NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 4, ISSUE 7, July-2017

SYSTEMATIC REVIEW OF IDENTITY ACCESS MANAGEMENT IN INFORMATION SECURITY

Ishaq Azhar Mohammed
Data Scientist & Department of Information Technology, Dubai, UAE
ishaqazhar14@gmail.com

ABSTRACT

This paper is a systematic review of Identity Access Management (IAM) in information security. Identity and Access Administration (IAM) involves tools, procedures, and policies for the management of user identities and user access in an organization [1]. These users may be staff or consumers, but the objective of an IAM system is to establish a unique digital identity that can then be controlled, updated, and monitored throughout the 'access lifetime' of each user. While a person only has one digital identity, numerous accounts may be included in the identity and various access restrictions may be established by each account per resource and context. IAM needs to offer access to the appropriate resources (applications, databases, networks, etc.) in the proper context for each particular identity [1]. It showed that the IAM solution was not effectively implemented, it is an innovative field, and has attracted broader organizational interests. Data security, compliance, owing to the security breach, data loss incidents, has been investigated most. With your own (BOYD) security inside personal mobile technology, you have identified vulnerabilities and risks, vulnerability management, policies, and good practices that contribute to information security failures. It is the technology, people, and processes that should function consistently to create a safe information system.

Keywords: Identity and access management, information technology, information security, identity management systems

INTRODUCTION

Identity and access management (IAM) security is an integral component of the overall IT security system that handles digital identities and user access inside an organization. IAM security comprises policies, procedures, and technology that minimize the risk of identity-related access in a company [2]. The ICT environment has developed a mixed approach for sector-specific access control. Web-based, remote access combined with applications distributed and hosted on the cloud on different networks. Companies are confronted with different administrative difficulties, data protection, increased operational burdens, monitoring problems, and regulatory compliance. For a company to maintain its competitive advantage, it must have effective internal controls in place. This is only feasible in organizations that have simplified their internal business procedures [2]. In the field of information security, identity management is generally seen as a potential for improving the operational process while also lowering costs, improving reporting capabilities, and ensuring regulatory compliance. However, in recent years, it has been shown that this is a notion that is misunderstood, complicated, and expensive [2]. An increase in the number of people engaging in threatening behavior in the online realm, especially those connected with identity theft, has also been seen. When it comes to economic decisions, identity theft has a major impact on people's choices. It also presents a substantial security concern to both businesses and individuals. Solution providers for identity management (IdM) help effectively improve the identity problems that result from the use of numerous different applications. They also support a methodology that encourages growth and security while lowering the costs related to managing clients, their identities, credentials, and attributes, among other things [3]. Identity theft is one of the most serious risks to data security across sectors, accounting for about 90% of all data breaches in the United States. Identity and access management (IAM) is expected to expand in the future in terms of the number of experts, identity access management technologies and software, as well as training and certification programs [3]. Listed below is all you need to know about this increasingly essential element of data security: The problem of having control over how individuals portray themselves on the internet is a technologically difficult one to solve. The maintenance of numerous and distinct copies of internet activities, login credentials, and profile information for each website is a need for web users.

According to a survey of password habits, the average Web user has about 25 login credentials accounts and inputs an average of eight passwords each day on the Internet.

PROBLEM STATEMENT

The main problem that this paper will try to solve is to review how identity and access management is important in information security. In this day and age, cybercrime is on the increase, and data breaches can be very costly as well as damaging to your organization's image [3,4]. Making certain that you closely monitor user access via identity management is an essential stage in the process of developing a secure security plan that is foolproof. Simply put, identity management is the process of ensuring that the appropriate individuals have access to the appropriate resources inside an organization. This entails determining each individual's needed degree of access to business data and only granting them the rights necessary to carry out their duties successfully [4,5]. Also required are procedures for authenticating users, which ensures that the person on the other side of the screen is who they claim to be on their computer screen [5]. When you have a dispersed workforce, it is far more difficult to maintain the visibility of your workers, and cybercriminals are well aware of this. Identity management is a simple, low-cost, and fast method to increase security while causing the least amount of disturbance.

