Journal of Theoretical and Applied Information Technology
15th February 2022. Vol.100. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SECURE IDENTITY AND ACCESS MANAGEMENT FRAMEWORK IN CLOUD ENVIRONMENT BASED ON DUAL-FACTOR AUTHENTICATION

FARIS MUDHHI ALRUWAILI[1], AYMAN MOHAMED MOSTAFA[2], OSAMA OUDA[3]

[1,2,3]College of Computer and Information Sciences, Jouf University, Sakakah 72388, Saudi Arabia

[3]Faculty of Computer and Information Sciences, Mansoura University, Mansoura 35516, Egypt

E-mail: [1]401101897@ju.edu.sa, [2]amhassane@ju.edu.sa, [3]omalsayed@ju.edu.sa

ABSTRACT

Assuring secure as well as user-convenient access to services and/or resources provided by cloud service providers is a crucial requirement for the widespread acceptance of cloud-based services. As a result, several Identity and Access Management (IAM) mechanisms have been proposed to address security and privacy issues inherent in cloud environments. A typical IAM mechanism mainly depends on a trusted third-party service, typically provided by an identity provider (IdP) server, to authenticate users before granting them access to services and/or resources provided by the cloud servers. These mechanisms, however, suffer from the lack of trust between the identity provider and cloud service provider. A fake identity provider can counterfeit access to cloud resources to disclose services using the user's identity without his/her consent. This paper presents a dual-factor-based IAM framework that alleviates such security concerns. In the proposed framework, the user's identity is verified by authenticating his/her credentials of the identity provider and by authenticating his/her iris biometric data by a directory server. The Bio Encoding Iris template protection scheme is employed to protect iris templates stored in the directory server. Experimental results on the typical iris dataset, CASIA-IrisV3-Interval, demonstrate the suitability of the iris biometric for the realization of the proposed IAM framework.

Keywords: *Identity And Access Management; Cloud Environment; Dual-Factor Authentication*

1. INTRODUCTION

Cloud computing is the next generation of networking and the new development style of computing. It is a collection of services presented as cloud computing architecture been layered [1]. The cloud consists of hardware, storage, networks, interfaces, and services as a set that delivers computing as a service based on user demand over the Internet. The emergence of the cloud environment has made it easier to treat computing systems as a collection of resources rather than a collection of independent data in managing each one [2]. Moreover, the cloud enables users to access its resources as services anywhere, which causes a revolution in its use and adoption. The multiplicity of service providers and the explosion in the number of users on the cloud make the process of authenticating and validating users on the cloud a challenging issue[3]. All this leads us to apply different security methodologies for securing the management of a large number of users. In addition, the assurance that only authorized users will have the ability to access resources.

Cloud computing security is a combination of technologies, controls, procedures, and policies that are used to protect data, information, and systems on cloud infrastructure [4]. Security of cloud refers to a set of countermeasures that IT organizations can apply to secure their cloud-based infrastructure through a cloud service provider against data theft, cyberattacks, and other recent threats [5]. There are many types of cloud computing security controls separated generally four categories. Firstly, deterrent control is used where administrative mechanisms such as procedures, guidelines, policies, standards, regulations, and laws are designed to prevent attacks on a cloud system [6]. Secondly, preventative control is applied and implemented to overcome threat events and to reduce the probability of any loss or errors [7]. The most used preventative control issues are standards,

processes, encryption, procedures, firewalls, policies, and physical barriers. Thirdly, detective control refers to the attempt to detect unusual acts and events to find problems once they have occurred such as review of account activity and reports, physical Inventories, and control self-assessment [8]. Finally, the corrective controls are considered the last line of defense for limiting the damage when a security attack was occurred such as business continuity planning, disaster recovery planning, incident response planning, and backup procedures [9].

Thus, the importance of identity management as a crucial part of cloud computing security has been increased in the last few years. Identity management is a security measure for managing users' and customers' identities to validate and authenticate their access to the cloud resources [10]. Identity management also controls access to resources by placing restrictions based on consumer identities. In today's cloud environment, an organization may collaborate with multiple cloud service providers to access various cloud-based applications. This requires deploying multiple authentication systems to enable the organization to authenticate employees and provide access to cloud-based applications [11].

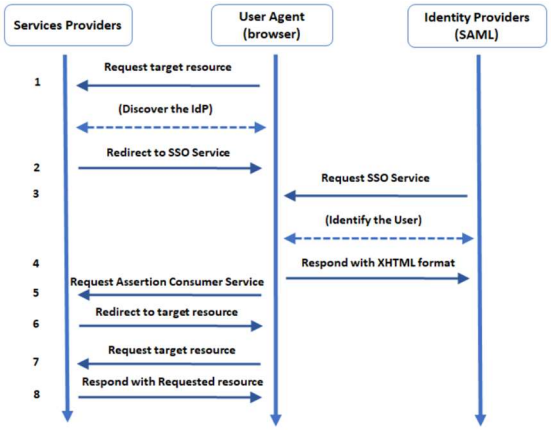

Figure1. Authentication using an Identity Provider (IdP).

