European Journal of Engineering and Technology Research
Vol 8 | Issue 4 | August 2023
ISSN 2736-576X

RESEARCH ARTICLE

IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations

Chetanpal Singh[1,*], Jatinder Warraich[2], and Rahul Thakkar[1]

ABSTRACT

Identity and Access Management proposes a web service that assists in controlling the entire work through secured ways. This research study has been started to highlight the importance of IAM by discussing its roles, characteristics, advantages and disadvantages. It is a framework comprising processes, policies, and the latest technologies, allowing the organization to monitor digital identities and control exclusive access to follow information based on user data. The IAM component proposes an approach of centralized user management, account management console, authentication approaches, and so on. In this research work, roles and key components of IAM have been discussed with all types of possible challenges. Furthermore, this research will help readers and future researchers easily identify the importance of IAM in maintaining security systems within organizations.

Keywords: Access control, IAM (Identity Access Management), reliability viable solutions, security maintenance.

Submitted: June 14, 2023
Published: August 31, 2023

10.24018/ejeng.2023.8.4.3074

[1] *Faculty of Business, Design and IT, Holmesglen Institute Chadstone Campus, Australia.*
[2] *Faculty of ICT, Victorian Institute of Technology (VIT), Australia.*

****Corresponding Author:***
e-mail: Chetanpal.singh@holmesglen.edu.au

1. Introduction

1.1. Research Background

User identity management is a common component that provides security and easy auditable access to some limited assets. The term "*Identity Access Management"* ensures the job identities and nature of the right people c easily accessed through relevant tools. The framework includes different processes, policies, and technologies to monitor user access and manage digital identities. Identity management is needed to improve data security, control user data access, and maintain distance from illegal access. It helps any organization to identify illegal access, mitigate data breaches, and propose sensitive information about the corporate world. The components of IAM can be classified into the following four important categories: '*authorization*', '*authentication*', '*central user repository*', and '*user management*' [1].

This research paper has been conducted to highlight IAM's significance, advantages, and disadvantages. It has been noticed that "*Google*", "*Facebook*", "*GitHub*", and other well-known web-based organizations provide free confirmation opportunities that can be easily coordinated through online applications. **'*KeyCloak*'** is an open-source IAM that focuses on current administrations and applications designed to provide a keyguard for application protections and administrations [1]. **'*Azure ATP (Advanced Threat Protection)*'** is a completely cloud-based solution that helps investigate and detect any type of security incidents across the entire network system. It assists in securing any organization from compromised identities and insider threats. It has the ability to identify the threat patterns along with its resources within the cloud and on-premises.

Nowadays, as passwords are one of the important predominant mechanisms used for authentication processes, it becomes impossible to remember those passwords if the users have more than one account. It frequently forces the users to choose weaker passwords which damages the user's own revealing passwords. It has been noticed that it becomes easy for attackers to grant access to those accounts and hack users' credentials. **'*SailPoint*'** cloud platform for maintaining identity security helps users to realize the accesses and identities of all the secure information [2]. This identity management solution helps organizations easily manage digital identities, employee permissions, data access, information security, and compliance. Similarly, it has also been noticed that **'*CyberArk*'** proposes the most extensible and complete platform of identity security that helps to protect critical assets and identities in the vicinity of zero trust. It is a complete 'security-focused IAM'. On the other hand, **'*Okta*'** is such an IAM platform that can be used easily and neutrally with all relevant existing solutions, which selects the best technologies. Identity authentication, as well as access control of different participating nodes, propose cross-chain transactions to practice different accesses [3].

In this research work, IAM proposes opportunities to access all types of cloud-resourced project-level access easily. It allows maintaining IAM standards to access the data that need to complete the job. Achieving identity authentication and access control in support of transaction circulation uses various types of changes which maintain low chain intrusion [2]. Moreover, with the assistance of the IAM scheme, it becomes easy to realize conversion based on cross-chain identity in the middle of recorded illegal transactions and different chains. IAM risks are always inherent in the cloud environment, where different types of potential risks are easily resolved through the help of cloud service providers. Therefore, it is also necessary to manage all the IAM risks, which are the outcomes of any cyber criminals, negligence in vendor management, industrial espionage, or maltreatment by any privileged users [5].

This research paper is organized into different chapters; chapter 1, within the introduction section, explains the background of the research work based on the proposed topic. In chapter 2, it has critically discussed the points of view of different authors' perspectives on IAM. It has explained the in-depth information, which helps the readers of this paper to acquire all the relevant information based on research objectives and questions. Chapter 3 has explained the research methodology, which is followed by the researcher while conducting the research. Chapter 4 is designed to explain the outcomes of this research work and comparisons between all the article papers. Chapter 6 provides the conclusion of this entire research work [6].

1.2. *Problem Statement*

This research work has been conducted depending on the significance of IAM. It is mainly an important cybersecurity activity that helps to organize different access management. With its assistance of it, it automatically boosts the entire monitoring processes and security controls. This research work will help to understand the importance of identity management systems that are actively used to propose safeguarding security-based incidents. As in the recent era, cybercrime incidents are increasing day by day, and it will be necessary to realize the importance of identity management systems [7]. Moreover, it can be said that the current research is needed to solve the possible issues behind the identity management system.