LITERATURE REVIEW

A. Identity and Access Management

The term "IAM" relates to digital identity in a business setting, and it must be regarded as a matter of great importance. Regardless of the many software solutions used by the business, resources must be controlled and allocated with correct access rights (access/politics administration) to the applicable identity/user (— for example, provisioning management). Identity management is the term used to describe this procedure. Identity access management is comprised of three functional areas: data security, provisioning, and compliance (or regulatory compliance) [5,6]. Cloud-based identity and access management solutions have gained popularity as a result of the information without boundaries concept. The traditional IAM access management solution was primarily concerned with data provisioning inside the organization. As technology advances and more data is stored in the cloud and on smart applications, it has become increasingly difficult for businesses to manage user access while complying with data protection regulations. The IDM market is just getting started on its journey toward growing popularity and deep penetration. On the other perspective, cloud security is believed to be fundamentally less secure than that of a private network architecture [6]. Concerns about the cloud being multi-tenanted and not knowing who the final service provider is are valid concerns. The idea of hybrid cloud technology is yet another novel concept, which offers a private cloud for mission-critical information while using a public cloud for less sensitive data. A new group, the open data center Alliance (ODCA), has been established to promote strict cloud computing security since the cloud is not doing enough to safeguard data and privacy. It has been shown that cloud-based IAM poses a security concern since it has been deployed improperly up to date; thus, businesses must rethink the processes that need to be improved rather than just plastering the process with new robust technology [6]. Unrealistic optimism [6] on the part of managers about information security has to be addressed. Simply said, simple cloud identity management (SCIM) offers a specified standard API and user schemas that have been accepted by cloud service providers and their vendors [7].

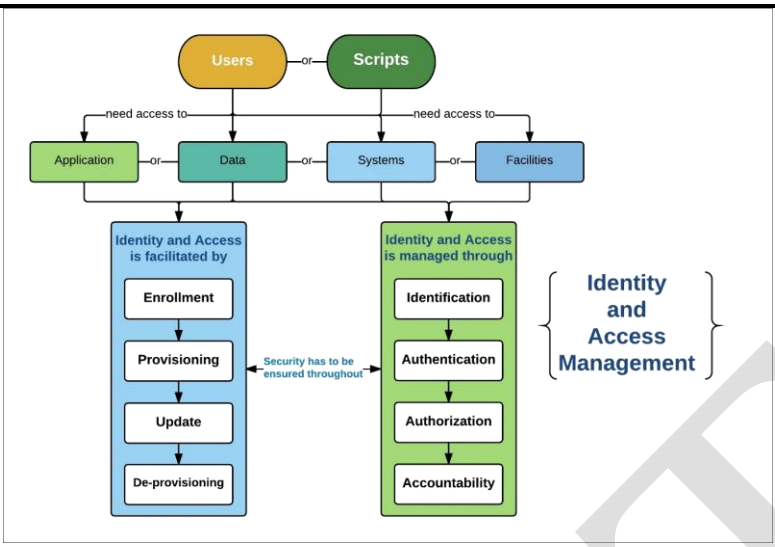

Fig i: An overview of IAM

B. Protection of Personal Information

Data security is divided into subgroups depending on the security field, the data in transit or at rest, the data storage location, the database structure, and the privilege identities that have access to the information [7,8]. Data that is in transit or will be in transit must be secured immediately to protect against a cyberattack. The General Data Protection Regulation (GDPR) guarantees that businesses unify their security policies [8]. Non-compliance fines may be very costly, therefore avoiding them is essential. Organizations can avoid fines by handling and ensuring that individuals consent to having their data or information documented and tracked down, responding to individuals' requests to have their data deleted, and being required to notify people in the course of a personal data breach using an information and data management solution. To distinguish between cloud security and data security, since this is mobile data storage, security controls have been subgrouped with data security [8,9]. While a large amount of data security research exists, the topic of study remains under-recognized as technology evolves and new fields for research emerge, such as mobile data, BOYD storage data, cloud information, as per the 2010 data. Verizon Business reports that 48% of the infringements are committed by insiders, 90% deliberately, and nearly 50% of the infringements include privilege misuse [9].