The cloud environment uses both traditional and new authentication and authorization mechanisms to provide identity and access management. The key traditional authentication and authorization mechanisms deployed in an environment are Windows ACLs [12], UNIX permissions [13], Kerberos [14], and Challenge-Handshake Authentication Protocol (CHAP) [15]. Identity management as a service (IDaaS) is defined as the management of user identities that provides assurance to users, credentials, access, the appropriate time, roles, and the privileges they have to access resources. Identity management systems (IDMs) are defined as the information systems and technologies which can be used to implement the strategies of identity management, procedures, policies, and guidelines [16]. IDMs collect the identities of the users, data assets to protect them from unauthorized access [17]. Identity management system is classified into two main categories based on deployment architecture and functional behavior [18].

Deployment based classification: Classification based on deployment, this classification handles storage architecture, identity information flow, and management. It includes the Isolated, Centralized, or Federated[18].

- Isolated Cloud IDM is used for small or medium organizations. The isolated IDM contains only one server that acts as a service provider for storing and identifying user identities. Once the user sends a request to the cloud service provider (CSP), the CSP checks the validity of the user and then sends the response to the user [19][20][21].
- Centralized Cloud IDM is different from isolated cloud IDM. In centralized Cloud IDM, the identity provider (IdP) is separated from the service provider (SP) where the IdP is treated as a trusted third party for ensuring the user identity sent to the service provider (SP)[20][21][22].
- Federated Cloud IDM is used as a hybrid between multiple organizations that can use the same identification for accessing multiple networks in different enterprises. In federated Cloud IDM, the storage architectures are distributed where identity information for the users are stored in multiple locations[20][21][23].

Feature based classification: The functional behavior class contains different user-centric systems of identity management. These systems may follow a federated identity management or centralized identity management. The functionality of the identity management can be based on user-centric or anonymous cloud IDM[18]:

- User-Centric Cloud IDMS: involves using a user in every identity provisioning transaction. In each cloud service, the authentication and authorization processes should be executed[19][20][24].
- Anonymous Cloud IDMS: provides the anonymity of IDM for keeping the owner

of the service in the cloud secret from everyone[25].

Cloud IDMSs have six features and every feature has more than mechanism [26]:

- Authentication and its mechanisms are something you know (OTP & CR), something you have (Tokens), and something you are (Biometrics).
- Authorization and its mechanisms are access control policies, OAuth, and access right delegation.
- Identity federation and its mechanisms are smart-card (Encryption), multiple IdPs and CSPs, hierarchical storage, and distributed computation.
- Privacy and its mechanisms are proxy-systems, user-roles, pseudonyms, encryption, and limited disclosure.
- User-centricity and its mechanisms are consistent experience, and data disclosures policies.
- Audit & Logging and its mechanisms are activity monitoring, and history maintenance.

Figure 1 depicts a typical IAM framework in cloud environments. As shown in the figure, current IAM frameworks mainly depend on a trusted third-party service, typically provided by an identity provider (IdP) server, to authenticate users before granting them access to services and/or resources provided by the cloud servers. However, existing IAM techniques in cloud computing environments suffer from a number of issues that can be summarized as follows [27], [28]:

- The lack of trust between the identity provider and cloud service provider may cause security breaches.[29]
- A fake identity provider can counterfeit access to cloud resources to disclose services using user's identity without his/her consent.[29]
- The service provider should also ensure that the identity provider will notify service providers when a new provider is added to the trusted domain.[29]

In this paper, dual-factor-based IAM framework is proposed to provide an authentication between identity provider and cloud service provider. In the proposed framework, the user's identity is verified by authenticating his/her credentials of the identity provider and by authenticating his/her iris biometric data by a directory server.

RELATED WORK

Securing access to services and resources in Cloud environments and hence managing identities of Cloud users have attracted several research groups over the past few years. This section surveys previous work of identity and access management on Cloud.

Sharma et al. [30] discussed various security issues of cloud services and proposed an on-demand Identity and Access Management as a service (IAMaaS) framework that enables cloud service providers to provide IAM as a cloud service in public cloud so that only users who have the right to access resources are given permission. The focus of this framework is on providing authentication and authorization, as administration of identities. Separate virtual machines were devoted to the IAM core and IAM manager. First, the credentials of the client are encrypted and stored in the database so that no one, including the cloud service provider, can view the user password. Then, when the user logs in, a token is generated and passed to the protected resources provided by the cloud server only if his credentials are verified.

Chong et al. [31] addressed the problem of feedback related to security threats to the trust management system and suggested a way to deal with it by proposing an approach that anticipates suspicious comments so that the impact of these comments on the expense of trust level can be minimized. Feedback-related threats such as DDoS, malicious rater, damage of trust information accuracy, malicious participants attack, injection attacks, exploit system vulnerabilities, Fraud, have been identified and acted upon system reliability requirements such as Accuracy of Information, Information Security.