1.3. *Research Aim & Objectives*

1.3.1. *Aim*

This research work will be carried on with the aim of completing the research work by focusing on the importance of "*Identity Access Management*" (IAM) along with all its pros and cons.

1.3.2. *Objectives*

- To highlight the role of "*Identity Access Management*" (IAM).
- To identify the key components and process of IAM that deeply impact on acquiring so many experiences on organizational productivities.
- To point out the possible challenges of IAM that can interfere with its credibility.
- To find out and analyze the solutions to mitigate all possible challenges of IAM.

1.3.3. *Research questions*

1. What is the role of the IAM identity and access management?
2. How do the key components and process of IAM develop a considerable impact on the experience of the user along with organizational productivity?
3. What are the challenges of IAM that can interfere with its credibility in terms of implementation in large firms?
4. Critically analyze the solutions present to mitigate the challenges of IAM and strategies required to adhere to when choosing the IAM system for the firm.

1.4. *Research Significance*

The significance of this research is to outline a framework that has been designed to assign digital identities. It consists of different types of processes and policies, along with the latest technologies. This section highlights the important roles of IAM, its key components, and possible challenges which adhere to its values of it. Security maintenance is always a pivotal part of any type of application [8]. Behalf of increasing awareness about identity management, it is required to carry on the entire research study to highlight the importance of identity access management to the readers of this paper and future researchers.

2. Literature Review

2.1. *Role of the IAM Identity and Access Management*

As in the latest technological era, the revolution of computerized devices is increasingly attractive constantly; due to that reason, most attacks also try to take various types of tactics to access users' devices [10], stated that, for handling the latest cyber-attacks, traditional security controls process cannot provide better outcomes, and with this, failed to handle threats also.

The Fig. 1 provided information about the IAM configuration phase, as well as the IAM operation phase. **"*Identity Access Management*"** (IAM) can support handling permissions, which manage how AWS resources can access users. IAM is also known as **"*role-based access controls*"** (RBAC), through which cloud customers can easily assign individual function, which is related to a set of permission to access other functions, data stores, as well as open Internet. Roles of strict IAM can be constructed for those functions which are limited to communicating with those important requirements to handle their activities.

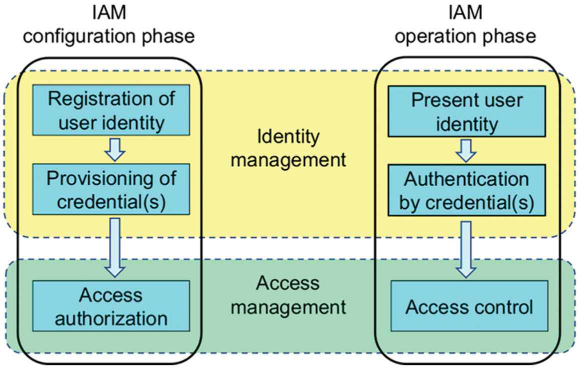

Fig. 1. IAM phases. Source: [10].

In this research paper, the author proposed **"WILLIAM"** as a workflow-aware access management model, as well as a reference monitor, which satisfies the functional requirements of the "serverless computing paradigm" [11]. ***William*** has the capability to encode a serverless application's protection state as a permission graph, which defines permissible transitions. It has the capability to avert unauthorized requests' processing costs, as well as minimize applications' attack surface also. By adopting IAM, business organizations can ensure high-quality security systems production processes and, with this, improve regulatory compliance also. IAM has the capability to increase the flexibility of traditional usernames, as well as password solutions [12].

Based on the previous author's statement [13] stated that, in information security systems, IAM plays a significant role. To handle the latest IT environment, and with this handle database platform, it is important for the users to identify network access properly. Through this research paper, the author tried to provide how IAM can connect with innovative Artificial Intelligence (AI) technologies to ensure high standard identity management, as well as user authentication [14].

Through the above Fig. 2, the author defined the AI approach to IAM. As in the current age, due to innumerable effectiveness, the popularity of AI and ML is constantly increasing; due to that reason, there is no doubt it can develop the efficiency of IAM. Modern technologies have the capability to speed up the latest IAM compliance. AI has the capability to detect abnormalities, as well as possible threats. It equips customers with the proper information required to take proper decisions, both technical, as well as non-technical [15]. Due to technological advantages, hackers are becoming proficient as well as daring constantly, and due to that reason, for infiltrating user's networks, often it can be difficult for organizational managers to handle issues properly. Through this research paper, the author clearly defines the beautiful relationship between AI and IAM. Through the research findings, it has been noted that the implementation of AI is a totally new approach, and there are no proper organizations that take any approach to implement AI in IAM. Those two are the most innovative combination for developing a suitable monitoring system through which IAM can visualize connectivity and decrease cyber breach risks. With the combination of innovative technologies, IAM can ensure that the right people can access the organizational network and, with this, manage employee applications also.