C. Provisioning

The term "provisioning" relates to the process of providing and controlling access to identities while ensuring their availability, integrity, and confidentiality. Provisioning is classed as a subset of security and includes IAM frameworks, industry standards, and cloud-based IAM. Using an IAM solution, you may minimize operational costs and the risk of a security breach by removing duplicate accounts and implementing a clear division of responsibilities [9]. For this study, IAM solutions have been classified under the Domain of Provisioning, since security components are inextricably linked and difficult to divide into distinct domains. Requirements have been subdivided and organized into domains of provisioning. Most identity and access management (IAM) systems include an automated user provisioning capability as one of their primary features. Provisioning comes into play when a new person enters the organization, when an existing employee transfers to a different department or division, or when an existing employee leaves the business [9]. The JML process (joiner, mover, and leaver) is the name given to this procedure. By connecting an IAM solution directly to human resources and personnel systems, you can link the process of establishing, updating, and removing user accounts with HR activities, thus improving efficiency. A variety of actions that may require changes to Management reporting, such as those connected to employee onboarding and offboarding, may immediately make a substantial difference to permissions for accessing systems and apps that are linked to corresponding employee accounts [10].

D. Compliance

Due to the growing stringency and complexity of regulatory compliance and industry requirements such as SOX, HIPAA, and GDPR over recent times, businesses are subjected to increased audits, compliance reviews, and required reporting. Collection of data, reporting and privilege review are all automated via IAM management solutions, allowing businesses and organizations to restrict access to just those people who need it while remaining more responsible for compliance requirements [10]. Companies may guarantee that data is well managed and that they are implementing proactive measures to fulfill ongoing regulatory compliance by implementing strategic information asset management security measures. Businesses must manage regulatory compliance and robust security procedures across all business and information technology environments on an ongoing basis to be in continuous compliance [10]. For businesses that depend on third-party SaaS applications housed in the cloud, this may be a difficult task to do. If a single application is found to be in breach of compliance rules, a company may be subject to a fine or other punishment. Compliance audits bring flaws to light and provide organizations with the chance to fix vulnerabilities and resolve compliance breaches. To conduct a successful audit, it is necessary to examine every element of security and compliance, including IAM protocols and the subtleties of access control rules, among other things [10, 11]. To guarantee that each area gets the proper amount of attention, the applicable compliance rules serve as guidelines.

Internal audits should be carried out regularly to ensure that compliance is maintained across networks and settings. The reports produced after each audit are used to influence security practices going ahead and to offer evidence if a business is needed to show regulatory compliance with the authorities [11]. Third-party compliance auditors perform external audits of all departments once a year and have the authority to impose penalties for any compliance breaches that are discovered. Considering that the average amount paid in non-compliance fines and penalties is about $1.1 million, it is more cost-effective to perform internal audits and deploy continuous network monitoring rather than waiting for compliance inspectors to discover security holes. Organizations should be continuously monitoring events, documenting activities, managing account provisioning, evaluating authentication processes, and upgrading data access control measures to guarantee the effectiveness of all security policies and safeguard sensitive information [12].

Third-party SaaS and cloud service providers must be included in the monitoring and compliance auditing process. Continuous compliance necessitates the adoption of cybersecurity best practices by all stakeholders, including the development and implementation of disaster recovery and business continuity strategies. Regular vendor evaluations, as well as close monitoring of software settings and vendor behavior, help to remove unknowns and provide valuable information for future software buying choices [12].