Lguliev et al. [32] presented a model that provided the dynamic management of identity federation of users that was an implementation single sign-on (SSO). SSO is the technology that allows one user access by the same password many resources in multi-agent providers. This model has three actors Service Providers (SPs), Identity Providers (IdPs), and Users. Identity information is shared between IdPs and accomplishes identity federation by the use means of formal Internet standards, such as the OASIS SAML specification, or by using open source technologies and other openly published specifications, like the Liberty Alliance Identity Federation Framework (ID-FF), Shibboleth, OpenID or WS-Federation.

Werner et al. [33] presented an overall evaluation is proposed with different evaluation criteria such as Transparency, Controllability, Minimization, Accountability, Data quality, Use limitation, User-friendly, Trust, and Obfuscation. This paper stated that different identity management characteristics must be provided to ensure the efficiency of IM.
Bhardwaj et al. [34] proposed deploying more security strategies in the Cloud environment to achieve the security goals that covered 13 security domains in cloud computing: program access security, data privacy security, database access security, internet access security, server access security, identity and access management, virtualization, encryption and key management, application security, incident response, notification, and remediation, data center operations, business continuity, and disaster recovery, traditional security, portability and interoperability, information lifecycle management, compliance and audit, legal and electronic discovery, governance and enterprise risk management, cloud computing architectural framework. Security and privacy issues force strong obstruction users to adopt Cloud services. This paper discussed how to assess cloud security risks by (QUIRC) a quantitative risk and impact assessment framework and define risks upon impact and probability. Also, a widely accepted method for the evaluation of impacts based on expert opinion is the Wide-band Delphi method, using rankings based on expert opinion about the likelihood and consequences of threats.
Barreto et al. [35] proposed to achieve good performance with intrusion tolerance by used the SecFuNet project and determined IT-VM as proper biases for it. This paper describes the experience in developing an OpenID intrusion tolerant identity provider, and the proposed architecture implemented to shared communication and memory between IdPs and VMs the agreement services and proxies on the level of Hypervisor that allows isolation to these. This model translates any intrusion into innocuous actions and kept the user information in separate compartments.
Chi et al. [36] proposed a solution to enhance the Open- Stack identity management mechanism, using the strong identity authentication and security management capabilities provided by FreeIPA to design a unified identity management component named Sentinel. Three services type was defined by Sentinel: access control service, external authentication service, and host management service which correspond to the security mechanisms that provided by FreeIPA. OpenStack uses a component of Kerberos in FreeIPA to authentication the user and ensure are transmitted usernames, passwords in encrypted form over the network which excel on Keystone authentication because it has greatly improved the security capabilities, and it adds the functions of the management of the host or virtual machine that Keystone does not have.
Moghaddam et al. [37] proposed user authentication model that based on a policies to address these problems : first is mismatch of Identity
management models based on particular policies and various security levels in various cloud servers, second is not managed the multi-purpose validation tasks based on policies which is in the multi level authentication, the proposed schema that contain four ingredient (check point, Policy Engine, Policy Database, Match Gate) to define access policy by cloud server. By using policy definition in cloud servers can provide a multi-level authentication process.
Shere et al. [38] described and analyzed various techniques that implement the identity management system on cloud. The authors made a comparison which presented advantages and disadvantages of each one of the techniques in the previous researches. The Authors' objective is to try find idea for FIM model to implement in OpenStack cloud.
Khreishah et al. [39] proposed a new IDM, they called Unified Identity Management (CIDM), and they fixed vulnerabilities and threats to identity management and addressed the security challenges that were provided when using the mobile client. The authors evaluated the security safeguards. And performance for ”Consolidated Identity Management (CIMD)” and also compared it with the current IDM. First, to avoid the vulnerability that causes IDM server penetration, is to separate the information portion (credentials) from potential insiders’ access to identity management. Second, to avoid mobile client weakness, the authors added a human interaction layer, which takes place after the user answers the secret question. Third, to avoid vulnerability ”network traffic interception”, the authorization information is split over multiple links instead of relying on a single link.
Ma . [40] proposed cryptography tool which call it an identity-based encryption with equality test (IBEET), the author combined the methods of ”public key encryption with equality test (PKEET) and identity-based encryption (IBE)”, Based on it, the author extracted a new encryption technic that the concept based on compute a trapdoor by the receiver, through use the secret key for the identity

then the receiver will send it to a cloud server for equivalence test.
Petrovska et al. [41] proposed a platform to achieve approach of high quality and multilayered which focus on and considerate security enforcement and audit, to the risk management that aim to efficient and effective.

The authors implemented and assignment the platform and tool by Oracle identity and oracle access management which occur after the authentication and authorization is accepted, the second stage of the risk management stand, come by propagate the identity of the authenticated and the profile information through create a security token which contain user name, roles and permissions specified to the user. Samlinson.E et al [42] proposed a mechanism to provide Identity as a service in a Federation environment to grant access to service providers based on Trust Agent (TA). When any user was created, the TA generated by an Identity provider and store in an account for every user, and records the transaction to TA. Once the user accesses another CSP the Trust Token (TT) with user attributes are sent to CSP to create trust between CSPs and TA and trust value is incremented as the user visits more CSPs.
The user-centric Trust-based identity management service first step User tries to access the Cloud Resource then SP redirects to IDP, IDP sends the user credentials to CSP, CSP authenticates the user. When the user successfully logs in to the system the IDM records the transaction details with the user attribute to the TA in the account created for the user. When the same user wants to access a service from a different CSP the IDM pulls out the Trust Token from the TA account and sends it along with the authentication.
Based on the previous literature review, an enhanced IAM framework is applied to provide authentication mechanism between directory provider and cloud service provider.