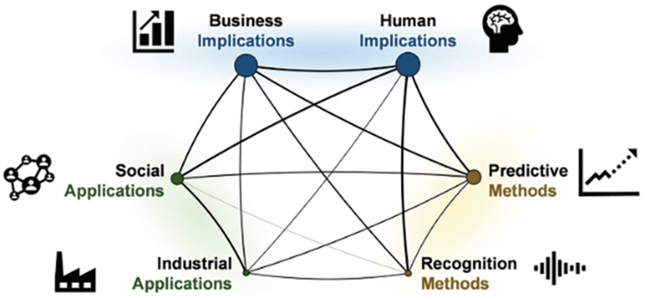

Fig. 2. IAM model for artificial intelligence. Source: [14].

2.2. *Key Components of the Process of IAM*

IAM professionals should have a proper vision for the IAM circumstances which satisfy the requirements of the corporate. Every IAM project should develop towards the required target state. The components of IAM can be categorized into four different categories, concluding authentication, user management, central user, and with this authorization. In the present age, most business organizations increase their focus on the adaptation of cloud infrastructure platforms in equal capability.

In hybrid IT architecture, IAM is a crucial component. Hybrid IAM has the capability to develop a basic credential, which can be allowed for access in cloud environments [16], defines components of hybrid IAM architecture, concluding ***on-premise corporate directory***, ***on-premise federation service***, ***Identity Sync services***, and with this ***cloud IAM service***. Directory services, which allow authentication to access organizational resources, conclude Active Directory. Directory objects highlight the user account as well as the service account. For that, identity service implements basic access management abilities concluding authentication, as well as authorization for the organizational applications. Fig. 3 shows how it supports identity standards, such as SAML as well as OpenID Connect, to allow access to both internal, as well as external resources. ***Identity Sync Service*** is basically implemented in cloud direction-based organizations to reduce risk, as well as complexity. In the public cloud, platform service implements fundamental IAM abilities, concluding authentication, federation, as well as access management, and with this can be exploited access assumption sources as well [17], [18].

Based on the previous author's opinion, the other author [19] defines IAM systems as required to be realized properly, that can be utilized for on-premises services, as well as cloud services correctly, as well as securely. IAM has the capability to provide massive security features for providing user access within the organization. "Security Assertion Markup Language", commonly known as SAML, is utilized in this research paper. It is basically a standard protocol structured by the "Security Services Technical Committee" [19]. An IAM SAML allows identity providers to ensure user authentication through interchanging user information, concluding login data, authentication state, identifiers, as well as different relevant

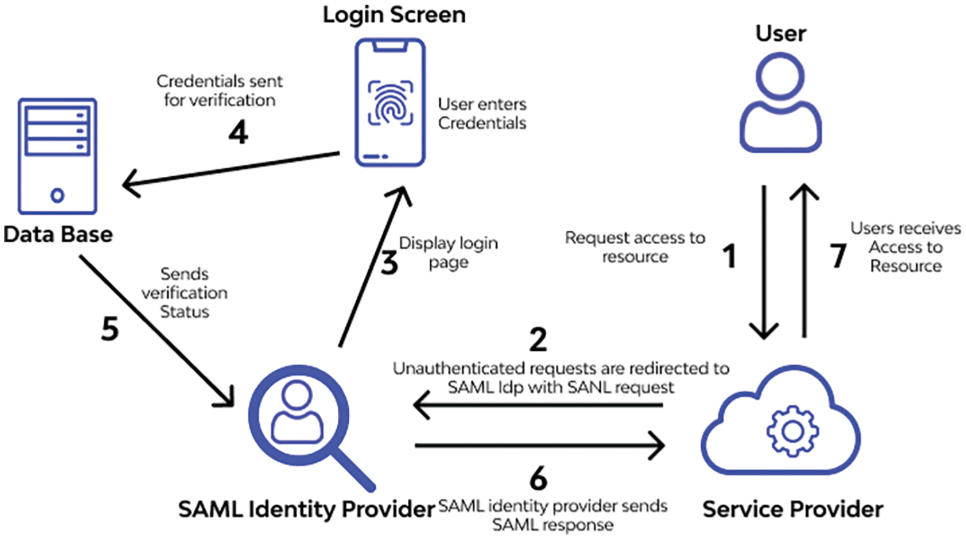
Login Screen
User
Credentials sent for verification
4
User enters Credentials
Data Base
Display login page
3
Request access to resource
1
7
Users receives Access to Resource
Sends verification Status
5
2
Unauthenticated requests are redirected to SAML Idp with SANL request
6
SAML Identity Provider
SAML identity provider sends SAML response
Service Provider

Fig. 3. SAML authentication process. Source: [15].

attributes between the service provider and, with this, the identity.

