Cloud Identity Management – A Critical Analysis

Temidayo Abayomi-Zannu and Isaac Odun-Ayo, *Member, IAENG*

***Abstract*— Cloud computing is a dynamic paradigm based on sound technology aimed at supporting IT users in essential computing task. Cloud providers offer services that can be used to carry out common task that is accessible online anywhere. Nevertheless, they come with some major challenges. The most common is that of security, which has made identity management necessary thereby compelling the Cloud service providers to ensure that users are properly authenticated. This paper presents the state of the art from some literature available on cloud identity management. The study was executed by means of review of some literature available on cloud identity management to examine the present trends towards providing a guide for future research in cloud computing.**

***Index Terms*—Cloud-computing; Identity management; Single Sign-On; Two/Multi Factor Authentication.**

I. INTRODUCTION

"CLOUD computing is defined as a model that enables convenient, ubiquitous and on-demand network access to a shared pool of configurable computing resources (e.g., servers, applications, storage, and services) that can be quickly allocated and/or deallocated with minimal management effort" [1]. Cloud computing is set to became the main focus of all activities around IT utilization. Cloud computing has the primary component to assist an enterprise and even SMBs to succeed in their IT endeavors. Cloud computing provide scalable, elastic, on demand services via the Internet to cloud users. The cloud utilizes the concepts of virtualization and multi–tenancy to deliver metered services to consumers through cloud service providers (CSPs). Cloud services are provided at three levels of abstraction. The Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) [2]. In SaaS, services and applications are delivered over the Internet and accessed using a web browser by the users. The cloud service provider ensures the deployment and maintenance of the applications, the operating system and other cloud services [3]. In PaaS, the service provider offers a platform for users to create and deploy applications. The implication of this is that the user has little or no control over the operating system and other cloud resources but manages and runs an application on the virtual resources provided by the service provider [3]. IaaS provides the cloud environment to the users in order for them to utilize the processing capability, storage and bandwidth, making it possible for them to run an operating system on a virtual machine of the cloud provider [4].

Cloud computing has four deployment models that describes the scope of service offered to the cloud customers. They are the private, public, community and hybrid clouds. Private clouds are usually owned and hosted by an organization. The infrastructure may be on premise or off premise, but it is secure because users belong to that organization [5]. Public clouds involve cloud providers that offer services to customers over the Internet. They own and control massive data centers and other infrastructure, sometimes spread over different geographical locations. Security and privacy is a concern on public clouds. Community cloud is owned by several organization with shared common interest. The infrastructure is shared among the organization based on agreed policies. Hybrid clouds is a combination of either private, public, or community clouds. The entities are unique but managed by a single unit [3].

Digital identity allows an entity to be represented in some forms of information that makes the entity recognizable within a particular framework [4]. Identity management (IDM) is a collection of related policies that allows the administration, maintenance, management, information exchange, discovery and authentication process used to identify an information with a view to ensuring overall security. [4]. Information can be accessed at anyplace and anytime over the Internet using cloud services. Therefore, there is the need to have an identity management scheme to verify a valid user and offer services based on such valid authentication credentials. An identity management process aims to secure the user and other processes in terms of private and sensitive information. Every enterprise is expected to restrict access to computing resources and sensitive information [6]. Cloud identity management systems are distinct from traditional methods because of unique characteristics of the cloud such as access control, scalability, virtualization, provisioning and multi-tenancy while allowing some important functions such as access rights, authentication and authorization to be given the deserved attention on the cloud [7].

A cloud IDM must secure virtual devices, dynamic machines and control points among others [8]. Certainly, traditional IDMs that simply manages users and services is a

