Review on Identity and Access Management for Cloud Platforms in Zimbabwe

Nunurai Loice Mhlanga
Department of Information Technology, Department of Information Science and Technology,
Harare Institute of Technology University
Harare Institute of Technology, P.O Box BE277, Belvedere Harare

***Abstract:-* Identity and access management (IAM) systems have evolved over the years with different degrees of adoption and use. Use of password and username remains one of the IAM systems being used by many firms across developing economies. However, it has emerged that such an approach has its own hassles and business implications. Among the several IAM technologies that can be implemented, SSO is gaining more market share due to its simplicity and robustness in securing cloud users especially against unauthorised access. Furthermore, it improves efficiency by allowing users to use the same credentials to log-on to multiple services. Enterprises prefer log-on systems than are more secure but delivering parsimony. This paper then provides some background on the development of IAM systems and the emergence of SSO before articulating on the reviewing on related work conducted by other researchers across the globe. The review of literature is aimed at priming the current study and giving insights into the possibilities of deploying SSO at New Generation Tech.**

Keywords: Accountability; Availability; Authentication; Authorisation.

INTRODUCTION

Modern technological working environments especially the cloud-based platforms are becoming more heterogeneous, dispersed, and hybridized such that more complex resources are needed to ensure that rightfully authorized network users get access to the right resources at the right time. [1]. Several studies have predicted that the compound annual growth rate (CAGR) of identity and access management (IAM) market size to be over 10% in 2018 and growing to over 13.21% by 2027. IAM has evolved to take on a number of forms depending on deployment model used, application field, or component of the management used. Password management, single sign-on (SSO), directory services compliance and governance, advanced authentication and audit are some of the different categories of IAM by component used. Based on application, IAM can be categorised as banking, financial services, insurance, manifacturing and education among other such functional areas. According to Dinesha [2], IAM can be categorised deployment model: on-premise or cloud-based. Empirical evidence shows that IAM systems usually work as hybrid of the above acategorised such as cloud-based SSO or advanced authentication for the financial services sector among others. SSO market is growing globally is tandem with the growing number of cloud and network users as more and more users are dependent on the Internet than on-premises services [3]. Shaulova [3] posits that SSO is growing at CAGR of 18.73% much higher than the global IAM growth rate suggesting that SSO is gaining more popularity among network and Internet users. Companies that are adopting SSO are recording higher revenues than those without. Firms adopting SSO in Europe record 46% higher levels of revenue than those without.

Usage of SSO in Africa and particularly in the sub-Saharan Africa is less known [3]. Single sign-on allows network users to use same credentials to access multiple services without the need to re-logon using different credentials [4]. Delivery of computing resources via the Internet as a service (IaaS) is gaining momentum. According to Galov [5], 83% of the workload for most users will be on cloud by 2022 and 30% of the information technology (IT) budgets will be allocated to cloud computing suggesting that the demand for SSO services will expontially grow. However, most companies in countries such as Zimbabwe still rely on password management systems without adopting SSO that is expected to reduce cloud users' number of passwords to use, improves productivity by allowing users to sign-on once using single set of credentials but access multiple services. SSO enhances organisational and cloud services security [4]. New Generation Tech is one Zimbabwean company that has invested significantly in offering its customers services through the cloud. However, the firm has not adopted the SSO technology risking its competitiveness given that a myriad of similar firms are joining the cloud services especially after the emergence of corona virus disease 2019 (COVID-19) global pandemic. It is argued in this paper that adoption of SSO by New generation Tech will not only improve its competitiveness in the hostile cloud services market, but also improves user productivity and hardens the cloud services security of the firm.

RELATED WORK

Reviewed literature indicates that identity and access management (IAM) is not a one size fit all nor is it one common strategy to manage access of online services remotely by cloud users [4] [5]. There are a number of strategies that can used including federated access management solutions, single sign-on systems, password management and auditing to build accountability of the user of computing resources [7]. However, the surveyed literature seems to show that the use of each of these strategies is not uniform from one firm to another. For instance, Beal [1] argues that federated access management is better strategy in that it gives users better options of using multiple credentials in a more fragmented working environment. However, [14] point out that use of federated access management (FAM) has its downside. First, the strategy has trustworthy challenges as in most cases it is provided by several identity providers (ID providers) whose trust may be uncertain especially in the contemporary cloud computing environment when hacking challenges are commonplace. Bhutani [1] argues that FIAM may result in multiple digital identities and credentials that may be cumbersome to remember and attributed to specific users. A simple mix-up of credentials may result in system oscillations and security instabilities. The risk of identity theft cannot be ruled out. In addition, the use of security assertion mark-up language (SAML) and OpenID may result in compromise of the scripting systems. Against the empirical weakness of FIAM, adoption of robust SSO becomes pertinent.