2.3. Analysis of IAM Challenges Developed During the Implementation Process

A firm or organization can easily face different challenges at the time outlining, implementing, as well as controlling IAM solutions. It has been noticed that the latest cloud-dependent IAM solutions propose simplified and uniform identity management practices, which easily become popular as the day advances, for optimizing the existing solutions of identity and access management. As per the opinions of the authors [20], the way of the latest businesses is completely revolutionized through storing, processing, as well as managing the relevant data. For all sizes of businesses, cloud security nowadays has become a great concern. The user's identity is verified through identification processes that easily access any cloud resources as well as control the user's actions to perform better. Implementation of effective authentication along with access controls is important for keeping away from any illegal access to all the cloud resources [20].

Fig. 4 shows there are so many challenges that are associated with the implementation of the IAM system, and those are '*lack of sufficient planning*', '*lack of management support*', '*poor user role management*', '*misapplication of the roles and responsibilities of access management*', '*lack of attention in the near future*', '*lack of relevant points of views*', and '*poor privileged access management (PAM)*'. The proposed system provides a dynamic field that always remains progressive for helping combat cybercrime for continuing the development of the latest methods. IAM should be implemented in the company of effective authentication mechanisms like MFA and RBAC to ensure the right of only authorized users to access cloud-based resources. Besides this, it has been required to regularly review the user's data [21].

Implementation of IAM represents its own challenges, together with many SMBs (small and medium-sized businesses) [21]. Whatever the size of an organization, it has come to know that board members, as well as business leaders, propose success on behalf of following the IAM initiative. Nowadays, almost all activities have slowly adopted the latest technologies, which creates an international shortage among all tech professionals. Finding trustworthy employees with sufficient knowledge creates difficulties in a global shortage system. All the important data should be encrypted in both situations that are in transit forms and even in rest positions. Both SSL (Secure Socket Layer) and TLS (Transport Layer Security) are utilized for data encryption [22].

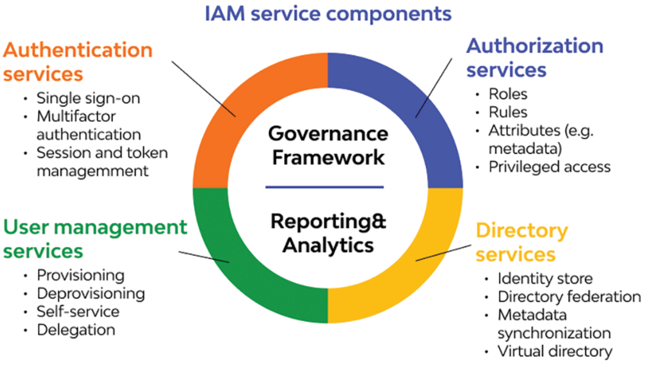

Fig. 4. IAM components. Source: [18].

It has also been noticed that the lack of proper planning guides to the mismanagement of different resources which are required to manage and implement IAM. It has been noticed that IAM needs an extensive roadmap that needs to be extended over the past few years, and this roadmap is completely supported by all the relevant stakeholders. The path of implementation of IAM should be designed by prioritizing the possible risks. As it is completely based on the latest technologies, it has been noticed that risks or challenges will change as time goes on, but at the same time, unexpected changes will arise. IAM implementation is difficult and completely resource-based. Despite all of this, it can be said that the implementation of IAM is a relevant opportunity to focus on access controls and proposed risk assessments in regard to IAM activities [23].

2.4. *Mitigation Strategies of IAM challenges*

Based on the previous author's opinion about the IAM's implementation challenges, it has been noted that there are different basic issues that should be mitigated properly. Among various issues, the most common risk is authentication issues [24] defines that, for ensuring authentication, it is important to implement authenticate method. Authentication factors can be categorized into three different groups, such as "personal identification numbers", biometrics, or authentication key. Additionally, the multi-layer security system is also an essential process that can support ensuring authentication. Through multiple authentication mechanisms within the IAM process, it can be easy to mitigate challenges as well as increase efficiency levels also.

2.5. *Research Gap*

This research is conducted by focusing on the importance of Identity Access Management. Besides this, its key components, roles etc., have been discussed here, but no detailed information about its risk mitigation strategies has been mentioned here. As this identity and access management system help to provide organizational security, it is necessary to follow uniqueness at the time of implementing IAM. There are robust solutions that help to mitigate all the possible threats, but in this research study, those are not discussed in-depth, and it creates gaps in this research work.

3. Research Methodology

3.1. *Research Overview*

The researcher put stress on evaluating the "role of "Identity Access Management" (IAM)", and in the process, the concern has been laid on assessing the set research question and aim. Even the researcher put concerned with evaluating the considered scholarly articles through the lens of positivist research philosophy. The considered research work will be formed by considering the secondary research method as it will support considering the qualitative research method generated from the literary analysis while emphasizing the content. The consideration of the deductive research approach supports the existing theories. Further, the researcher has managed the ethical issues for managing the research result [20].