Manuscript received October 05, 2018; revised October, 2018. This work was supported in part by Center of ICT/ICE Research, CUCRID Building, Covenant University, Ota, Nigeria
T. Abayomi-Zannu is with the Department of Computer and Information Sciences, Covenant University, Ota, Nigeria. (+2348060978562; temidayoabayomizannu@gmail.com)
I. Odun-Ayo is with the Department of Computer and Information Sciences, Covenant University, Ota, Nigeria. (e-mail;isaac.odun-ayo@covenantuniversity.edu.ng)

fairly static manner cannot be suitable for cloud purposes. For example, it is critical to inform the IDM when a service has been terminated or a machine de-provisioned so that it can revoke future access [9]. IDM is expected to store details of such inactive processes until they become active again. Therefore, access management to the data of such devices becomes critical and must be in line with the service level agreement [8]. Again, normal IDM cannot be utilized on the cloud because of the unique nature of cloud operations and infrastructure. The purpose of this paper is to examine cloud computing and identity management system. The paper discusses issues in IDM and thereafter highlights current IDM trends in industry. The remaining part of the paper is organized as follows: Section 2 discusses related work. Section 3 examines types of IDM and IDM architectures. Section 4 highlights industry IDM trends. Section 5 concludes the paper and future work suggested.

II. RELATED WORK

Security in cloud computing: opportunities and challenges in [10, 11] proposed a cloud computing architectural framework. Security challenges at various abstractions of cloud computing were examined. Identity management and access control were also examined in some details. Cloud computing security issues and challenges: a survey in [3] presented a survey of security issues in terms of cloud delivery and deployment modes. It also examined identity management in the area of cloud computing. Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth in [12] proposed a framework for identity management using Shibboleth. The main focus was to provide identity management to enhance authentication and authorization in cloud computing. Assessment criteria for cloud identity management systems in [7] proposed some criteria for assessing cloud identity management system. Identity management system is essential for access control; hence a comparative analysis will further enhance security on the cloud. Integrated Federated Identity Management for Cloud Computing in [13] discussed the identity management based on the different cloud layers. An integrated federated identity management was proposed and implemented. The benefits of the model were outlined in the paper. ICEMAN: an architecture for secure federated inter-cloud identity management in [14] considered the fact that no identity management schemes exists at the inter-cloud level. It proposed an inter-cloud IDM cloud security. Consolidated Identity Management System for secure mobile cloud computing in [4] observed that mobile users store personal information in an insecure manner on mobile devices.

Current IDMs for mobile devices have limitations making them vulnerable. A consolidated IDM is proposed to mitigate the vulnerabilities. Privacy-preserving digital identity management for cloud computing in [15] used encryption techniques for digital identity management. The proposed model allows verification of a user identity on multiple clouds. Identity and access management as security-as-a-service from clouds in [16] is a great enhancement of the identity management system. The identity and access management are distinct and it is implemented as a service on the cloud. Identity in the cloud in [17] discussed the simple cloud identity management, which is a recent standard being adopted by cloud services providers. This model was developed by the open web foundation. A novel virtual identity implementation for anonymous communication in cloud environments in [6] seeks to further secure the process of identity management on the cloud. The approach is to hide the user's identity by authenticating an unknown user in an unknown environment. Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework in [18] proposed a model that enhances authentication and security both for an organization and the employees. The model is implemented and results have significant implication on the identity management of users.

III. FUNCTIONS AND CLASSIFICATIONS OF IDENTITY MANAGEMENT SYSTEM

A. Layers of Identity Management System

IDM comprises identity of the user used throughout a certain period based on software and components used to address such a user and this consists of three main type of entities, namely the user, identity provider (IdP) and the service provider (SP) [4]. The following are the main function of IDMs [4] [15]

- **Account Management:** The process of providing identity within an enterprise is used for the users, administrators and developers in terms of provisioning and de-provisioning which enables the provisioning of users and groups in different systems.
- **Authentications:** It is essential to determine who a person claims he/she is through the process of authentication which allows the user to be identified using various methods such as biometrics, login and user passwords.
- **Authorization:** This is meant to enable various kinds of level of access for different parts or operations within a computing system. It is the process of determining the permissions or rights that users have.
- **Federation:** This a process where organizations agree to collectively share authentication information based on trust. The identity of users is shared beyond the confines of an individual organization. Federation enables an authentication process on a global scale.
- **Auditing:** This is simply an accounting process that allows activities to be monitored so that occurrences can be traced to particular users when the need arises.

B. Classification of Identity Managing System

Cloud IDMs are utilized to represent and recognized identities in the digital world. IDMs can be classified into 4 distinct categories. Namely isolated, centralized, federated and anonymous. They are discuses in the subsequent paragraphs [7].

