www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

Identity and Access Management: High-level Conceptual Framework

Sanket Devlekar[1]; Vidyavati Ramteke[2*]

[1]Symbiosis Centre for Information of Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India.

[2*]Symbiosis Centre for Information of Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India.

[2*]vidyavati@scit.edu

Abstract

Information security is shifting from a traditional perimeter-based approach to an identity-based approach where the organization's boundaries are where their digital identities exist. The organization has multiple stakeholders having access to various organization resources. Systems and applications are part of organization resources that help them achieve their business goals. These systems and applications are internally or externally exposed to allow all stakeholders to have seamless access, thus making identity and access management a big challenge. Identity and Access Management (IAM) is a fundamental part of information security. It plays a critical role in keeping the organization's information security posture resilient to cyber attacks. This paper will identify various components of an IAM solution that are essential and should be considered while implementing and assessing the IAM solution and provides a high-level IAM framework that will allow information security professionals to assess the IAM security posture of an organization.

Key-words: Identity and Access Management Framework, IAM Framework, Identity Management, Access Management, Cyber attacks.

1. Introduction

"74% Of Data Breaches Start With Privileged Credential Abuse." This paper highlights the importance of identity and access management, whereby a robust IAM implementation can prevent unauthorized access. Identity management is a critical infrastructure. Cyberattacks target and exploit centrally positioned IAM infrastructures and compromise the whole organization even compromise critical societal services and critical infrastructures and therefore be high relevance in security [1]. An IAM framework is a flexible, scalable framework that provides a security architecture used to provide

information security. IAM solutions can be deployed on-premises or off-premises, i.e., on the cloud. Businesses are looking for digital transformation to take advantage of the latest technological advancements, which is visible from the rapid adoption of SaaS and PaaS-based solutions. With the sudden change in global situations, organizations must adopt the cloud. It is not merely a digital transformation move but also a business continuity measure, which is evident from the rapid adoption to cloud services in the recent pandemic [2]. Though security and privacy are the main reason for reluctance for an organization to adopt cloud solutions aggressively. The IAM solution provided by the cloud platforms can be a possible solution to minimize security risks.

Cloud services are capable and mature to manage the security risk if the right security controls are carefully implemented. An IAM system deployment is not limited to any framework, but many arrangements are possible based on organization requirements [3]. For this paper, the IAM components described in the IAM framework are classified into three categories: identity repository, identity management, and access management. These three categories are the key focus areas in the further proposed high-level IAM security framework.

2. Literature Survey

The works (United States Patent Application Publication Patent No. US 2008/0028453 A1, 2008) (Sullivan, 2009) (F. Damon and M. Coetzee, 2013) indicate frameworks that reflect the components that a security professional must dwell in determining the IAM security posture of an organization. The framework observed by Sullivan gives a conceptual framework for identity and access assurance based on SABSA (Sherwood Applied Business Security Architecture). Whereas (United States Patent Application Publication Patent No. US 2008/0028453 A1, 2008) (F. Damon and M. Coetzee, 2013) describes various components techniques and technologies required for an IAM implementation [4]. Security controls are essential for accountability and auditing. External auditors examine and verify the internal controls established by the client, many of these controls are associated with access controls, for example, logical access. ISACA guides auditors regarding IAM assessment relative to regulations, standards, and framework. Cloud-based IAM solutions are SaaS, PaaS, and IaaS offerings [5]. Microsoft provides product IAM solutions via Active Directory services in their server operating system offerings which can be deployed in-house. It also offers a cloud-based IAM solution via its Azure cloud services. Similarly, AWS offers SaaS-based products. Organizations can set a hybrid IAM implementation using Microsoft products running on AWS instances. The trend for cloud IAM solutions is heading for standardization, which is evident from

adopting open standards like SAML 2.0, OAuth, OpenID, which is possible for vendors by providing cross integration and adopting open standards in their IAM offerings. The efficiency and effectiveness of an IAM implementation can be pegged against whether it meets the organization's business, statutory, regulatory, and contractual requirements and secondly to maintain Confidentiality, Integrity, and Availability (CIA- triad). There is a shortage of a holistic approach to meet both these requirements. The existent research either focuses on either technical or business aspects of security aspects. However, a holistic approach is required for an efficient and effective IAM implementation. This paper proposes a framework that attempts to encompass all the latest trends and factors that need to be considered to implement secure and effective IAM solutions [6].