The ability to maintain compliance with security laws and regulations is much more than a best practice; it is an absolute need for all companies and organizations that handle private or sensitive data. Companies across sectors can face the challenge of protecting data and ensuring ongoing compliance by using identity and access management system that is appropriate for their needs [13].

E. Traditional Identity Access Management (IAM)

IAM access was formerly considered to be a departmental problem, such as a data security concern; however, with the second phase of IAM, it is now recognized that IAM is a business-wide topic. Business divisions must work collaboratively to ensure that IAM works efficiently. Many retailers have attempted to offer off-the-shelf goods in the past, but their efforts have been unsuccessful [13, 14]. As a result, rather than addressing the root cause of the problem, the system has been patched up. As a result of company growth and the requirement to offer platform open access to both internal and external clients, it has now become clear that an identity approach is essential for surviving in a competitive market while also providing a robust security solution [14]. The implementation of the IAM (auto-provisioning tool) had been unsuccessful. The registration and termination of new user profiles in Active Directory were the only processes that were automated. Users were manually provisioned into other banking programs, such as Quicken. This technology not only introduced additional steps to administrators' workloads but also left administrators with the task of completing account creation that had been left unfinished. Once the automated program had been run, administrators needed to wait for

the account creation procedure to be completed, which might take several minutes. When account access was required immediately, this proved to be very challenging [14].

F. Cloud-Based Identity Access Management (IAM)

This is the second wave of identity access management, which includes increased levels of application accessibility to external users, more usage of cloud-based services, and increased use of social networking platforms that need access to applications. An increasing number of IT infrastructures are either SaaS or cloud-based in operation. Because the perimeter is decreasing, an IAM solution must include social, mobile, and cloud technologies into its design and implementation. In addition to networking, an IAM system provides identity-based control over data [14,15]. Either in the cloud or on a mobile device, data must be protected. For information to be encrypted, it must first be identified and then granted access to it by those who have the necessary permissions. In the case of SaaS and the cloud, there is a disadvantage in that companies are often reduced to a security model that is "one size fits all." Currently, according to Richard Walters, CTO of SaaS ID, the absence of granular control and auditing is hindering CIOs in regulated sectors from benefitting from the productivity and scalability of SaaS [15]. Walters thinks that, at the moment, the cloud offers a blind spot for CIOs. However, they are unable to observe what workers have done in the time between their login and their logoff. Furthermore, they do not have the means to audit interactions with web-based applications." Administrative, monitoring and assurance of access to information inside the Bank's internal premises as well as applications hosted on the cloud are the responsibilities of the Information Security Management Department. If you need information, you must have it accessible when you need it, and it must be both accurate and private. If you fail to provide information on time or with integrity, you may be liable for compensation, loss of business, exposure of corporate secrets, and other legal problems [15]. Having stronger security systems requires management and enforcement [15,] and for a secure system to be implemented, both people and technology must work together in unison [6]. A regulated change control process is required, with all stakeholders cooperating to achieve the desired result. [16].

G. The Importance of Roles Of Identity In Information Security

The purpose of identity is to register people inside a system, so everyone who has entry to it is verified correctly, which is one of the 3 major foundations of security. It is critical for improved access control that the responsibilities of identities be well defined and that the person who wishes to get access to them can be easily identified and verified. The ability to regulate what a certain user needs in terms of what he or she may access is essential for maintaining information security. The ideal situation is to appeal to the principle of "minimal privileges," in which a person receives authorization and only sees on his or her screen what has been granted to him or her via the administration of permission groups [16].