3.2. *Research Methods*

Identity and access management security are regarded as the prime element of the entire IIT security system that manages digital identities along with user access in the firm. In order to evaluate the role of IAM, the concern has been laid on making effective utilization of the **"secondary research method"**. Further, the qualitative data reflected the research's significance in terms of justifying the objectors of the research [23]. The researcher to recognized key components and processes of IAM and acquired the key facts through a secondary data collection method. The consideration of the secondary data supported the acquisition of literary sources and supported the accumulation of sufficient data that can help in meeting the set research aim and objectives. Further, the consideration of the secondary research method supported to conduct of the research works fast and in a cost-effective way by using the data of past researchers who have used vital data for reflecting IAM implementation.

3.3. *Research Philosophy*

The considered research work has made effective utilization of the ***"Interpretivism research philosophy"***, which supported the researcher to put more stress on factual data. This philosophy helped the researcher to form the belief by which the required data will be accumulated, evaluated and utilized [25]. In the process, this research philosophy enabled the researcher to conduct the research work in a subjective way while stating that data evaluates the rationalization of the research in an effective way and the main meaning is acquired at the end of the research method. When conducting the secondary research method for evaluating challenges of IAM that can interfere with its credibility in terms of implementation in large firms, the interpretivism research philosophy enabled to conduct of the research in depth while providing higher range validity as it involved authentic data.

3.4. *Research Approach*

The research formed on evaluating the role of "IAM identity and access management" make effective use of the ***"Deductive research approach"***. This particular deductive research approach enabled us to put stress on utilizing the existing theories. This supported critically emphasizing the key contents of the present information white acquired the reliable evaluation from it to justify the cumulated content [22]. Apart from this, the researcher put stress on reflecting the key facts as well as ideas reflected in the literary contents to give an effective evaluation and stating the relevancy of the objectives set. Further, the researcher reflects on the efficiency of the objectives set by considering the qualitative research method and making a considerable contribution to future research development. This deductive research approach supported more logical inferences involved in the literary data that highlight the relevance of the research.

3.5. *Research Design*

The considered research work has made effective utilization of the ***"Descriptive research design"*** to systematically accumulate the data for evaluating the IAM identity and access management role in the organization in a critical way. This research design does not enable the researcher to manipulate the data but evaluates it in its actual version to extract the desired outcome [21]. This enabled the researcher to evaluate the key components of the IAM in an effective way and the way it reduces the threat of identity-related access in the firm. The consideration of the descriptive research design enabled to form of the strategy by which varied components of the paper have been integrated and assuring that the research problem can be addressed effectively.

3.6. *Research Data Collection*

The ***"Secondary data collection method"*** has been used in this research paper, and this supported to make effective utilization of the existing data acquired from the scholarly articles. Even in the process of collecting the data, the concern has been laid on making utilization of the "government and non-government records", "magazines", "newspapers, libraries", and "internet" [23]. Even the record of different organizations using "systematic review of identity Access Management (IAM)" can be considered to evaluate the critical use of the IAM and the issues that it laid in the process of implementation in the large organization. The accumulated literary sources reflected the new aspect of the considered research topic. In the process of data collection, the stress has been laid on making utilization of the literary sources.

3.7. *Research Data Analysis*

In the research work, the concern has been laid on making utilization of the "qualitative data analysis" method. This supported to make use of only descriptive data, and no statistical data have been utilized in the process of undertaking the overall research work. This enabled systematizing the descriptive data collection via scholarly articles and then evaluating it. It helped to stress accumulating effective data and then facilitating the key elements for implementing the IAM [24]. In the process, the acquired data has been interpreted in an effective way to ensure that the data analysis process can be executed in an authentic way. This supported undertaking a critical analysis of the accumulated paper from the scholarly articles to reflect the overall scenario associated with the considered research topic.

3.8. *Data Validity and Reliability*

The researcher has evaluated the necessity of IAM and the way it involved the policies, methods and techniques that support reducing identity-associated access in the firm. In order to achieve this, the research has put concern on considering the reliability to form consistency and the aspect of the research result that supported reflect the relevancy of the research effectively [26]. Further, the researcher has reflected on managing consistent outcomes though out the research and the work or evening the rationale of counting secondary research methods.

The validity of the research work has been considered to reflect the accuracy development in the result of the research and recognize the genuineness of the research output gathered via literary sources. Even in the process, the concern has been laid on making use of literary sources published in the last three years to ensure that only current data can be used to meet the set aim and objectives.

4. Result & Comparison

The six distinct papers are related to one another in a variety of ways. All of the papers arrive at the same conclusion, which is that workflow integration, blockchain technology, distributed ledger technology (DLT), enhanced authentication methods, and artificial intelligence (AI) all have the potential to enhance identity and access management (IAM). Every single study acknowledges that concerns regarding safety and confidentiality are the main barriers to the implementation of these technologies in IAM [24]. However, there are a few significant differences that may be found between the six publications as show in Table I.

4.1. *Result of the Papers*

The six papers offer a range of viewpoints on the possibility of enhancing IAM through the use of AI, sophisticated authentication techniques, blockchain technology, distributed ledger technology, and workflow integration. These are some of the subjects that the papers cover.