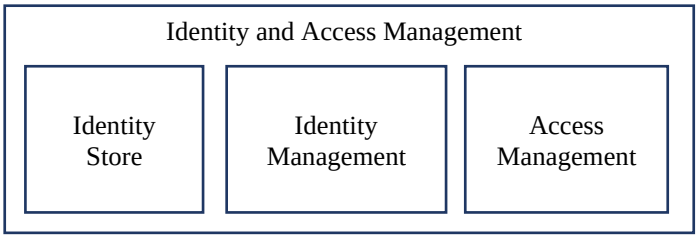
3. Overview of Identity and Access Management

Identity as an identity has evolved from a traditional perimeter-based security model to identity-defined security. Organizations are increasingly required to distribute and mobilize, either by employees working from remote locations or teleworking, wherein lies the foundation of the management of identity throughout one's whole lifetime. It describes how the personal data evolves over a lifetime and what implications this evolvement has over the management of these identities by laying down the building blocks [7]. Organizations need to implement identity management to:

- Reduce costs and improve operational performance.
- Compliance with regulations.
- Enable more agility in business operations.
- Mitigate risks.

Identity and access management is the collection of technologies, processes, and policies for managing, controlling, and protecting access to organization resources. It involves managing digital identities their authorization within or across system and enterprise boundaries to increase security and productivity. The impact can be measured across three areas: reduces cost, increasing operational efficiencies, and improving employee productivity [8]. A view is required for IT professionals to create a robust and secure IAM implementation.

Figure 1 - IAM Components



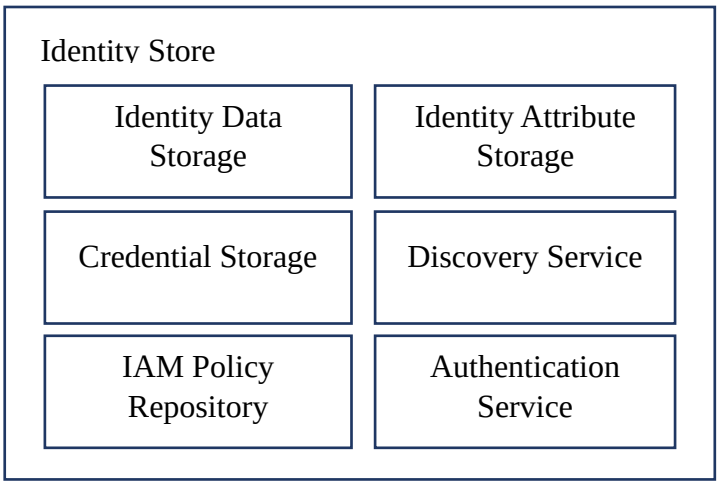
Received: 19.07.2021 – Accepted: 18.08.2021

Figure 1 provides an overview of the core components of the IAM framework. Each component is a group that contains subcomponents that will be essential in assessing IAM security posture. The first component is Identity Store broadly includes identity storage, credential storage, discovery, and authentication services. Identity management includes functions related to identity administration; typically, this is done by establishing an identity lifecycle management process [9]. Access management refers to the process and technologies used to access the organization's specific application, information, and resources based on certain rights and privileges.

3.1. Identity Store

Digital identity is the representation of any individual or entity in an electronic format. It can be a person, process, service, or resource in an IT system. It refers to the unique identifiers and set of associating attributes. A digital identity can be mobile; mobility can be from devices, physical location, and context. This aspect helps in creating context-aware applications. Identity Store is the location where users (digital identities) and roles are managed. The identity store stores the identity data in a particular schema. A schema consists of entry types and attributes that describe how different identities are represented in the database. Provisioning is based on the identity data stored in the identity store. Workflows are determined based on the processing of this data. Business roles and privileges are also stored here. It is done by a role-based access policy (RBAC) or attributes-based access policy (ABAC). An identity repository has the following sub-components, structured data storage where identity information is stored, attribute storage that stores the additional attributes, and service to make the data available to network users and administrators [10].