3. PROPOSED IAM FRAMEWORK

In this section, we present our proposed IAM framework and describe how it can address the security issues inherent to existing IAM techniques that we have discussed in Section I. To enhance trust between Identity Providers (IdPs) and Service Providers (SPs), we propose to provide authentication and authorization processes by introducing an additional server, hereafter called a Directory Provider (DP), to further authenticate the user by verifying his biometric data. The authentication process is based on a mandatory communication between both IdP and DP. Both IdP and DP must authenticate the user in order to grant or deny access to the cloud resources. On one hand, the IdP uses security assertion markup language (SAML) 2.0 protocol to authenticate the user by his/her credentials (username and password).

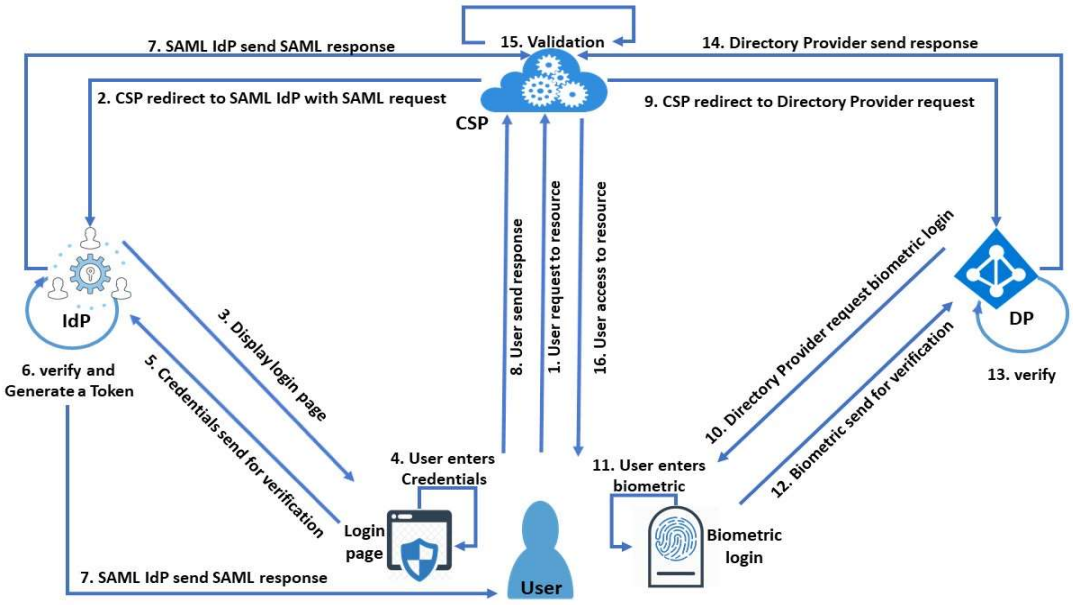

Figure 2. Proposed Iam Framework

In a nutshell, when the CSP receives a user request to access a given service/resource provided by the cloud, it requests the IdP to authenticate that

user. As soon as the IdP receives such request from the CSP, it redirects the user to enter his/her credentials via the login page to prove his/her identity. If the correct credentials are received by IdP, the user's identity will be verified. Then, the CSP requests the DP to further authenticate the user, but this time it is done through a biometric method, the directory provider redirects the user for proof of identity through entering his biometric data. Th final verification decision is based on the results obtained from both phases. That is, the CSP verifies the user identity based on data received from the three parties (IdP, DP, and user) before granting the user to access the requested cloud service and/or resource.

The workflow of the proposed IAM framework is depicted in Figure 2 and is described as follows:

1) The whole process is initiated when a user, U_i, requests access to a cloud service/resource provided by a given cloud service provider, CSP, by sending an access request to CSP.

2) In order to make an access control decision, the CSP firstly generates a SAML request to the IdP to verify the user's identity. This request is identified by a timestamp T_1.

3) The browser running by U_i is redirected to a single sign-on (SSO) URL to collect user credentials from U_i.

4) In this step, the user U_i inputs his credentials, user name (UN_i) and password (PW_i), in order to get access to the required service/resource.

5) The user credentials are sent to the IdP in order to verify the identification parameters of the user.

6) The IdP verifies the received credentials and generates an authentication token Idt_{Ui} for U_i in case they are correct. Otherwise, the user U_i will be denied from accessing the required service/resource hosted by CSP.