1) Isolated IDMS

Isolated IDMs makes use of a single server for the service provider and also the identity provider and it manages the identity information in storage for the user including user

ISBN: 978-988-14048-5-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

activities. This method is usually adopted by small and medium businesses [7]. Before getting service, the user is expected to complete the identity process at CSP1 and thereafter, CSP1 directs the user's request to its IDP for further attention. After a successful authentication process, a response is provided to the user. The IDM does need any third-party assistance for credentials and verification in this method. On the other hand, the process becomes cumbersome with increased services because each service must ascertain the credentials of users that have been authorized [7].

2) Centralized Identity Managing System

Centralized IDMs separates the functions of the service providers and identity providers. In this case, management and storage of identity data including resources is handled by a third party single IdP that is trusted. The process starts with the collection of identity data by the IdP from the CSP in respect of the users. Thereafter, a cloud user may send an authentication request and it is routed to the relevant IdP who provide the necessary authentication response as shown at [7].

3) Federated Identity Managing System

Federated IDMs enables the subscribers from several organizations to utilize the same identity data in order to obtain access to the networks that exist in group of trusted enterprises. The federated management system is enjoying wide usage because it eliminates the need for individual authentication accounts [19]. The systems enable access across several domains to user credentials by external parties. The Federated IDM makes it possible to store identity information in different locations using the distributed storage architecture. As shown in [7], a user may wish to carry out the authentication process through CSP1 before getting service. At CSP1, the process commences using the push and pull method that enables the CSP to access identity credentials stored by multiple service providers and IdPs. Although a service provider can maintain its own individual database to manage user credentials, the CSP must however, link that information through the user's identity during the process of authorization and authentication.

4) Anonymous Identity Managing System

In anonymous IDMs, the user credentials can be kept relatively secret from users and providers alike. This is because there is no name associated with the identity information making it anonymous [20]. It however essential that the anonymity should be sufficiently strong to prevent leakage. Such leakage may not be deliberate but could be as result of credentials being linked with other information that may be published.

C. Shibboleth

The OASIS security assertion makeup Language (SAML) introduced a system that allows for exchange of security information among organizations online. The SAML assertions is a portable one that enables trusted utilization among applications in different domains for the purpose of security [5]. The OASIS SAML framework provides rules for using these SAML assertions to request, create and communicate [4]. The user has the privilege of having a single sign on that is available across multiple domains. These organizations belong to the same federation and share identity credentials. The Shibboleth has the IdP and SP systems. The IdP manages the user authentication and also maintains the user credentials [4]. In addition, it is responsible for proving user credentials to trusted organizations within the federation. Shibboleth has four components.

- **Handle Service:** This service is responsible for the authentication mechanism. In addition, it creates the token which is the SAML assertion that takes credentials to the users and also enables an organization to select appropriate authentication mechanism.
- **Attribute Authority:** This component manages the service providers request concerns. It handles attributes with application of relevant privacy policies. It also enables users determine who can access them and proving a choice of directory to organizations.
- **Directory Service:** This is external to shibboleth and it stores users attribute locally.
  - **Authentication Mechanism:** This mechanism is not within shibboleth and allows user authentication with the central service using a password/login. SP Shibboleth stores the resources required by the user for access. It also manages access control based on request by the IdP. An SP may comprise various applications, but it will be considered a single entity by the IdP. The SP Shibboleth has three main services.
    - **Assertion Customer Service:** This is responsible for receiving messages to (SAML) to establish a secure environment.
    - **Attribute Request:** It is responsible for obtaining and passing user attribute for the resources manager.
    - **Resources Manager:** It intercepts request for resource and makes decision to central access based on user attributes.

D. Identity Managing System Vulnerabilities.

The cloud is inherently risky, security-wise and many traditional identity and access management do not translate well to it [18]. Most organizations use out-of-date password policies for example eight character with complexity that do little to defend against the methods that hacker use to gain access to password. The correct way to defend against password guessing is to passphrase [7]. However, even those organizations that correctly implement passphrase may find it difficult to extend this policy to the cloud since many cloud applications enforce a maximum password length.

