International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 11 Issue 4, April- 2021
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

IDENTITY AND ACCESS MANAGEMENT BASED ON IAM GOALS AND INDICATORS IN CLOUD COMPUTING- A REVIEW

Shabana Parvez Mulla[1], Dr. Amit K Srivastav[2]

Department of Management

[1,2]Capital University, Koderma, Jharkhand, India

ABSTRACT:

The current rise in popularity of cloud-based web services can be linked to the fact that these services are not only simple to use but also economical. This is made feasible by the utilisation of a wide variety of malleable service models, including as IaaS, PaaS, and SaaS, in addition to multi-tenancy, which makes it possible for several users to share the same resources. The dangers that are connected with these service models, particularly those that concern to one's privacy and one's security, are significant. The hazards that are linked with these service models. This study is review work of previous studies which signifies the stand that how important IAM performance is in addition to its infrastructure qualities and examines how those IAM objectives are necessary to establish sustainable IAM management in an organisation. This strategy is made to be quickly upgraded to support a business's changing needs.

Keywords: IAM, Cloud Computing, Goals, Management

INTRODUCTION:

Cloud computing is becoming increasingly important to today's corporations as a means of meeting the demands of modern businesses. The present popularity of cloud web services can be attributed to the fact that they are easily accessible and cost effectively. This is made possible through the use of numerous adaptable service models, including IaaS, PaaS, and SaaS, as well as multi-tenancy. The risks that are associated with these service models, particularly those that pertain to one's privacy and one's security, are significant(Jonker & Petković, 2014). Businesses require a dependable, flexible, modular, and user-centered Public key Infrastructure (IAM) technology in order to decrease the risks associated with cloud web services. Because it stops unauthorised users from accessing the cloud web service, the integration of authentication and attribute-based access control makes the programme run more efficiently(Committee, 2011; Pullman & Streff, 2007). Because digital technology is advancing at a rate that has never been seen before, and because it is anticipated that By 2020, the Iot technology (IoT) will connect over 1.5 trillion unitsthe year 2025, businesses are being forced to adapt to a rapidly shifting technological landscape that has eliminated traditional organisational boundaries. Every industrial organisation is seeing a shift in their business models, societal norms, legal framework, and number of digital identities as a result of the increasing adoption of various mobile devices and the expanding number of digital identities.

As businesses work to keep up with the latest technological developments, many of them are looking for advantages that cloud computing can provide. These advantages include Simple application login, flexibility to choose and use the functions which are most suited for their needs, and minimal maintenance (apart from setup, there are no hardware or existing financing). But at the other approach, homogeneous architectures that include cloud services, on-premises services, and a diverse range of devices provide a number of security difficulties, particularly with regard to authentication and encryption(L. Fuchs et al., 2011).In addition, new privacy regulations, as well as rules that continue to evolve, frequently necessitate a review of existing practises to ensure that they continue to be compliant.

In order to find a solution to these problems, businesses will require an identity management and access control approach that is integrated, consistent, and centralised. This article introduces Identity Access Management Goals and its indicators' relevance with the intention of assisting businesses in simplifying, optimising, and improving identity and access management across on-premise as well as cloud-based software platforms. It brings up how the performance of IAM is equally important as its infrastructural attributes are and explores how those IAM goals are mandatory to create a sustainable IAM managementin an organisation. This strategy is designed to be easily adapted to meet the shifting demands of a business. A lot of companies have put in place Authentication and Authorization (IAM) solutions enable organisations to reap from the many advantages of using the cloud yet reducing the dangers associated with worries about confidentiality and security. Network security, or IAM, is a field of study that ensures the appropriate people have access to the appropriate resources somewhere at appropriate times as well as for the appropriate purposes (Witty et al., 2014). In addition, dangerous cloud infrastructure is protected by the network security monitoring systems. This enables client access control to be trustworthy and practical, which is crucial for the website of any firm. On the other hand, identity access management (IAM) is not a miracle cure, nor does it eliminate all of the privacy and security risks that are connected to cloud computing. In addition, different firms that fall under the purview of the IAM may have requirements for unique identities (or duplicate identities). This paper aims at reviewing the related researches and literature in the domain of IAM Goals and its Indicators. In this paper we will be bringing forth all the related studies that have stated about the IAM Goals.

Methodology Adapted:

This study adopted the reviewing approach of the previous studies in the same area of research, and there by evaluating all the aspects that was brought to light in the prior studies related to the IAM Goals and Indicators. The first step was screening up of the relevant papers for which we included 2 databases Scopus , Proquest and EBSCO. The initial screening process gave us 725 articles, which after screening on the basis of our required criteria the number of articles finally we found relevant for our study came to 10. The review of those 10 research papers are mentioned below.

Literature Rationale:

The existing IAM research does not provide performance metrics of IAM in general and focuses mostly on particular technical or organisational aspects of IAM infrastructures. Literature in research and practise (Advisory, 2009; L. Fuchs et al., 2011; Ludwig Fuchs et al., 2009; Hovav & Berger, 2009; Steven & Peterson, 2006) highlights the fact that the primary drivers for modern IAM in organisations are risk reduction, IT cost reduction, compliance requirements, data and process quality, and business facilitation.