7) The IdP encrypts Idt_{Ui} using a hash function (H) in order to eliminate any disclosure of the created token. The hash value is computed by applying H on the concatenation of the identity token Idt_{Ui} with the username UN_i and the timestamp T_1 of the original message that has been sent in step 2 as illustrated in the following equation:

$$Hash\ H_1 = Idt_{Ui} || UN_i || T_1 \quad (1)$$

where || denotes the concatenation operator. Based on the value of T_1, both the IdP and CSP can confirm that there is no delay exists on the message. As a result, the man-in-the-middle attack can be hindered. The created SAML response is sent to the CSP and the identity token Idt_{Ui} is sent to U_i.

8) A login request is sent by Ui to the CSP using the identity token Idt_{Ui} Let Idt_{Uj} denote the identity token received by the CSP from a general user U_j. The CSP performs a matching process by firstly creating a hash of the Idt_{Uj} using the following equation:

$$Hash\ H_2 = Idt_{Uj} || UN_i || T_1 \quad (2)$$

A matching process is applied to match both hashes H_1 and H_2. If both hashes are identical, then no threats or malicious attacks exits on the identity token. As a result, the user passes the first verification check and is ready to undergoes the second check.

9) In order to alleviate the security issues of existing IAM techniques, once the user passes the first traditional check, a request is sent from the CSP to the DP to perform a second stage of the authentication process. Precisely, the CSP sends the identity token Idt_{Ui} of U_i to the DP.

10) The DP requests U_i to present his biometric data as a second authentication factor. In this work, we utilize iris biometric in order to validate our framework. Iris is widely adopted in many authentication systems due to its uniqueness and reliability [43].

11) A fresh biometric sample is captured from the iris of U_i.

12) The acquired biometric feature of U_i is sent to the DP as a response to the received request.

13) The DP verifies the biometric feature of the U_i to confirm his/her identity.

14) If the biometric feature sent by U_i is verified, a confirmation is sent to the CSP that the user

is authentic. Otherwise, the denial message is sent to the CSP.

15) The CSP performs a validation process by validating the two authentication factors received from both the IdP and DP servers.

16) If the two authentication factors are authentic, access to the requested service/resource is granted to U_i; otherwise, the access is denied.

4. EXPERIMENTAL RESULTS

The performance of the proposed IAM framework is primarily based on the second authentication phase. That is, the phase that depends on iris authentication. Thus, a number of experiments on the publicly available CASIA-IrisV3-Interval data-set [44] have been conducted to validate the functionality and assess the performance of the proposed two-factor IAM framework. This data-set contains 2655 iris images, of 320 × 280 pixels, captured from 396 eyes (classes) of 249 subjects. Each iris image is firstly pre-processed to localize the inner and outer boundaries of the iris region using the circular Hough transform [45].

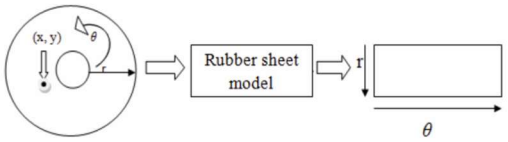

Figure 3. Iris normalization using the rubber sheet model proposed by Daugman [46].

Then, iris normalization was done by converting the localized iris region from Cartesian coordinates to Polar coordinates following Daugman's rubber sheet model [46] illustrated in Fig. 3. Unique iris features were then extracted by filtering the normalized iris region using a 1D log-Gabor filter. The extracted features were finally encoded into a 20 × 480 = 9600-bit binary template.

The distance between two iris-codes X and Y can be calculated using the normalized Hamming distance defined as follows:

$$d_H(X.Y) = \frac{1}{N}\sum_{j=1}^{N} X_j \oplus Y_j \quad (3)$$

where N is the number of the bits in the iris-code. In order to account for unwanted regions in iris images, such as eyelashes and eyelids and light reflections, we have not only generated an iris-code for each iris image in the adopted database but also generated a noise mask to mark corrupted bits in each iris template. An example of a normalized iris region along with its corresponding iris-code and noise mask is shown in Fig. 4. Neglecting the masked bits in the matching process would improve the recognition accuracy when matching two iriscodes. This can be done by reformulating the above equation into the following form [47]:

$$d_H = \frac{\|(\mathrm{Code_A} \cap \mathrm{Mask_A}) \oplus (\mathrm{Code_B} \cap \mathrm{Mask_B})}{\|\mathrm{Mask_A} \cup \mathrm{Mask_B}\|} \quad (4)$$

where $\mathrm{Code_A}$ and $\mathrm{Code_B}$ represent the iris-codes of the gallery and probe samples, respectively, $\mathrm{Mask_A}$ and $\mathrm{Mask_B}$ represent their corresponding masks, and ∩, ∪, and ⊕ represent the AND, OR, and XOR Boolean operations, respectively.

TABLE I. SUBSETS USED IN THE EXPERIMENTS OF EVALUATING IRIS RECOGNITION ACCURACY USING A GENERIC NOISE MASK.

	Subsets	
	P1	P2
Classes	1-132	133-396
No. of Images	880	1759

To account for users' privacy issues that can be raised as a result of storing plain iris-codes in the directory server, we employed the BioEncoding template protection scheme proposed by Ouda et al. [48], [49]. BioEncoding is a cancelable iris biometric scheme that is based on non-invertible transformation of the binary iris-code. This is done by dividing the original iris-code into a set of m-bit non overlapping words and then mapping each word into a single bit based on a random Boolean function. In this paper, we utilize BioEcnoding to obtain protected templates from the original iris codes using m = 3. To protect users' privacy and template security, protected templates are stored in the directory server instead of the original templates.