Figure 2 - Components of Identity Store

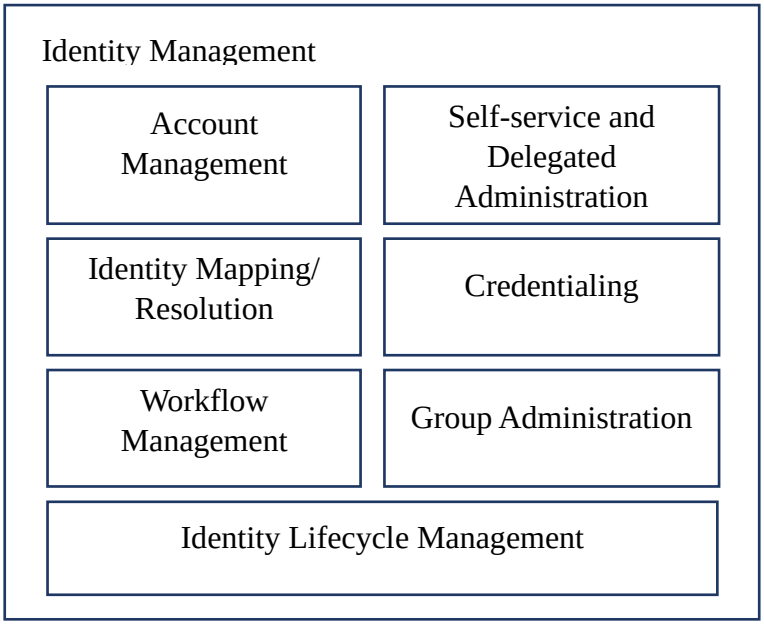


Received: 19.07.2021 – Accepted: 18.08.2021

Components of Identity Store are given in Figure 2. Identity stores are of two kinds internal or external. Identity store is implemented using Active Directory, Custom store with LDAP server/ Server built-in store or using a Cloud IAM solution.

3.2. Identity Management

Figure 3 - Components of Identity Management



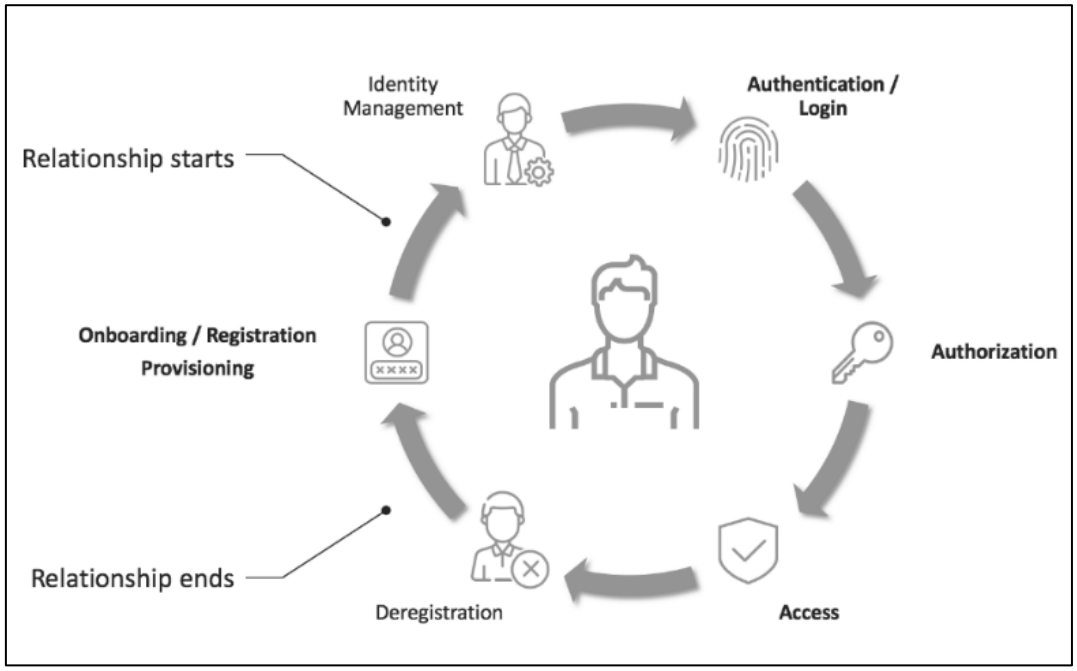
Components of Identity Management are shown in Figure 3. Identity management refers to the process essential for maintaining and managing the entire cycle of digital identities and their attributes. There are three ways to implement identity management from various cloud scenarios: in-house, as a service, and hybrid solution, as observed by E. Bertino. In the in-house alternative, identities are managed by organizations themselves, and the onus of maintenance and security is on them [11]. Identity management implemented via outsourcing, utilized by service providers are also known as IDaaS (Identity as a Service). There are companies having enterprise IDaaSs products with powerful integration. The third is the hybrid implementation, where there is a need to integrate identity solutions of multiple service providers. Each cloud provider may provide its own IAM services. These can be all integrated with the help of open standards and protocols or proprietary connectors. Also, the privacy and security concerning identity management and the findings describe areas for designing an identity management system [12]. Concerning the United States Patent Application Publication Patent No. US 2008/0028453 A1, 2008, we can collate major components in identity management, as shown in Figure 3. Table 1 shows widely used technologies for different ways of IAM implementation:

Table 1 - Used Technologies for Different Ways of IAM Implementation

Type	Examples
1. On-premise	Corporate directory. E.g.: Microsoft Active Directory, Open LDAP, Oracle Identity Store (OID), LDAP user store
2. Cloud	Cloud IAM. E.g.: AWS IAM, Azure IAM, Oracle IAM, Goggle Cloud Identity, etc. Internet identity providers. E.g.: Login with Google, Amazon, Facebook, or any Open ID Connect (OIDC) compatible identity provider.
3. Hybrid	Federating existing users. E.g.: AWS AD, Azure AD, Oracle Net Service, etc.

3.2.1. Identity Lifecycle

Figure 4 - Identity Lifecycle



The digital identity lifecycle in Figure 4 represents each stage of identity within an organization. It describes the phases in which an identity goes through in an organization. First, the onboarding process takes place. From here onwards, the relationship starts then an integrated identity management platform handles the administration of the identity. An onboarding process involves the

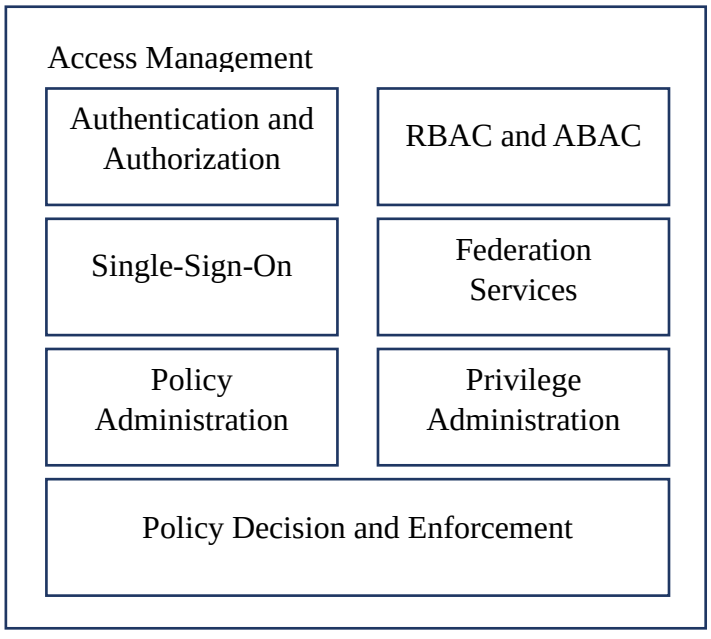
creation of digital identity [13]. It is usually carried out by HR and within the human resource management system (HRMS). Provisioning is all about providing the digital identity appropriate access to the resource. It involves provisioning and designs-provisioning resources to entities. Based on the business role and privileges, the authentication mechanism is configured for that identity, which also involves giving authorization and access to the right resources based on the principles of least privileges. Once the lifespan of the identity is served, the human resource management system initiates a deregistration process. The digital identities are managed using an identity lifecycle management process defined in companies' IAM policy [14].

Access management includes the processes and technologies that allow users to access organization resources. Under access management in IAM, we talk about a process that performs three primary activities: Identification, Authentication, and Authorization.

3.3. Access Management

Identification is a process of describing an entity to the system with the help of a unique identifier. Authentication involves verifying the claim of the entity it claims to be, which is commonly done through user credentials. Authorization is the process of determining rights (policy decision) and ensuring only authorized rights are exercised (policy enforcement). Components of Access Management are shown in Figure 5.