Password guessing is not the only method hackers will use to gain access to accounts, credential theft is usually simpler via email phishing, a tactic favored by nation state and organized crime attackers. Therefore, cloud IDM policies need to reflect this risk and organizations should do their best to mitigate this by enforcing multifactor authentication on all Internet facing services. To enhance cloud IDM, the organization must ensure that the cloud IDM policy defends against actual methods hacker use to

ISBN: 978-988-14048-5-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

target user accounts. A centrally controlled robust cloud IDM must be in place to cover cloud services, cloud applications, outsourced IT, vendors and third parties [21]. In addition to provisioning of passwords, enterprises must ensure that when employers changes role or leave the company, their access is altered or removed. It is also important to know who has access and to what applications, combined with alerting mechanisms that can report on unusual log on activity on cloud servers.

IV. IDENTITY MANAGEMENT SYSTEM INDUSTRY PERSPECTIVE

A. Identity Access Management-as-a-Service

Identity Access Management-as-a-Service (IDaaS) is a process to ensure secure IDM. IDaaS is useful in the area of machine learning, management and other security data. Attention is now moving to using IDaaS to secure on premise applications. IDaaS will be useful on premise for synchronizing user directories, syncing password hashes and authentication users to active directory federation services. Using IDaaS to control access to on premise applications has several benefits. It will allow for the consolidation of visibility, control and policies in one place [22]. By 2019, 40% of IDaaS implementation will replace on-premise IDM implementations [23]. The increased utilization of IDaaS is partly due to the difficulty and high cost in running and maintaining an IDaaS infrastructure on premises. In addition, the ever-expanding utilization of other something-as-a-service offerings allows the decision to be widely accepted. Also, web and mobile applications allows a natural means for the transition from in-house IDM to IDaaS. It was also predicted in the eGuide that by 2019, use of password and tokens will drop by 55% which is due to the introduction of recognition technologies and with reduce cost and higher accuracy of biometrics, they are offering good opportunities for use continuously in authentication.

B. Involvement of Cyber Security Experts in Identity Management System

IDM involves a lot of tools such as access policy, multiple data responsibility, manual process and others. User authentication was and is still been dependent on user names and password which makes nearly every organization vulnerable to credential harvesting, identity theft and cyber-attacks. [22]. Enterprises will be more open minded to a cloud-based control plans and with SaaS offerings for IDM such as Okta, Ping, Centrify etc., it can become a better alternative in an attempt to seek out solutions to unify tools in IDM for cloud-based activities. Username/ password authentication has to go because it is a security nightmare and it has proven that other replacement methods like smart cards or security tokens in the past were too expensive but a large support for fido specification and pervasive biometrics which are now being built into mobile devices may terminate the use of username and password authentications which would make IDM skills more valuable and rare.

C. Enhancing Identity and Access Management

The IDM provides multiple means of identification and authentication like biometric, single sign-on, one-time passwords, etc. and more than one of these can be used together which provides a more secured and accurate user identification when compared to a simple username and password. Due to this, if one means of authentication is compromised, another means of authentication is there as a safe guard [7].