Moreover, in order to further preserve users' privacy against violation, user-specific noise masks should not be stored in the directory server. Thus, we followed the method described in [50] to find a generic mask for iris-codes. In this method, a subset

of the iris-codes along with their noise masks are used to find the common parts in a large number (α) of noise masks. To obtain the generic mask, we divided the adopted iris data-set into two subsets as illustrated in Table 1. The first subset was used to find the generic mask whereas the second subset was used to evaluate the recognition accuracy of the iris-based authentication system. Similar to the work presented in [50], α is set to 200 in our experiments. Fig. 5 shows an example of a user-specific noise mask and a generic mask generated using α = 200.

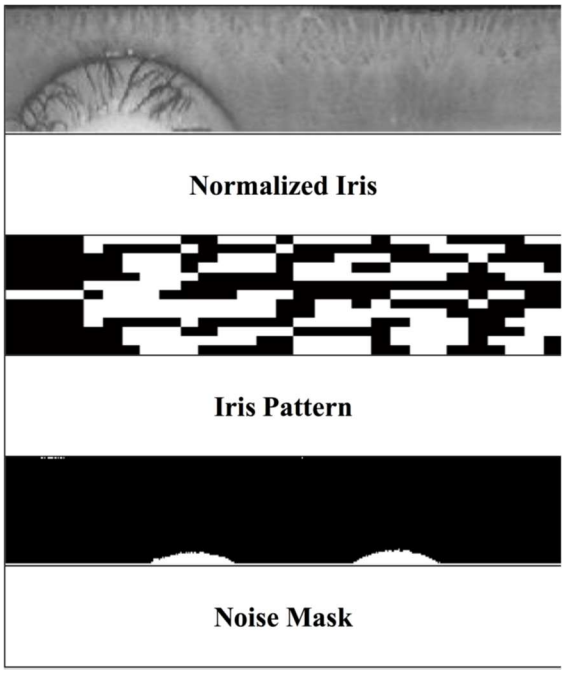

Figure 4. An example of a normalized iris region along with its corresponding iris-code and noise mask.

Figure 5. An example of a mask (a) generated from a specific class (b) multiple classes [50].

Figure 6 shows the distribution of the Hamming distance scores obtained by cross-comparison among the mated protected iris-codes (genuine distribution). The figure also shows the imposter distribution after aligning the compared nonmated protected pairs of bit sequences by shifting them 7 times and preserving only the best match found for each pair. It can be noticed that the overlap between the two distributions results in a false reject rate (FRR) of 0.049% at false accept rate (FAR) = 0. The obtained results illustrate the suitability of the iris biometric for the realization of our proposed IAM framework. Specifically, it is evident that the proposed framework can alleviate the issues of existing IAM methods at the expense of a small false rejection rate (< 5%). Additionally, smaller false rates can easily be achieved using advanced matching schemes such as the adaptive Hamming distance schemes [47], [51].

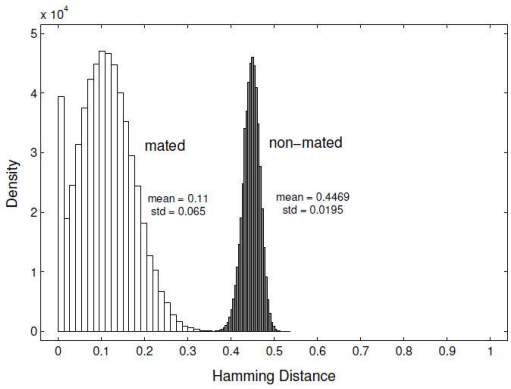

Figure 6. Hamming distances distributions for mated and non-mated iris-codes after circular alignment.

5. CONCLUSION

In this paper, we have proposed a dual-factor-based identify and access management framework for securing access to services and/or resources provided by cloud servers. Unlike current IAM frameworks which mainly depend on a trusted third-party service, typically provided by an identity provider (IdP) server, to authenticate users before granting them access to services and/or resources provided by the cloud servers, the proposed framework verifies the user's identity by not only authenticating his/her credentials by the identity provider but also by authenticating his/her iris biometric data by a directory server. This dual-factor authentication paradigm alleviates the security issues inherent in IAM frameworks that rely only on verifying data stored by identity providers and hence enhances the trust between cloud servers and identity servers. Results obtained from experiments conducted using the BioEncoding template protection scheme on the standard CASIA-Iris V3- Interval dataset demonstrate that iris data can reliably and efficiently be employed as a second factor of the proposed IAM framework. In

our future work, we intend to improve the obtained error by employing advanced matching schemes such as the adaptive Hamming distance method. In addition, an additional layer of security will be embedded in the proposed IAM framework in order to ensure the authentication between communicating entities.

ACKNOWLEDGEMENT

The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

REFRENCES:

[1] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," Future Generation Computer Systems, vol. 79, pp. 849–861, 2018.