- A variety of chances for IAM improvement are presented by the application of AI, some of which are highlighted below:
  - ○ This method can be used to automate a number of processes, such as password management and user provisioning.
  - ○ Supplying information on user behavior that can be used to spot potential dangers in the immediate area.
  - ○ Spotting unusual user activity patterns and using that information to help prevent assaults.
- One way to improve IAM's current security is to use more complex authentication processes. These steps increase the difficulty of unauthorized users accessing systems and data, which ultimately enhances the security of IAM.
- By providing a tamper-proof and decentralized method of storing identifying information, blockchain technology can help identity and access management (IAM) increase its security and privacy. Identity and access management (IAM) can become more secure as a result of this.
- Identity and access management (IAM) could become more effective with the use of distributed ledger technologies. This is achieved by offering a shared, unchangeable ledger of access control-related data.
- The process of providing and rescinding access to systems and data can be automated with the use of workflow integration, which can increase IAM's effectiveness. As a result, IAM could be more efficient.

4.2. *Comparison of Results*

The six papers give a thorough explanation of how blockchain technology, distributed ledger technology, workflow integration, more robust authentication methods, and artificial intelligence may improve IAM. But each of the six papers focuses on a different subject. Paper 1 examines the perspectives of IT professionals, whereas Paper 2 examines the technical challenges of enhanced authentication systems. In contrast, Paper 3

TABLE I: Comparison of Different Literature in AIM

Sl. No.	Title of the paper	Citation	Critical Discussion	Result
1	"The Interaction Between Artificial Intelligence and Identity and Access Management: An Empirical Study"	[4]	The author of this paper looks into the relationships between identity access management (IAM) and artificial intelligence (AI). To gather their opnions on AI and IAM in light of the study's findings, the authors polled 100 individuals who work in the information technology sector. The poll's findings indicate that the majority of IT professionals are upbeat about the prospect of AI assisting IAM. But they also expressed their worry about how AI may harm people's safety and privacy in the future.	In the first paper in this series, the researcher examines the perspectives held by IT specialists. The researchers who were in charge of drafting Paper 1 noticed that IT staff members generally had a positive outlook on the application of AI to enhance IAM. But in addition to that, they also emphasized worries about the effects AI will have on people's safety and privacy.
2	"Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing"	[9]	The author of this paper examines the usage of sophisticated authentication techniques to meet identity and access management (IAM) needs in cloud computing. According to the authors, utilizing novel authentication techniques can enhance IAM security in cloud computing. They assert that further research on this subject will be needed in the future. The authors also stress the importance of conducting additional research that is more in-depth within this sector. They do, however, concede that the implementation of more complex verification methods might be challenging and costly.	In the second paper, the researcher examines the technical details of various advanced authentication techniques in greater detail. The authors of Paper 2 propose that cloud computing can be used to create a greater level of security for IAM and that this level of security can be contributed by improved authentication mechanisms. However, they do mention that installing more sophisticated authentication techniques might be difficult and expensive.
3	"Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi-Application Outsourced in Cloud"	[23]	A decentralized and dynamic single sign-on (SSO) identity access management solution for many cloud-hosted applications has been shown in this study. This work's goal is to achieve that. The system includes the use of blockchain technology to achieve decentralization and dynamic behaviour, respectively. The strategy, according to the authors, has the potential to increase both the security and effectiveness of IAM in cloud computing, and they advise using it.	An overview of a centralized, static single sign-on and identity access management system is provided in Paper 3, and it may be applied to a number of cloud-based applications. The system includes the use of blockchain technology to achieve decentralization and dynamic behaviour, respectively. The strategy, according to the authors, has the potential to increase both the security and effectiveness of IAM in cloud computing, and they advise using it.
4	"Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review"	[24]	This article offers a thorough analysis of blockchain-based identity management systems, or BIMs, for usage in contexts relating to the Internet of Things in the healthcare industry. Twenty different BIMs that are either now in use or being developed were uncovered by the authors. The authors contend that BIMs should be taken into consideration since they have the potential to enhance the security and privacy of IoT-related health data. They further assert that this potential might be leveraged to raise the standard of BIMs.	In Paper 4, which is available here, the BIMs used in health-related IoT are examined in-depth. Twenty different BIMs that are either now in use or being developed were uncovered by the authors. The authors contend that BIMs should be taken into consideration since they have the potential to enhance the security and privacy of IoT-related health data. They further assert that this potential might be leveraged to raise the standard of BIMs.
5	"Identity and Access Management using distributed ledger technology: A Survey."	[25]	In the preceding part, the researcher discussed distributed ledger technology (DLT), which is used in this work to give study of identity and access management (IAM). The authors talk about the various ways distributed ledger technology (DLT) applications could be used to improve IAM. According to the authors, distributed ledger technology (DLT) has the potential to spark a period of radical change in IAM.	The fifth paper provides an introduction to IAM by utilizing DLT. The authors talk about the various ways distributed ledger technology (DLT) applications could be used to improve IAM. According to the authors, distributed ledger technology (DLT) has the potential to spark a period of radical change in IAM.
6	"Workflow integration alleviates identity and access management in serverless computing."	[26]	The difficulties that arise when employing serverless computing for identity and access management (IAM) are the main subject of this study. According to the authors, integrating workflows is one way to assist in mitigating the effects of these difficulties, and this should be taken into consideration as a viable solution.	In paper six, which is available here, the difficulties that arise with IAM in serverless computing are analyzed. According to the authors, integrating workflows is one way to assist in mitigating the effects of these difficulties, and this should be taken into consideration as a viable solution.