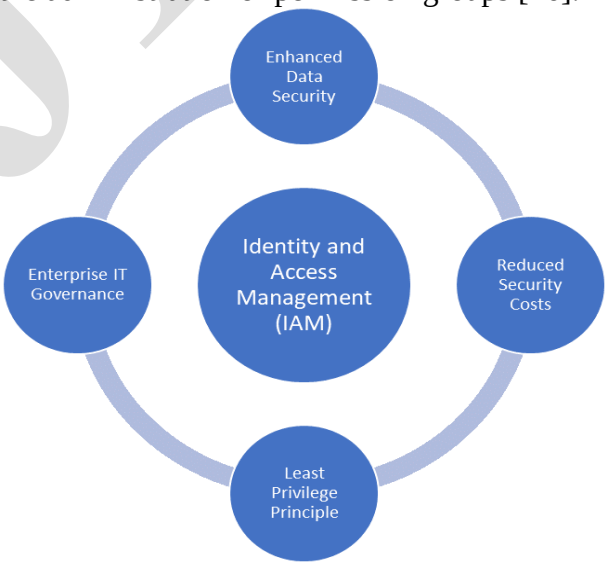

Fig i: Important roles of IAM in Information security

IAM FUTURE

With the increasing IT difficulties that many businesses face, the future of IAM in information security will advance. As a result of the diverse geographical, social, and economic factors that exist in the United States, identification systems are an essential part of integrated development strategies. Comprehensive models with widespread coverage can provide many advantages for public and private entities, especially when they are digital. These include making it easier for people to gain access to services and privileges and to receive services, as well as enhancing the efficiency of public management, strategizing, and service provision [17]. Moreover, early data indicates that identification systems could provide a range of economic advantages to the public service, including less fraud and leakage in transfers, increased administrative productivity, improved collection of taxes, and new income streams [17]. The adoption at the national level of strong and comprehensive identification systems thus gives businesses the opportunity for substantial financial benefits. Nevertheless, much like with the public sector, determining the direct economic impact of identification systems on private companies may be difficult to determine. It is expected that the breadth and size of access control in the US will continue to expand. The growing use of technologies such as big data, cloud solutions, and the Internet of Things will continue to alter the future of information and communications technology (ICT) [18]. As the importance of digital identities grows, so does their protection. To remain competitive, businesses must adapt to changing demands. This involves adopting identity management systems that are compatible with their present business requirements while also allowing them to adapt to future developments.

ECONOMIC BENEFITS

As security problems continue to grow in complexity, greater technological needs would be beneficial to the United States information technology sector. Manufacturing industries will bolster the US economy by shipping a variety of information security products. The continued growth of the Internet economy in the United States is dependent on the proper development of online identification information. Identity management is critical in a variety of settings, such as the enterprises, and governance, to support corporate operations and services and to allow consumer-facing online experiences and transactions [18]. IdMS is a critical area of study in the areas of identification and identity management. Robust, widely utilized identification systems may also help private businesses across sectors improve their revenue levels and revenue-generating possibilities, including via the following: – Expanded identifiable customer base. The absence of identity papers creates a physical barrier to accessing public and private services that need identification. Thus, expanding the reach of strong identification systems has the potential to expand the client base of businesses across a range of sectors. By lowering the transaction costs associated with confirming or validating one's identity, digital, interoperable, and queryable identification systems may contribute to a reduction in customer desertion [19]. Moreover, if these technologies enable businesses to measure risk more correctly, they not only help avoid fraud but also reduce the number of false positives (low-risk clients have erroneously given high-risk scores) and transactions that have been denied for incorrect checks. For instance, businesses in the U.S. online retail sector lost $118 billion in sales each month owing, compared with $9 billion in reported fraud, to unjustified transaction denials.

As the importance of digital identity grows in the online world, IdMS is a major element for the effective development and growth of secured, trustworthy, and user-friendly IdMS, which is critical for building confidence in terms of e. As a result, the development of IdMS has resulted in significant changes to e-transactions; therefore, researchers recommend that further study into IdMS research must involve the interactions of users and systems. Digital identification systems play an equally significant role in the business sector. Many businesses—including those that would provide financial and banking services, phone companies, online sales channels, and aviation services, among others—must validate and verify their users' identifications at different points throughout the service lifecycle to conduct business with them and provide services. Customer identity is often validated via government-issued or approved credentials, such as with a national identification card, passports, or other documentation. Where credible evidence of identity is rare, businesses are likely to have smaller accessible client pools, increased administrative costs, and increased fraud risks [19].