[2] M. Bahrami and M. Singhal, "A dynamic cloud computing platform for ehealth systems," in 2015 17th International Conference on E health Networking, Application & Services (HealthCom). IEEE, 2015, pp. 435–438.

[3] R. Buyya, "Cloud computing: The next revolution in information technology," in 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010). IEEE, 2010, pp. 2–3.

[4] X. Xiao-tao, C. Zhe, J. Fei, and W. Hui-tao, "Research on serviceoriented cloud computing information security mechanism," in 2016 2nd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2016, pp. 2697–2701.

[5] M. Kumari and R. Nath, "Security concerns and countermeasures in cloud computing paradigm," in 2015 Fifth International Conference on Advanced Computing & Communication Technologies. IEEE, 2015, pp. 534–540.

[6] K. P. Iyer, R. Manisha, R. Subhashree, and K. Vedhavalli, "Analysis of data security in cloud computing," in 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB). IEEE, 2016, pp. 540 543.

[7] A. Varma, K. Saxena, and S. K. Khatri, "Preventive measures to secure issues in cloud computing," in 2019 International Conference on Intelligent Computing and Control Systems (ICCS). IEEE, 2019, pp. 504–508.

[8] B. Nedelcu, M.-E. Stefanet, I.-F. Tamasescu, S.-E. Tintoiu, A. Vezeanu et al., "Cloud computing and its challenges and benefits in the bank system," Database Systems Journal, vol. 6, no. 1, pp. 44–58, 2015.

[9] T. Lamis, "A forensic approach to incident response," in 2010 Information Security Curriculum Development Conference, 2010, pp. 177–185.

[10] P. Nida, H. Dhiman, and S. Hussain, "A survey on identity and access management in cloud computing," Int. J. Eng. Res. Technol, vol. 3, no. 4, 2014.

[11] P. Shi, H. Wang, X. Yue, S. Yang, S. Yang, X. Fu, and Y. Peng, "Corporation architecture for multiple cloud service providers in jointcloud computing," in 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW). IEEE, 2017, pp. 294–298.

[12] S. PONGSRISOMCHAI and S. NGAMSURIYAROJ, "Automated it audit of windows server access control," in 2019 21st International Conference on Advanced Communication Technology (ICACT). IEEE, 2019, pp. 539–544.

[13] M. Uphoff, M. Wander, T. Weis, and M. Waltereit, "Securecloud: an encrypted, scalable storage for cloud forensics," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018, pp. 1934–1941.

[14] S. C. Patel, R. S. Singh, and S. Jaiswal, "Secure and privacy enhanced authentication framework for cloud computing," in 2015 2nd International Conference on Electronics and Communication Systems (ICECS). IEEE, 2015, pp. 1631–1634.

[15] A. Ghilen, M. Azizi, and R. Bouallegue, "Integration and formal security analysis of a quantum key distribution scheme within chap protocol," in 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2015, pp. 1–7.

[16] X. Ma, "Managing identities in cloud computing environments," in 2015 2nd International Conference on Information Science and Control Engineering. IEEE, 2015, pp. 290–292.

[17] A.-S. Shehu, A. Pinto, and M. E. Correia, "Privacy preservation and mandate representation in identity management systems," in 2019 14th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2019, pp. 1–6.

[18] U. Habiba, R. Masood, M. Awais Shibli and M. A Niazi, "Cloud identity management security issues & solutions: a taxonomy," Springer journals: Complex Adaptive Systems Modeling, vol. 2, no. 5, 2014.

[19] Alrodhan WA, Mitchell CJ: Enhancing user authentication in claim based identity management. In Collaborative Technologies and Systems (CTS), 2010 International Symposium on. Piscataway, New Jersey, United States: IEEE, 2010, pp.75–83.

[20] Cao Y, Yang L: A survey of identitymanagement technology. In IEEE International Conference on Information Theory and Information Security (ICITIS): IEEE, 2010, pp.287–293.

[21] Jøsang A, Fabre J, Hay B, Dalziel J, Pope S: Trust requirements in identity management. In Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Vol. 44: Australian Computer Society, 2005, pp.99–108.

[22] Windley PJ: Digital Identity. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2005. Yan L, Rong C, Zhao G: Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In Cloud Computing.2009, pp.167–177.

[23] Chen J, Wu X, Zhang S, Zhang W, Niu Y: A decentralized approach for implementing identity management in cloud computing. In Cloud and Green Computing (CGC), 2012 Second International Conference on. Piscataway, New Jersey, United States: IEEE, 2012, pp. 770–776.

[24] Suriadi S, Foo E, Jøsang A: A user-centric federated single sign-on system. J Netw Comput Appl 2009, vol. 32, pp.388–401. Elsevier, 2009.

[25] McCallister E: Guide to Protecting the Confidentiality of Personally Identifiable Information. Collingdale, PA, United States: Diane Publishing; 2010.

[26] Ferdous MS, Poet R: A comparative analysis of identity management systems. In High Performance Computing and Simulation (HPCS) 2012 International Conference on. Piscataway, New Jersey, United States: IEEE, 2012, pp. 454–461.