proposes a decentralized and dynamic SSO IAM framework for cloud multi-application outsourcing. Despite this, Paper 4 provides a comprehensive review of BIMs and their relationship to the Internet of Medical Things. The findings from both of the aforementioned investigations are included in this volume's presentation. In Paper 5, IAM is presented by utilizing DLT, and after that, the difficulties associated with merging IAM with serverless computing are investigated. The six papers present an in-depth analysis of how IAM could be improved with the implementation of blockchain technology, distributed ledger technology, workflow integration, more dependable authentication approaches, and artificial intelligence. However, it is essential to keep in mind that these technologies are still in their infancy and that a large number of obstacles need to be conquered before a sizeable percentage of the population will be able to make use of them. However, it is essential to keep in mind that research on these technologies is still in its infant stage. This is something that must not be forgotten.

Rather than focusing on improving IAM with just one of these technologies, the best strategy would be to improve it simultaneously with all of them. Businesses may make use of a wide range of different technologies to build identity and access management (IAM) systems that are safer, more efficient, and easier to use. In the end, the type of paper that is appropriate for you will be determined by the specific criteria that you have. Paper 1 is an excellent option to go with if you are interested in the beliefs held by those who operate in the field of information technology because it offers a variety of points of view. Paper 2 should be studied in its entirety if you wish to acquire a deeper comprehension of the more complicated aspects of modern authentication systems.

5. Conclusion

IAM plays an important role in the case of accessing important data. As the cybersecurity industry becomes aware of maintaining login credentials, it becomes important to accomplish IAM solutions depending on access privileges and user credentials. After conducting this research work, it can be concluded that IAM systems utilize different protocols and standards for securing personally identifiable information. With the assistance of this system, it becomes easy to follow the track of users' activities as well as prior authorizations, which can easily change the employees' performances. It has the ability to integrate the authentication of organizational infrastructure in the company of identity governance that follows different data security policies by following or informing any top-level decisions [27]. At the time of collecting relevant information from various research papers, it has come to know that the right and rule of compliance management software helps to automate as well as follow the track of different components of the IAM activities [28].

All the updated services and applications always prefer both storage and cloud services together with any kind of traditional systems and on-premise servers. Most organizations always target to sort out cyber-attacks and external threats so that all the employees can easily maintain the regular workflow. As the day advanced, it really has become so challenging to find out all the internal threats and cyber-attack incidents in the organization. It has been noticed that all the latest applications and required services propose cloud services over the traditional systems and servers, which easily manage security areas through using different tools, which creates difficulties in managing the entire identity management processes. Identity-based activities are basically used to accumulate all the relevant data, such as public keys. Data-centric characters always propose outcomes by following the latest security needs for secured communication. The data source authentication always makes sure about the data packets that have been followed during the identity access management processes.

So after completing the entire research work, it can be concluded that data-centric authentication always proposes a common security service that is needed by proposing different types of security solutions [29]. The key importance behind the IAM system is to automate recording, capturing, and controlling access permissions and user identities to improve data security. Not only that, but it also helps to provide solutions that can easily identify possible issues and find ways to mitigate them. Future research on this proposed topic will open a new door to be updated with the attitude of the latest technologies as well as keep away from any data breaches or cyberattacks. With the assistance of IAM, people can easily avoid sharing any long-term credentials as well as propose protection against any kind of illegal access. Maintaining user authentication is an important component of best practices of access management which helps to keep away any kind of unauthorized access and secure the data from data breaches [30]. Future research on this topic will help to be more conscious about the responsibilities of identity and access management.

Acknowledgment

I would like to thank God for all the blessings and opportunities bestowed on me. I would like to thank my family for their love, prayers, encouragement and unconditional support throughout my research process. Special thank you to my sisters and other family members, without whom I wouldn't have made it so far and enjoyed life half as much! I would also like to express my gratitude to my supervisor for guidance, support, clarity and constructive feedback throughout the dissertation project. Lastly, thank you to the survey participants, without whom this project would not be possible.

References

[1] Divyabharathi DN, Cholli NG. A review on identity and access management server (keycloak). *Int J Secur Priv Pervasive Comput (IJSPPC)*. 2020;12(3):46–53.

[2] Ding Y, Zhang Y, Qin B, Wang Q, Yang Z, Shi W. A scalable cross-chain access control and identity authentication scheme. *Sens*. 2023;23(4):2000. doi: 10.3390/s23042000.

[3] Sankaran A, Datta P, Bates A. Workflow integration alleviates identity and access management in serverless computing. *ACSAC '20: Annual Computer Security Applications Conference*, pp. 496–509, December 2020. doi: 10.1145/3427228.3427665.