TABLE I
POPULAR IDENTIFICATION MANAGEMENT USAGE

References	Passwords	Biometric Scan	Single Sign-On (SSO)	Two/Multi Factor Authentication (TFA)	OAUTH Protocol 1.0 & 2.0	Security Token	Security Assertion Markup Language (SAML)	Open ID Authentication Protocol	One Time Passwords (OTPs)
(Leandro, Nascimento, Dos Santos, Westphall, & Westphall, 2012)	x	x	x			x	x		
(Stihler, Santin, Marcon Jr., & Fraga, 2012)			x			x	x	x	
(Habiba, Abassi, Masood, & Shibli, 2013)				x	x		x	x	x
(Bhardwaj & Kumar, 2014)			x					x	x
(Bradford, Earp, & Grabski, 2014)	x		x	x					
(Dhatchayani & Sriram, 2014)	x		x				x		
(Habiba, Masood, Shibli, & Niazi, 2014)			x		x		x	x	x
(Khalil, Khreishah, & Azeem, 2014)	x				x	x			
(Saini & Mann, 2014)							x	x	
(Sarhan & Lilien, 2014)			x					x	
(Yeluri & Castro-Leon, 2014)	x	x	x			x	x		x
(Werner & Westphall, 2016)							x	x	
(Banday & Mehraj, 2017)				x	x		x	x	
(Isaac, Nicholas, Modupe & Olasupo, 2017)	x		x						
(Khajehei, 2017)			x		x		x		
(Kostopoulos et al., 2017)		x		x				x	
(Odun-Ayo, Ajayi & Omoregbe, 2017)			x			x	x	x	
(Odun-Ayo, Ajayi & Omoregbe, 2017)			x					x	x
(Odun-Ayo, Ajayi & Omoregbe, 2017)	x		x				x		
(Odun-Ayo, Misra, Omoregbe, Onibere, Bulama & Damasevicius, 2017)			x		x		x	x	x
(Salaria, 2017)	x	x	x		x	x	x	x	
(Suguna, Anusia, Shalinie, & Deepti, 2017)						x			
(Werner, Westphall, & Westphall, 2017)			x				x	x	
(Anilkumar & Sumathy, 2018)	x	x	x		x			x	
(Bhandari, Patel, & Bhandari, 2018)			x					x	
(Fremantle & Aziz, 2018)					x	x	x	x	
(Indu, Anand, & Bhaskar, 2018)	x	x	x	x	x		x	x	x
(Khajehei, 2018)			x				x	x	
(Odun-Ayo, Odede & Ahuja, 2018)							x	x	
(Odun-Ayo, Agono & Misra, 2018)			x					x	
(Odun-Ayo, Ajayi & Misra, 2018)	x		x	x					
(Odun-Ayo, Ananya, Agono & Goddy-Worlu, 2018)		x							
(Odun-Ayo, Okereke & Orovwode, 2018)							x	x	
(Odun-Ayo, Okereke & Orovwode, 2018)						x		x	
(Schulze, 2018)	x		x	x			x		x
(Vo, Fuhrmann, & Fischer-Hellmann, 2018)					x		x		

ISBN: 978-988-14048-5-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Based on the analysis, passwords are still being used till today but are never used alone because it is a security nightmare. This is due to the fact that users still prefer using a password as a means of authentication but now passwords are used with other authentication means like biometrics, tokens etc. Biometric scan has become quite popular but hasn't been fully implemented which is due to the fact that it requires a separate hardware like a finger print scanner or facial recognition device for it to work. Some of these like a fingerprint scanner are now been installed on smartphones and some laptops which has helped with the integration. Single sign-on (SSO) is an authentication service that allows a user to sign into other applications automatically once the user logs into their account and a very popular implementation of this is Google's services which is widely accepted by the users.

Two/Multi factor authentication is the use of not just a password as a means of authentication but the use of multiple means like security questions, one-time passwords and others. It is based on what the user knows and what the user has as a means of authentication and added security which is also widely accepted by users. OAUTH Protocol 1.0 & 2.0 is an industry-standard protocol for authorization that allows users to grant applications or websites permission to access their credentials without the need for a password and has been implemented in Facebook, Twitter etc. Security tokens is a physical device provided by a service provider that is used as an added security and authentication means to gain access to an electronically restricted resource but adds an extra cost due to the device itself. Security Assertion Markup Language (SAML) is an open standard that is used for sharing security information about authentication, authorization, and identity across multiple systems while also providing a framework for SSO and is a very popular means of authentication in the cloud.

Open ID Authentication Protocol is an open, decentralized, free framework for user-centric digital identity which allows a user to use an existing account to sign into multiple websites, without the need to create a new password which has been very popular with users and also service provides because they do not need to pay any royalty fees for using the service. One Time Passwords (OTPs) is a type of password that is valid for only one use and is sent to the user through their email or mobile phone which adds an added layer of security. This has become widely accepted by users since they do not require any special hardware or software to gain access to the service and once that password has been used or hasn't been used in the next few minutes, the password becomes useless.