Exploration of the adoption of other IAM technology solutions showed that robust SSO in a cloud environment may offer better security solution without compromising on the efficiency most sought by the enterprises [6]. In a study conducted by Nida [14] to try and explore how effective IAM can be implemented. The study made use of reviewing empirical studies conducted in the past and in different cloud working environments. Several papers were reviewed that showed that most of the contemporary IAM solutions are offered by cloud vendors. There is limited scope of individual firms developing and adopting their own SSO solutions to their own specifications. According to Shinder [8], IAM systems are being offered as standalone Internet-based online solutions. There are a number of firms that are competing to develop and sale their IAM as a service. It is part of the security as a service (SaaS) solution for the cloud computing environment. Dhairu [4] laments that the growing number of vendors are increasing costs of running cloud services. Some firms charge significant costs per demand of service. This is especially true for firms in developing economies who can hardly afford to procure and use licensed software solutions worse for security they perceive as optional [9]. Developing in-house solution for firms experiencing financial constraints is unavoidable and pertinent. This study intends to develop such a solution for New Generation Tech in Zimbabwe.

SSO solution is most appropriate if hosted on a virtual environment [3]. Access to cloud computing should be on-demand and scalable. The IAM platform may need to be scalable to reflect the dynamic nature of demand for cloud services [9]. Most previous IAM solutions have relied on standalone server systems that consumes considerable amounts of hardware and financial resources. Shifting focus to virtual environments improves scalability and optimisation of existing hardware and software infrastructure [2]. Therefore, this study proposed to make use of virtual machines (VM) existing at New Generation Tech to host the IAM solution. This was expected to be dynamic and scalable enough to accommodate the trending number of New Generation Tech cloud services customers.

Mohammed [15] sought to understand the significance of IAM solutions for different businesses. The author explored the use of artificial intelligence in the authentication process of the IAM system. The researcher sought to understand if it was possible to fuse artificial intelligence (AI) in the authentication process of the IAM system and discovered that not all features of the AI can be deployed for a functional IAM solution. The study discovered that use of AI in federated access management environments worsened users' ability to remember dynamic changing user passwords and related responsibilities. AI increased the complexity of the IAM system. Information technology personnel had to repeat work in most cases to train the system and also to manage their users. AI increased the risk of users being able to access resources and data inappropriately. This was also echoed by Chen [13]. Integrating AI into the IAM system only increased the complexity of the IAM system with increasing the risk of poor accountability of the activities of the users. It also increased burden in the users to remember many passwords and effort to learn to be more interactive with the intelligent modules.

Ishaq [15] also sought to explore how IAM alternative solutions function in a multinational information-sharing environment for the security and defence firms. Multinational and information sharing environments require trailing users and improving visibility and accountability of each user. Such type of environments is sensitive and prone to significant security breaches. Therefore, improved identity and access management systems become imperative. In security and defence type of working environment, Galov [5] propounds that information has to be shared quickly while at the same time attempting to limit unauthorised access to information. This requires authentication and identification systems that are responsive and quick. The study therefore sought to understand how the Department of Defence (DoD) of America was maintaining and deploying its IAM resources. The study established that DoD deploys multiple IAM resources and tools in terms of technologies and policies. IAM for DoD is not a single set of solution but an array of processes, tools and policies. As observed by Lee [16], such complex IAM are appropriate for large firms and national departments as opposed to small sized firms. Small firms can hardly maintain such complex array of resources. Moderate set of IAM architecture that achieves similar security and efficiency requirements may be needed [4].

Lauri [17] investigated the possibilities of standardising the IAM solutions for large European company in the pharmaceutical industry. The study was focused on identifying the whole array of IAM solutions deployed across different countries and recommend for a standardised IAM system. The case study design made use of survey questionnaires among experts from different firms across different countries in Europe. The survey data was analysed statistically to find the possibilities of standardised IAM solution for Europe. The results showed that due to multiplicity of needs of different firms and different models of IAM used, it is difficult to standardise such a solution. Therefore, the above discourse clearly indicates that IAM is a complex set of strategies whose superiority depends on the context being explored. Firms in developing economies might find it difficult to deploy complex IAM tools and processes as for the DoD of America. Locally developed solutions might be more appropriate to suit their developmental contexts.

SUMMARY OF THE REVIEW AND RESEARCH GAP

Surveyed literature clearly shows that cloud computing is on-demand and ever increasing. Yet there is no consensus as to the appropriate access and authentication system for the cloud services customers [2]. However, there is common agreement that utilization of cloud computing services requires strict control of access and authentication checks for each customer. There are several ways of authenticating cloud services customers: bio-metric, 3D password, third party authentication, graphical, and textual authentication. Designing and implementing an effective authentication system is particularly critical for cloud computing [6]. Failure to implement an effective authentication system may allow attackers to even take control of the accounts and activities of the bona fide cloud services customers. Several models have been proposed for service providers to allow cloud users to use single sign-on (SSO) for multiple cloud services.