[4] Mohammed IA. The interaction between artificial intelligence and identity and access management: an empirical study. *Int J creat Res Thoughts (IJCRT), ISSN*. 2021;2320(2882):668–71.

[5] Cameron A, Williamson G. Introduction to IAM Architecture (v2). *IDPro Body of Knowledge*. 2020;1(6). doi: 10.55621/idpro.38.

[6] Carnley PR, Kettani H. Identity and access management for the internet of things. *Int J Future Comput Commun*. 2019;8(4):129–33.

[7] Saranya N, Sakthivadivel M, Karthikeyan G, Rajkumar R. Securing the cloud: an empirical study on best practices for ensuring data privacy and protection. *Int J Eng Manag Res*. 2023;13(2):46–9.

[8] Liu H, Han D, Li D. Fabric-IoT: a blockchain-based access control system in IoT. *IEEE Access*. 2020;8:18207–18218.

[9] Alsirhani A, Ezz MM, Mostafa AM. Advanced authentication mechanisms for identity and access management in cloud computing. *Comput Syst Sci Eng*. 2022;43(3):967–84.

[10] Kaiser T, Siddiqua R, Hasan MMU. A multi-layer security system for data access control, authentication and authorization. Doctoral dissertation. Brac University; 2022.

[11] Gangavarapu T, Jaidhar CD, Chanduka B. Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artif Intell Rev*. 2020;53:5019–81.

[12] Du J, Jiang C, Wang J, Ren Y, Debbah M. Machine learning for 6G wireless networks: carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service. *Ieee Veh Technol Mag*. 2020;15(4):122–34.

[13] Chaudhry SA, Alhakami H, Baz A, Al-Turjman F. Securing demand response management: a certificate-based access control in smart grid edge computing infrastructure. *IEEE Access*. 2020;8:101235–43.

[14] Mandal S, Bera B, Sutrala AK, Das AK, Choo KKR, Park Y. Certificateless-signcryption-based three-factor user access control scheme for IoT environment. *IEEE Internet Things*. 2020;7(4):3184–97.

[15] Song F, Ai Z, Zhang H, You I, Li S. Smart collaborative balancing for dependable network components in cyber-physical systems. *IEEE T Ind Inform*. 2020;17(10):6916–24.

[16] Saini A, Zhu Q, Singh N, Xiang Y, Gao L, Zhang Y. A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet Things J*. 2020;8(7):5914–25.

[17] Putra GD, Dedeoglu V, Kanhere SS, Jurdak R. Trust management in decentralized iot access control system. *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–9, IEEE, May 2020. doi: 10.48550/arXiv.1912.10247.

[18] Kayes ASM, Kalaria R, Sarker IH, Islam MS, Watters PANg A, Hammoudeh M, *et al*. A survey of context-aware access control mechanisms for cloud and fog networks: taxonomy and open research issues. *Ah S Sens*. 2020;20(9):2464.

[19] Sevilla G. *Zoom vs. Microsoft Teams vs. Google Meet: Which top videoconferencing app is best*. PC Mag; dated 16 April 2020. https://au.pcmag.com/how-to-work-from-home/66389/zoom-vs-microsoft-teams-vs-google-meet-a-videoconferencing-face-off.

[20] Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet Things J*. 2021;8(14):11717–31.

[21] SophosLabs Research Team. Emotet exposed: looking inside highly destructive malware. *Network Security*. 2019;2019(6):6–11.

[22] Alsirhani A, Ezz MM, Mostafa AM. Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing. *Comput Syst Sci Eng*. 2022;43(3):967–84.

[23] Fugkeaw S. Achieving decentralized and dynamic SSO-identity access management system for multi-application outsourced in cloud. *IEEE Access*. 2023;11:25480–91.

[24] Alamri B, Crowley K, Richardson I. Blockchain-based identity management systems in health IoT: a systematic review. *IEEE Access*. 2022. doi: 10.1109/ACCESS.2022.3180367.

[25] Ghaffari F, Gilani K, Bertin E, Crespi N. Identity and access management using distributed ledger technology: a survey. *Int J Netw Manag*. 2022;32(2):e2180.

[26] Tang Y, Yang J. Lambdata: Optimizing serverless computing by making data intents explicit. *2020 IEEE 13th International Conference on Cloud Computing (CLOUD)*, pp. 294–303, IEEE, October 2011.

[27] Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet Things J*. 2021;8(14):11717–31.

[28] Belchior R, Putz B, Pernul G, Correia M, Vasconcelos A, Guerreiro S. SSIBAC: self-sovereign identity based access control. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1935–43. IEEE, December 2020. doi: 10.1109/TrustCom50675.2020.00264.

[29] Bera B, Saha S, Das AK, Vasilakos AV. Designing blockchain-based access control protocol in IoT-enabled smart-grid system. *IEEE Internet Things J*. 2020;8(7):5744–61.

[30] Tan L, Shi N, Yang C, Yu K. A blockchain-based access control framework for cyber-physical-social system big data. *IEEE Access*. 2020;8:77215–26.