CONCLUSION

The main objective of this study was to evaluate how identity and access management applies to information security. A business may achieve a healthy balance between security, risk reduction, educating its workers (both customers and employees), and using the services they need whenever they require them by establishing a dependable IAM program, according to the results of this study. An access management system may be very beneficial to applications, and it is strongly suggested that it gets the attention it deserves in light of the benefits and failure avoidance it can offer. Data breaches, as well as financial and reputational harm to your business, maybe avoided by following these steps. In today's environment, one of the most important elements of cybersecurity for companies is determining their organizational maturity concerning the principles of IAM. It will offer an assessment of your organization's present status in terms of the security of its digital assets and infrastructure, as well as recommendations for improvement.

REFERENCES

1) P. De Hert, "Identity management of e-ID, privacy and security in Europe. A human rights view", Information Security Technical Report, vol. 13, no. 2, pp. 71-75, 2008.
2) Tracey, “Security at the data level,” Network Security, issue 5, pp. 6-12, May 2013.
3) S. Mansfield-Devine, “Security review: The past year,” Computer Fraud & Security, 2013.
4) M. Potts, “The state of information security,” Network Security, vol. 2012, issue 7, pp. 9-11.
5) Y. Demchenko, "Virtual organisations in computer grids and identity management", Information Security Technical Report, vol. 9, no. 1, pp. 59-76, 2004.
6) Everett, "Identity and Access Management: the second wave", Computer Fraud & Security, vol. 2011, no. 5, pp. 11-13, 2011.
7) C. Gunter, D. Liebovitz and B. Malin, "Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems", IEEE Security & Privacy Magazine, vol. 9, no. 5, pp. 48-55, 2011.
8) M. Hummer, M. Kunz, M. Netter, L. Fuchs and G. Pernul, "Adaptive identity and access management—contextual data-based policies", EURASIP Journal on Information Security, vol. 2016, no. 1, 2016.
9) Shlomi, “Privileged identity management: Securing the enterprise Network,” Security, vol. 2010, issue 12, pp. 4-6, December 2010.
10) H. Jason, “Why the traditional approach to information security is no longer working,” Network Security, issue 1, pp. 12-14, 2013.
11) K. S. Madhan and R. Paul, “A roadmap for the comparison of identity management solutions based on state-of-the-art IDM Taxonomies,” Education & Research, Mysore, India: Infosys Technologies, 2010.
12) H. Liu and M. Liang, "Efficient identity-based hierarchical access authentication protocol for mobile network", Security and Communication Networks, vol. 6, no. 12, pp. 1509-1521, 2012.
13) Lomas, "Information governance: information security and access within a UK context", Records Management Journal, vol. 20, no. 2, pp. 182-198, 2010.
14) L. Martin, "Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management", Information Systems Security, vol. 16, no. 1, pp. 9-14, 2007.
15) R. Oppliger, "Microsoft .NET Passport and identity management", Information Security Technical Report, vol. 9, no. 1, pp. 26-34, 2004.
16) K. Rannenberg, "Identity management in mobile cellular networks and related applications", Information Security Technical Report, vol. 9, no. 1, pp. 77-85, 2004.
17) M. Small, "Business and technical motivation for identity management", Information Security Technical Report, vol. 9, no. 1, pp. 6-21, 2004.
18) J. Smith, "Getting the Right Balance: Information Security and Information Access", Legal Information Management, vol. 10, no. 1, pp. 51-54, 2010.
19) M. Uddin and D. Preston, "Systematic Review of Identity Access Management in Information Security", Journal of Advances in Computer Networks, vol. 3, no. 2, pp. 150-156, 2015.