These factors have the potential to serve as a jumping off point in the process of developing performance metrics for long-term IAM maintenance. For example, this researchers note the significance of reviewing and evaluating IAM systems in numerous of their papers ((Ludwig Fuchs et al., 2009; Hovav & Berger, 2009; Hummer et al., 2018; Steven & Peterson, 2006)These publications may be found on Royer's website. They apply the concept of balanced score cards to IAM, thereby giving a generic technique for measuring the performance of an IAM system. To evaluate the worth of IAM systems, they concentrate the majority of their attention on financial issues. They have aims that are comparable to ours. The study contend that it is necessary to take into account the overall performance of IAM as an enterprise-wide cross-cutting functionality in order to be successful.

(Witty et al., 2014)) outlined a number of assessment dimensions that can be used to compare different architectural approaches to federated environment access control. They use these dimensions as a basis to construct metrics for evaluating the performance of an IAM system in the work that is referred to as (Advisory, 2009).

However, the majority of the attention is directed toward the architecture, and researchers think of performance as a quantitative measurement that is determined by how long the activities of the various systems take.

According to standards, performance means having a broader viewpoint than those standards, which focus on an IAM system's capacity to make judgments in a timely manner. (Ludwig Fuchs et al., 2009)conduct a systematic literature review in addition to an architectural trade-of, analysis method (Steven & Peterson, 2006) in order to derive requirements and metrics for authentication and user profiles in Identity Management architectures. This study was published in (Jonker & Petković, 2014)publication. These measurements, on the other hand, put an emphasis on the architecture's underlying technological implementation. The indications that are provided by (Steven & Peterson, 2006)allow for the measurement and management of risk inside IAM systems. They present some helpful metrics that may be used to determine whether the execution time of requests and the delivery of access permissions are satisfactory in their current state. Their strategy places an exclusive emphasis on the areas of lowering risks and enhancing the quality of processes, while ignoring the significance of a number of other important domains.An overall perspective and judging from a top-level goal that IAM centres around have not yet been addressed. Neither of these issues have been resolved.

Findings And Conclusion:

This study has laid down a path of bringing up the fact to summarise, throughout the course of this study, we were able to show that many IAMs are relevant and exist is a need. Indicators that contribute to the analysis of an already established IAM By Upon determining that they were applicable to real-world settings, we were able tosupply academics and industry professionals with useful information outcomes in regard to the manner in which IAM performance can be expressed quantitatively or qualitatively, whichever is more appropriate. Using our findings as a starting point, the first step towards a holistic approach of having an IAM measurement framework which can lead the researchers to come up with various constructs and tools to evaluate different tangents related to the IAM goals and Indicators in an organizational level.

Towards the conclusion it is concluded that the currently available research on IAM does not provide performance measures of IAM in general but rather focuses mostly on specific technical or organisational features of IAM infrastructures. Therefore, we would recommend that there lies a huge scope of developing scales relevant to measure the performance of IAM specifically related to the objectives that they are intended to achieve so that the sustainability of IAM in Cloud Computing is maintained.

References:

Advisory, K. I. T. (2009). *Report findings at a glance*. http://news.bbc.co.uk/1/hi/health/1445747.stm

Committee, B. (2011). basel III a global regulatory framework. In *Basel Committee on Banking Supervision, Basel* (Issue June). http://www.bis.org/publ/bcbs189_dec2010.pdf

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security - A survey and classification of the research area. *Computers and Security*, *30*(8), 748–769. https://doi.org/10.1016/j.cose.2011.08.002

Fuchs, Ludwig, Broser, C., & Pernul, G. (2009). Different Approaches to in-house Identity Management. *ARES '09. International Conference OnAvailability, Reliability and Security*, *n.a.*(n.a.), 122–129.

Hovav, A., & Berger, R. (2009). Tutorial: Identity management systems and secured access control. *Communications of the Association for Information Systems*, *25*(1), 531–570. https://doi.org/10.17705/1cais.02542

Hummer, M., Groll, S., Kunz, M., Fuchs, L., & Pernul, G. (2018). Measuring identity and access management performance - an expert survey on possible performance indicators. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-January*(January), 233–240. https://doi.org/10.5220/0006557702330240

Jonker, W., & Petković, M. (2014). Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8425 LNCS*, 9–13. https://doi.org/10.1007/978-3-319-06811-4

Pullman, N., & Streff, K. (2007). Identity and access management. *Managing Information Assurance in Financial Services*, 208–239. https://doi.org/10.4018/978-1-59904-171-1.ch010

Steven, E. J., & Peterson, G. (2006). Introduction to identity management risk metrics. *IEEE Security and Privacy*, *4*(4), 88–91. https://doi.org/10.1109/MSP.2006.94

Witty, R. J., Allan, A., Enck, J., & Wagner, R. (2014). *Identity and Access Management Program Plan*. *June*, 1–33.