Figure 5 - Components of Access Management



3.3.1. Access Control Models

The user receives (rights) roles and privileges based on access control models. Access control models include both physical and digital access control. Following are the various access control models:

1. Mandatory Access Control (MAC): Control's access is based on matching objects security labels with hierarchy levels (e.g., Top Secret, Confidential, Secret), and access is strictly controlled by an administrator, usually implemented in government systems.

2. Discretionary Access Control (DAC): Control's access is based on the discretion of the object owner. The owner decides on which subject gets access to objects based on some set of rules. An administrator manually gives access to the user to a system or application based on his or her discretion. Operating systems like Linux, Windows, and UNIX are based on DAC [15].

3. Role-Based Access Control (RBAC): Control's access is based on roles defined in an organization, e.g., Manager, Administrator, HR, and Intern

4. Attribute-Based Access Control (ABAC): Control's access is based on the following types of attributes: user attributes, attributes related to application or systems, and present environmental conditions like location, time, etc.

5. File System Security: The file system on operating systems has read, write and execute access assigned to user and group.

6. Network Access Control (NAC): It is a method of controlling and securing devices user access to their network, e.g., CISCO ISE.

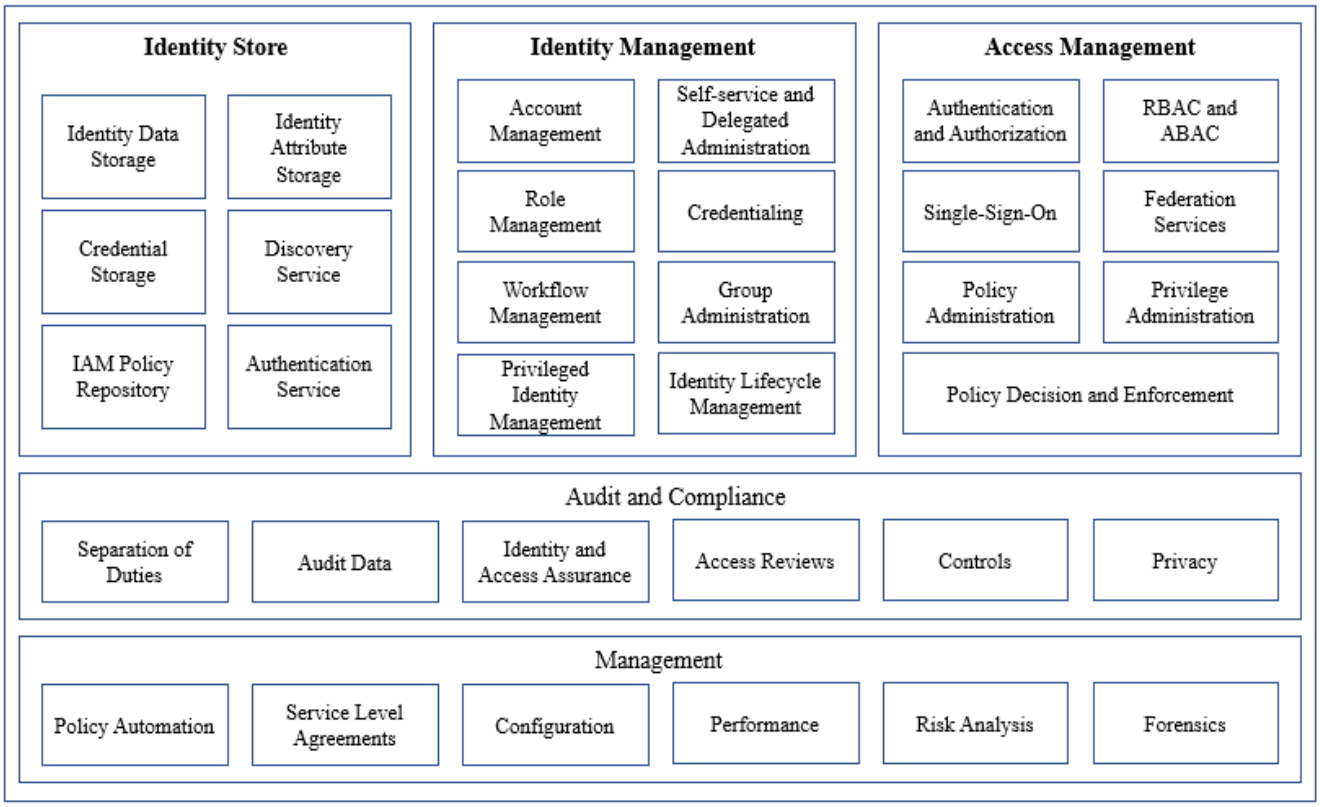
RBAC and ABAC are the most widely used access control models in an IAM system within an organization. RBAC uses the roles within the organizations to grant access to resources [16].

