chamoun and T. Nicolas, "Cloud based private data analytic using secure computation over encrypted data," *Journal of King Saud University-Computer and Information Sciences*, vol. 25, pp. 1–12, 2021.