Chen and team proposed a combination of OAuth protocol in combination with identity federation and identity mapping to enable a new form of single sign-on model for the cloud users [13]. In this model, OAuth-based single sign-on solution was proposed and the empirical results showed that the strategy enabled users not to repeatedly enter their username and passwords to access different cloud services. However, the proposed model has not been applied across different cloud services scenarios especially in environments that serves numerous cloud users. There has not been much understanding of how this model works especially where multiple security domains may be impacted. For instance, it is not clear how such a model may be operational for private cloud as that offered by New Generation Tech in this case. Though, the model proffered opportunities for complexity identity management and may improve user efficiency, its value against other techniques remains unclear.

Furthermore, the surveyed literature does not empirically demonstrate how a specific IAM solution such as use of SSO with virtualised directory services can be designed and deployed. The current research attempts to fill up this gap by fusing virtualisation into the directory services and SSO infrastructure. It is hoped to improve robustness of the solution in terms of scalability and efficiency.

CONCLUSION

This review discussed the past studies related to designing and development of IAM solutions. Particular focus was on exploring the deployment of SSO integrated with a virtualised directory service. The surveyed literature showed increasing adoption of IAM solutions but with multiplicity of diversities of strategies. Federated identity and access management is popular but complex and risks users inappropriate use of resources. It also increases burden of users having to remember many sets of credentials. There surveyed clearly indicated numerous gaps to be filled especially with respect to finding solutions appropriate for firms in developing economies such as Zimbabwe. The research gaps clearly show the widening gap in orientation and deployment of IAM solutions. There is need to develop a solution for small firms in developing countries with less resources but harnessing all the current technologies on offer.

ACKNOWLEDGEMENTS

I would like to thank Jehovah for granting me the wisdom and knowledge to undertake this research, without him I would have not been able to complete the research. I would also like to thank my Supervisor Mr. Bakasa for his support and guidance throughout the research without whom I would have not gotten far. My deepest gratitude to my family for their unwavering support and understanding during the time of the research.

REFERENCES

[1] A. Bhutani, “Identity and access management (IAM) market size by solution,” Global Market Insights , Washington DC, 2018.

[2] H. A. Dinesha and V. K. Agrawal, “Multi-level authentication technique for accessing cloud services,” *International Conference on COmputing, communication and applications* , vol. 10, no. 1, pp. 1-4, 2018.

[3] S. Shaulova , “Global single sign-on market share,” Veracious Statistics Research , New York, 2021.

[4] A. A. Dahiru, J. M. Bass and I. K. Allison, “Cloud computing adoption in sub-Saharan Africa: An analysis using institutions and capabilities,” in *Society 2014*, Lancashire, 2016.

[5] N. Galov, “Cloud adoption statistics for 2021,” Hosting Tribunal , Washington DC, 2021.

[6] R. Carvalho, “Cloud computing authentication security with diversity and redundancy,” Instituto Superior Tecnico, Madrid, 2014.

[7] Verified Market Research , “Identity and access management market worth $29.29 billion, globally by 2027 at 13.21% CADR,” Cision PR Newswire, New York, 2021.

[8] C. Shinder, “Idenity and access management in the cloud,” Technet, New York, 2021.

[9] Deloitte, “Cloud and identity and access management,” Deloitte, London, 2018.

[10] S. Radoslav, “37 heavenly cloud computing statistics for 2021,” Tech Jury, New York, 2021.

[11] V. Beal, “Identity and access management (IAM),” TechnologyAdvice, New York, 2021.

[12] I. A. Mohammed, “The interaction between artificial intelligence and identity and access management: An empirical study,” *International journal of creative research thoughts* , vol. 3, no. 1, 2015.

[13] G. Chen, Y. Du, P. Qin, L. Zhang and J. Du, “A new single sign-on solution in cloud,” *Cmputer engineering and networking* , vol. 277, pp. 755-761, 2013.

[14] Nida, Pinki, H. Dhiman and S. Hussain, “A survey on identity and access management in cloud computing,” *International journal of engineering research and technology,* vol. 3, no. 4, 2014.

[15] I. A. Mohammed, “Analysis of identity and access management alternatives for a multinational information-sharing environment,” *International journal of advanced and innovative research* , vol. 1, no. 8, 2012.

[16] B. Lee, “SSO is not identity management,” Jump Cloud , New York, 2021.

[17] L. Laitinen, “Case study on identity and access management in an EU level pharamaceutical company,” Aalto University , London, 2016.