V. CONCLUSION

Cloud computing is relevant in providing valuable on-demand, elastic, scalable and reliable services to customers. A lot of effort and investment is saved by user while leveraging on applications and infrastructure provided by the CSP. Identity and access management is a critical issue in cloud computing. A malicious user can exploit can exploit the identity access to gain access to user credentials and information on the cloud. There are various architectures in place to ensure a secured IDMs. A lot of effort still need to be put in place to ensure a robust, all-encompassing IDM for cloud computing. It is recommended that more studies be conducted on cloud IDM policies and multifactor authentication on all Internet facing services.

ACKNOWLEDGMENT

We acknowledge the support and sponsorship provided by Covenant University through the Centre for Research, Innovation and Discovery (CUCRID).

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", NIST Special Publication, 2011, pp. 800-145.

[2] I. Odun-Ayo, M. Sanjay, G. Daniel and O. Nicholas. "Cloud Computing and E-Governance: Current Issues and Developments" Paper presented at the 4th Covenant University Conference On E-Governance in Nigeria (CUCEN 2017) Organized by Covenant University, Ota, Ogun State, Nigeria, 7-9 June, 2017, pp. 46 – 64.

[3] A. E. Youssef, Exploring Cloud Computing Services and Applications, Journal of Emerging Trends in Computing and Information Sciences, vol. 3, no. 6, July, 2012.

[4] I. Khalil, A. Khreishah and M. Azeem "Consolidated Identity Management System for secure mobile cloud computing", Computer Networks, 2014, pp. 99–11.

[5] I. Odun-Ayo, M. Sanjay, A. Olusola and A. Olasupo "Cloud Multi-Tenancy: Issues and Developments" Paper presented at the 4th IEEE/ACM International Conference on Big Data Computing, Applications and Technologies, (BDCAT 2017). Organized by University of Texas, Texas, USA, 5-8 Dec, 2017, pp. 209-214.

[6] I. A. Gomaa and E. Abd-Elrahman "A Novel Virtual Identity Implementation for Anonymous Communication in Cloud Environments", The 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2015), Procedia Computer Science, 2015, pp. 32-39.

[7] U. Habiba, A. G. Abassi, R. Masood and M. A. Shibli, "Assessment Criteria for Cloud Identity Management Systems", International Symposium on Dependable computing (PRDC 2013), 2-4 Dec, 2013.

[8] SETLabs Briefings, "Cloud Computing Identity Management", vol 7, no 7, 2009, pp. 45-54.

[9] I. Odun-Ayo, A. Falade and V. Samuel, "Cloud Computing and Open Source Software: Issues and Developments," Lecture Notes in Engineering and Computer Science: Proceedings of The International Multi-Conference of Engineers and Computer Scientists, Hong Kong, 14-16 March, 2018, pp. 140-145.

[10] M. Ali, S. U. Khan and A. V. Vasilakos, "Security in Cloud Computing: Opportunities and Challenges", Information Sciences, 2015, pp. 357-383.

[11] A. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", A. Abraham et al. (Eds.): ACC 2011, Part IV, CCIS 193, pp. 445-454, 2011. © Springer-Verlag Berlin Heidelberg 2011

[12] M. A. P. Leandro, T. J. Nascimento, D. R. Dos-Santos, C. M. Westphall and C. B. Westphall, "Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth", ICN 2012: The Eleventh International Conference on Networks, 2012.

[13] M. Stihler, A. O. Santin, A. L. Marcon Jr. and J. S. Fraga, (2012), "Integral Federated Identity Management for Cloud Computing", Accessed on 24 May 2017.

[14] G. Dreo, M. Golling, W. Homme and F. Tietze, (2013), "ICEMAN: An Architecture for Secure Federated Inter-Cloud Identity Management", Access on 24 May 2017.

[15] E. Bertino, F. Paci and R. ferrini, (2009), "Privacy-preserving Digital Identity Management for Cloud Computing" Accessed on 24 May 2017.

[16] D. H. Sharmaa, Dr. C. A. Dhote and M. M. Potey, "Identity and Access Management as Security-as-a-Service from Clouds", 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science, vol. 79, 2016, pp. 170-174.

[17] T. Spencer, (2012), "Identity in the cloud", Computer Fraud & Security 2012.