4. Proposed IAM Framework

The final IAM framework is introduced in Figure 6, consisting of components and subcomponents within an IAM solution.

The framework contains five main components which a security professional should consider while performing a security assessment. It can also be used by organizations that are undergoing IAM implementation or looking to upgrade. They can create a roadmap to evolve their current IAM state to an advanced IAM implementation by referring to various components and subcomponents [17].

Figure 6 - IAM Framework



4.1. Components

4.1.1. Identity Store

It includes subcomponents that are mainly storage-based (identity storage, attribute storage, credential storage, and policy repository) and discovery and authentication services required for access to the storage.

4.1.2. Identity Management

Includes essential areas for managing the identities to using the identity store. Account management involves CRUD operations on identities. These actions are performed because an identity goes through various modifications, for example, location change, profile update, new projects, new requests, etc. Self-services and delegated administration are also required to avoid frequent requests from the IT administrators. It enables users to perform certain tasks, such as password, reset, assign roles, increase privileges, etc. Delegation of such tasks or having a self-service mechanism improves user experience and increases accountability. Credentialing is a process that allows checking the

eligibility of an entity for a particular task or action, which goes along with role modeling, where the roles for any user are determined based on the organization's HR policy. Group administration functionality allows administrators to group entities and apply rules and controls on them. One area of concern was managing users and roles associated with the administration of systems and applications; such identities are called privileged identities. It is essential to have strong control and management on such accounts, like root access, which significantly affects business operations. Privileged identity management monitors and protects super user accounts in the organization. The process and workflows in the IT systems are managed by an identity and access management lifecycle process, varying from organization requirements and IAM maturity [18].

4.1.3. Access Management

Access management includes authentication and authorization mechanisms, RBAC and ABAC, SSO, Federation services, policy administration, privilege administration, and policy decision and enforcement. Authentication mechanisms vary based on the access assurance defined based on the IAM policy, which may require the adoption of multifactor authentication (MFA). IAM systems widely use RBAC and ABAC for authorization and setting up accountability [19].

4.1.4. Audit and Compliance

This includes separation of duties (SOD) policy, audit logs, identity and access assurance, access reviews, controls, and privacy. One of the key policies in an organization is the SOD policy, which serves as an internal control to prevent errors and fraud. It is an attempt to have checks and balances in place so that no single individual can perform tasks [20]. One aspect of compliance with standards and regulations requires having audit logs. Audit logs record operations that modify the configuration or metadata of resources. It enables for setting automated responses to the event and in the case of forensics. Identity and access assurance mechanism ensure that the entities access to organization resources based on a set of rules and varying access levels, observed Sullivan. Access reviews are also referred to as Access certification, which is validating access rights within systems or applications [21]. Periodically, managers, application owners, or business stakeholders must review current user privileges and identify risks. It is mandatory for compliance and risk management. An IAM system has various technological components, which need to be configured with necessary security controls. This set of security controls is technology-specific and based on best practices or as

necessary for meeting compliance to particular standards, e.g., ISO 27001. Privacy is a dreading issue, especially in cloud and hybrid IAM implementation. IAM tools use different mechanisms to address privacy issues.

4.1.5. Management

It includes policy automation, service level agreements (SLA), configuration, performance, risk analysis, and forensics. IAM implementations are not perfect solutions, and they keep evolving as technologies evolve and as per business requirements. The IAM system should have policy automation to better manage and control the entities in the organization. IAM tools provide automation pipelines that help centralize and automate IAM policy creation, which helps efficient policy administration. IAM solutions also support automation concerning incident response. IAM systems also provide tools for risk detection and risk analysis based on an inbuilt detection engine. The risk detection engines monitor risk based on heuristics, machine learning, or third-party product integration. Forensics tools in the IAM solution or a third-party forensics tool can be integrated into IAM system. It allows the conduct of investigations and collection of evidence, which is vital to meet legal requirements in any adverse event. IAM providers also allow for the export of audit logs to be exported to other forensics tools [22].