[27] H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," The journal of supercomputing, vol. 76, no. 12, pp. 9493–9532, 2020.

[28] I. Indu, P. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," Engineering science and technology, an international journal, vol. 21, no. 4, pp. 574–588, 2018.

[29] Y.Liu, D. Hea, M. S. Obaidat, N. Kumar, M. K. Khan, K. Chooh, "Blockchain-based identity management systems: A review," Journal of Network and Computer Applications, ELSEVIER, vol. 166, pp. , 2020, doi.org/10.1016/j.jnca.2020.102731.

[30] D. H. Sharma, C. Dhote, and M. M. Potey, "Identity and access management as security-as-a-service from clouds," Procedia Computer Science, vol. 79, pp. 170–174, 2016.

[31] S.-K. Chong, J. Abawajy, M. Ahmad, and I. R. A. Hamid, "Enhancing trust management in cloud environment," Procedia-Social and Behavioral Sciences, vol. 129, pp. 314–321, 2014.

[32] R. Alguliev and F. Abdullayeva, "Identity management based security architecture of cloud computing on multi-agent systems," in Third International Conference on Innovative Computing Technology (INTECH 2013). IEEE, 2013, pp. 123–126.

[33] J. Werner, C. M. Westphall, and C. B. Westphall, "Cloud identity management: A survey on privacy strategies," Computer Networks, vol. 122, pp. 29–42, 2017.

[34] A. Bhardwaj and V. Kumar, "Cloud security assessment and identity management," in 14th International Conference on Computer and Information Technology (ICCIT 2011). IEEE, 2011, pp. 387–392.

[35] L. Barreto, F. Siqueira, J. Fraga, and E. Feitosa, "An intrusion tolerant identity management infrastructure for cloud computing services," in 2013 IEEE 20th International Conference on Web Services. IEEE, 2013, pp. 155–162.

[36] Y. Chi, G. Li, Y. Chen, and X. Fan, "Design and implementation of openstack cloud platform identity management scheme," in 2018 International Conference on Computer, Information and Telecommunication Systems (CITS). IEEE, 2018, pp. 1–5.

[37] F. F. Moghaddam, P. Wieder, and R. Yahyapour, "A policy-based identity management schema for managing accesses in

clouds," in 2017 8th International Conference on the Network of the Future (NOF). IEEE, 2017, pp. 91–98.

[38] R. Shere, S. Srivastava, and R. Pateriya, "A review of federated identity management of openstack cloud," in 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE). IEEE, 2017, pp. 516–520.

[39] I. Khalil, A. Khreishah, and M. Azeem, "Consolidated identity management system for secure mobile cloud computing," Computer Networks, vol. 65, pp. 99–110, 2014.

[40] S. Ma, "Identity-based encryption with outsourced equality test in cloud computing," Information Sciences, vol. 328, pp. 389–402, 2016.

[41] J. Petrovska, A. Memeti, and F. Imeri, "Soa approach-identity and access management for the risk management platform," in 2019 8th Mediterranean Conference on Embedded Computing (MECO). IEEE, 2019, pp. 1–4.

[42] E. Samlinson and M. Usha, "User-centric trust based identity as a service for federated cloud environment," in 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013, pp. 1–5.

[43] J. Daugman, "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons," Proceedings of the IEEE., vol. 94, no. 11, pp. 1927 - 1935, 2006.

[44] The CASIA Iris Image Database. [Online]. Available: http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp.

[45] L. Masek et al., "Recognition of human iris patterns for biometric identification," Ph.D. dissertation, Citeseer, 2003.

[46] P. Verma, M. Dubey, P. Verma, and S. Basu, "Daughman's algorithm method for iris recognition—a biometric approach," International journal of emerging technology and advanced engineering, vol. 2, no. 6, pp. 177–185, 2012.

[47] R. Tobji, W. Di, N. Ayoub, and S. Haouassi, "Efficient iris pattern recognition method by using adaptive hamming distance and 1-d loggabor filter," Int. J. Adv. Comput. Sci. Appl, vol. 9, no. 11, pp. 662 669, 2018.

[48] O. Ouda, N. Tsumura, and T. Nakaguchi, "Tokenless cancelable biometrics scheme for protecting iris codes," in 2010 20th international conference on pattern recognition. IEEE, 2010, pp. 882–885.

[49] O. Ouda, N. Tsumura, and T. Nakaguchi, "Bioencoding: A reliable tokenless cancelable biometrics scheme for protecting iriscodes," IEICE TRANSACTIONS on Information and Systems, vol. 93, no. 7, pp. 1878–1888, 2010.

[50] O. Ouda, K. Nandakumar, and A. Ross, "Cancelable biometrics vault: A secure key-binding biometric cryptosystem based on chaffing and winnowing," in 2020 25th International Conference on Pattern Recognition (ICPR). IEEE, 2021, pp. 8735–8742.

[51] A. B. Dehkordi and S. A. Abu-Bakar, "Iris code matching using adaptive hamming distance," in 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA). IEEE, 2015, pp. 404– 408