[18] M. Bradford, J. B. Earp and S. Grabski, (2014), "Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework", International Journal of Accounting Systems, vol. 15, 2014, pp. 149-165.
[19] I. Odun-Ayo, O. Ajayi, and A. Falade, "Cloud Computing and Quality of Service: Issues and Developments," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists, Hong Kong, 2018, 14-16 March, 2018, pp. 179-184.
[20] I. Odun-Ayo, T. Oladimeji, and B. Odede, "Cloud Computing Economics: Issues and Developments," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2018, Hong Kong, 14-16 March, 2018, pp. 190-195.
[21] J. Madden (2016) 'Cloud-based identity management services can work for your on-premises apps, too', TechTarget Computer Weekly Publication.
[22] T. Green "Gartner's top 10 security predictions", Network World Publication.
[23] E-Guide (2016) 'How I am Has Evolved on The Cloud: The Good and The Bad', TechTarget Publication.
[24] C. Anilkumar and S. Sumathy, "Security strategies for cloud identity management - a study," Int. J. Eng. Technol., vol. 7, no. 2, pp. 732–741, 2018.
[25] I. Odun-Ayo, S. Misra, N. Omoregbe, E. Onibere, Y. Bulama, R. Damasevičius "Cloud-Based Security Driven Human Resource Management System" Paper presented at the Eighth International Conference on the Applications Digital Information and Web Technologies (ICADIWT 2017) Organized by Universidad Autonoma de Ciudad Juarez, Juarez City, Mexico, 29-31 March, 2017, pp. 96-106.
[26] R. Garima and S. Rama, "A Review Paper on Cloud Identity Management Systems," in International Conference on Cloud Computing and Big Data, June, 2016.
[27] V. Monfort and K.-H. Krempels, Eds., Web Information Systems and Technologies, vol. 226. Cham: Springer International Publishing, 2015.
[28] I. Odun-Ayo, O. Nicholas, O. Modupe and A. Olasupo "Cloud Ownership and Reliability - Issues and Developments" Paper presented at 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2017). Organized by Guangzhou University, Guangzhou, China, 12-15 Dec, 2017.
[29] I. Odun-Ayo, F. Agono and Sanjay Misra, (2018), "Cloud Migration: Issues and Developments," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists, Hong Kong, 2018, 14-16 March, 2018, pp. 231-236.
[30] K. Khajehei, "Preserving Privacy in Cloud Identity Management Systems Using DCM (Dual Certificate Management)," Int. J. Wirel. Microw. Technol., vol. 8, no. 4, pp. 54–65, Jul. 2018.
[31] A. Salaria, "Biometric Identification and Token Generation Approach for Implementing Cloud Identity Management," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 7, no. 4, pp. 164–166, Apr. 2017.
[32] I. Odun-Ayo, O. Ajayi and N. Omoregbe, "Cloud Service Level Agreements Issues and Development", Proceedings of the International Conference on Next-Generation Computing and Information Systems (ICNGCIS, 2017), Model Institute of Engineering and Technology Jammu, India, 11-12 Dec, 2017, pp. 1-6. DOI 10.1109/ICNGCIS.2017.18.
[33] R. Bhandari, D. Patel, and B. Bhandari, "Improving Privacy of OpenID Cloud Identity Management Framework: Formal Analysis, Verification of Protocol," Int. J. Comput. Appl., vol. 180, no. 17, pp. 27–31, Feb. 2018.
[34] R. Yeluri and E. Castro-Leon, Building the Infrastructure for Cloud Security, vol. 13, no. 8. Berkeley, CA: Apress, 2014.
[35] J. Werner, C. M. Westphall, and C. B. Westphall, "Cloud identity management: A survey on privacy strategies," Comput. Networks, vol. 122, pp. 29–42, Jul. 2017.
[36] I. Odun-Ayo, C. Okereke and H. Orovwode "Cloud and Application Programming Interface - Issues and Developments," Lecture Notes in Engineering and Computer Science: Proceedings of the World Congress on Engineering 2018, London, U.K., 4-6 July, 2018, pp. 169-174.