5. Conclusion

This research proposes an IAM framework that will help IAM professionals and security professionals to get a holistic view of various IAM components that need to be considered for implementation and assessment. This research gives a high-level overview to IAM stakeholders. Further research is possible concerning coming up with an implementation level framework based on particular IAM technologies with necessary security controls, which can serve as tool for IAM and information security consultants. We launched IAMaaS as a platform that allows cloud service providers to provide IAM as a cloud service in the public cloud. IAMaaS is compliant with key cloud technologies, such as portability, elasticity, and pay-per-use. The solution was applied as a series of VMs in a cloud environment to conform to the cloud paradigm. This technology can be used in a hybrid mode with current on-premise platform-based applications to improve their security capabilities. Users will create a virtual private region in the cloud with IAMaaS to secure their secured

resources. Integration of this POC with numerous other SECaaS programs will be the focus of future work.

Conflict of Interest: There is no conflict of interest among the authors.

Funding: Self-funded.

Ethical approval: Not applicable.

References

Active Directory Domain Services on AWS. (2018). Amazon Web Services: https://d1.awsstatic.com/whitepapers/adds-on-aws.pdf

Ahmed K.E.U., A.V. (2011). Identity and Access Management in Cloud Computing. *Cloud Computing for Enterprise Architectures. Computer Communications and Networks. Springer*.

Amazon Web Services. (2018). *Active Directory Domain Services on AWS*. Retrieved from https://d1.awsstatic.com/whitepapers/adds-on-aws.pdf

Baldwin, A., Casassa Mont, M., Beres, Y., & Shiu, S. (2010). Assurance for Federated Identity Management. *Journal of Computer Security*, 519–550.

Columbus, L. (2019). *74% Of Data Breaches Start With Privileged Credential Abuse*. Forbes: https://www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged-credential-abuse/#114c3fd73ce4

E. Bertino, K. T. (2011). Identity Management: Concepts, Technologies, and Systems. *Artech House*.

F. Damon and M. Coetzee. (2013). Towards a generic Identity and Access Assurance model by component analysis - A conceptual review. *Proceedings of the First International Conference on Enterprise Systems*. Cape Town.

Fritsch, L. (2020). Identity Management as a target in cyberwar. *Open Identity Summit (OID).* Göttingen: DOI: 10.18420/ois2020_05.

G. Roussos, D. P. (2003). Mobile Identity Management: An Enacted View. I*nternational Journal of Electronic Commerce*, 81-100.

Jorge Werner, C. M. (2017). Cloud identity management: a survey on privacy strategies, Computer Networks. *Computer Networks*, 29-42.

Kaur, H. (2011). *Identity and Access Management—Its Role in Sarbanes-Oxley Compliance*. ISACA: https://www.isaca.org/resources/isaca-journal/past-issues/2011/jonline-identity-and-access-management-its-role-in-sarbanes-oxley-compliance

Laboratory, B. N. (2011). *Separation of Duties for MODERATE level Information Systems*. https://www.bnl.gov/cybersecurity/policies/separation-of-duties.php

Maher Shinouda, S. M. (2016). *Identity and Access Management (IAM) Reference Architecture*. University of Waterloo: https://uwaterloo.ca/watitis/sites/ca.watitis/files/uploads/files/watitis_iam_ref_arch_maher_sean_2016.pdf

Marianne Bradforda, J. B. (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 Information Systems*, 149-165.

Marit Hansena, A. P. (2008). Identity management throughout one's whole life. *Information Security Technical*, pp. report 13 83–94.

Mehraj, M.T. (2017). Directory services for identity and access management in cloud computing. *3rd International Conference on Applied and Theoretical Computing and Communication Technology*, 334-337.

O. Foundation. (2016). *Openid connect*. http://openid.net/

Osmanoglu, E. (2013). *Identity and Access Management: Business Performance Through Connected Intelligence.*

Sharma, A., Sharma, S., & Dave, M. (2015). Identity and access management - a comprehensive study. *International Conference on Green Computing and Internet of Things*, 1481-1485.

Siriwardena, P. (2017). Identity Architect Ground Rules: Ten IAM Design Principles. *WSO2*.

Sullivan, D. (2009). *The definitive guide to security management.* Channel partner real-time publications.

Thinh Nguyen, S. C. (2008). *The United States Patent Application Publication Patent No. US 2008/0028453 A1*.