[37] I. Odun-Ayo, O. Ajayi and S. Misra "Cloud Computing Security: Issues and Developments," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2018, London, U.K., 4-6 July, 2018, pp. 175-181.
[38] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," Eng. Sci. Technol. an Int. J., vol. 21, no. 4, pp. 574–588, Aug. 2018.
[39] P. Fremantle and B. Aziz, "Cloud-based federated identity for the Internet of Things," Ann. Telecommun., vol. 73, no. 7–8, pp. 415–427, Aug. 2018.
[40] I. Odun-Ayo, C. Okereke and H. Orovwode "Cloud Computing and Internet of Things: Issues and Developments," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2018, London, U.K., 4-6 July, 2018, pp. 182-187.
[41] M. T. Banday and S. Mehraj, "Directory services for identity and access management in cloud computing," in 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2017, pp. 334–337.
[42] I. Odun-Ayo, B. Odede and R. Ahuja "Cloud Applications Management: Issues and Developments", Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 10963 LNCS, pp. 683-694.
[43] R. Schulze, "Identity and Access Management for Cloud Services Used by the Payment Card Industry," in Cloud Computing – CLOUD 2018, vol. 10967, M. Luo and L.-J. Zhang, Eds. Cham: Springer International Publishing, 2018, pp. 206–218.
[44] K. Khajehei, "Role of Identity Management Systems in Cloud Computing Privacy," Int. J. Educ. Manag. Eng., vol. 7, no. 3, pp. 25–34, May 2017.
[45] I. Odun-Ayo, M. Ananya, F. Agono and R. Goddy-Worlu "Cloud Computing Architecture: A Critical Analysis", IEEE Proceedings of the 2018 18th International Conference on Computational Science and Its Applications (ICCSA 2018), Melbourne, Australia, 2-5 July, 2018, pp. 1-7. DOI:10.1109/ICCSA.2018.8439638.
[46] T. H. Vo, W. Fuhrmann, and K.-P. Fischer-Hellmann, "Privacy-preserving user identity in Identity-as-a-Service," in 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2018, pp. 1–8.
[47] M. Suguna, R. Anusia, S. M. Shalinie, and S. Deepti, "Secure identity management in mobile cloud computing," in 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 2017, pp. 42–45.
[48] U. Habiba, R. Masood, M. A. Shibli, and M. A. Niazi, "Cloud identity management security issues & solutions: a taxonomy," Complex Adapt. Syst. Model., vol. 2, no. 1, p. 5, Dec. 2014.
[49] I. Odun-Ayo, O. Ajayi and N. Omoregbe, (2017), "An Overview of Data Storage in Cloud Computing.", Proceedings of the International Conference on Next-Generation Computing and Information Systems (ICNGCIS, 2017) Model Institute of Engineering and Technology Jammu, India, 11-12 Dec, 2017, pp. 29-34. DOI:10.1109/ICNGCIS.2017.9.
[50] A. Kostopoulos et al., "Towards the Adoption of Secure Cloud Identity Services," in Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17, 2017, pp. 1–7.
[51] V. N. Dhatchayani and V. S. S. Sriram, "Trust aware identity management for cloud computing," Int. J. Inf. Commun. Technol., vol. 6, no. 3/4, p. 369, 2014.
[52] A. Bhardwaj and V. Kumar, "Identity management practices in cloud computing environments," Int. J. Cloud Comput., vol. 3, no. 2, p. 143, 2014.
[53] J. Werner and C. M. Westphall, "A model for identity management with privacy in the cloud," in 2016 IEEE Symposium on Computers and Communication (ISCC), 2016, pp. 463–468.
[54] C. Sullivan, "Protecting digital identity in the cloud," in The Cloud Security Ecosystem, Elsevier, 2015, pp. 149–170.
[55] A. Sarhan and L. Lilien, "An Approach to Identity Management in Clouds without Trusted Third Parties," in 11th Western Michigan IT Forum, 2014, pp. 18–27.
[56] S. Saini and D. Mann, "Identity Management issues in Cloud Computing," Int. J. Comput. Trends Technol., vol. 9, no. 8, pp. 414–416, 2014.

ISBN: 978-988-14048-5-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)