Computer Systems Science & Engineering
DOI:10.32604/csse.2022.019355
Article

Tech Science Press

Identity Governance Framework for Privileged Users

Mansour Hammoud Alruwies[1], Shailendra Mishra[2,*] and Mohammed Abdul Rahman AlShehri[1]

[1]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, 11952, Saudi Arabia
[2]Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia
*Corresponding Author: Shailendra Mishra. Email: s.mishra@mu.edu.sa
Received: 11 April 2021; Accepted: 15 May 2021

Abstract: Information technology companies have grown in size and recognized the need to protect their valuable assets. As a result, each IT application has its authentication mechanism, and an employee needs a username and password. As the number of applications increased, as a result, it became increasingly complex to manage all identities like the number of usernames and passwords of an employee. All identities had to be retrieved by users. Both the identities and the access rights associated with those identities had to be protected by an administrator. Management couldn't even capture such access rights because they couldn't verify things like privacy and security. Identity management can help solve this problem. The concept behind identity management is to centralize identity management and manage access identity centrally rather than multiple applications with their authentication and authorization mechanisms. In this research work, we develop governance and an identity management framework for information and technology infrastructures with privileged access management, consisting of cybersecurity policies and strategies. The results show the efficiency of the framework compared to the existing information security components. The integrated identity and access management and privileged access management enable organizations to respond to incidents and facilitate compliance. It can automate use cases that manage privileged accounts in the real world.

Keywords: Privileged access management (PAM); lightweight directory access protocol (LDAP); identity management; access control; cyber-attack

1 Introduction

The outbreak of the COVID-19 pandemic has led to an inevitable rise with the use of digital technology nationwide under socio-economic distancing requirements to territorial lockdowns. Individuals and organizations now have to adapt to a changed way of working as well as living. Increasing digitalisation is leading to industries as well as educational institutions moving to work online. Governance and the management of identity will become relevant. With the rapid intensification of digital, tracking in the workplace and the problem of technostress will become rampant [1].

It is becoming increasingly clear that information technology (IT) enhances the competitiveness of an organization's in the highly competitive global marketplace of the 21st century. However, the actual practice of information technology depends heavily on efficient and appropriate IT governance. As the world becomes more digital, businesses and educational institutions are moving to work online. Identity governance and management are becoming increasingly important. In turn, the actual practice of information technology depends heavily on effective and appropriate IT governance [2].

The ideology proposed in this research focuses on managing privileged access for users under the control of a system or organization. Since security is the main concern of any organization, the level of security features available with the access management scheme should be well organized and arranged according to the time requirements. Previous authors [3–6] are mainly concerned with the analysis of information security components and risk analysis. This research focuses on managing privileged access using Active Directory services to provide an authentic and improved way of identity management for any organization.

The proposed framework will be useful to avoid various problems associated with the identity access management problem. The research mainly aims to integrate identity access management along with privileged user access management using Active Directory. Privileged access involves an active directory as a subset in the identity access management scenario. This research proposes a new and authentic way to provide privileged users a framework for managing authentication and organization work. The encouraging enormous growth and survival of all types of government systems and information technology (IT) have become fundamental. When it comes to higher education, the situation is different because universities are a special category of institutions that require a wide range of data and technologies to support teaching, learning, and research activities, such as software, educational systems, cloud applications, wireless networks, e-learning platforms [7]. To fulfill their purpose, universities or educational institutions are very versatile institutions that require both acceptable IT and information systems (IS). Information technology includes various software, various frameworks, educational systems, cloud services, and some applications [8].

The flow of communication inside and outside the enterprise poses many challenges to user security and privacy. Restricting the adversary attack is highly required, and building a mechanism that can use a framework and proper access among the authorized users. Due to these technological improvements, this paper is optimized with the integration of the Identity Access Management framework and Privileged Access Management (PAM) such as Active Directory. A highly centralized Identity and Access Management (IAM) is one of the biggest challenges for organizations today to ensure secure and compliant access to IT resources. One of the key drivers for the integration of IAM services and infrastructures and processes is the effective implementation of existing compliance criteria. Whereas previously only a limited set of enforcement criteria and policies needed to be met, governments and organizations are now gradually implementing compliance requirements that can only be controlled through standardized IAM procedures, policies, and technologies [9,10].

The benefits of process acceleration through successful IAM initiatives are also playing an increasingly important role for modern enterprises, even if initially only relevant competency characteristics were important [11]. Today, IAM means can already successfully automate much of the user management of enterprise applications, providing dedicated security analytics while enabling government services and cloud integration. The underlying access control model is mostly role-based Access Control (RBAC). RBAC improves productivity by combining employee permissions and roles [12,13]. Compared to RBAC, ABAC is much more flexible and allows mapping and coarse-grained access rules. ABAC monitors the virtues of subjects, objects, or environmental influences against well-prepared rules and allows or ignores access based on their implementation. IAM workflows such as onboarding/offboarding/

relocating employees are easier to subject to attribute-based policies than static roles [14,15]. ABAC models depend heavily on the scope and validity of the inherent attribute values of these policies [16]. Consequently, organizations using ABAC need a standardized approach to maintaining attribute data quality.

The main contributions of this research are summarized as follows:

- This research focuses on managing privileged access for users under the control of a system or organization.
- The research aims to integrate identity access management along with privileged user access management using an Active Directory.
- A framework is proposed that denotes the role of Active Directory services for both authentication and privileged access provisioning, which will be useful to avoid various problems associated with the identity access management problem.

The rest of the paper is organized as follows. Literature related to Identity and Access Management is discussed in Section 2. The proposed hybrid approach of IAM and PAM is presented in Section 3. The implementation of the Hybrid Approach is discussed in Section 4. The result analysis of the proposed hybrid system as an active directory and an experimental analysis of the proposed system and previous works are compared in Section 4. Finally, Section 5 concludes the paper with some of the future directions given.

2 Literature Survey

The literature review explains the need for identity governance, identity management frameworks in higher education institutions, and outsourcing of public sector employees. It aims to understand the key issues and summarize the primary concept of current challenges to understand the framework, legalization, digital transformation, governance, and identity management. Social media has become another powerful platform as a large amount of specific information flows through social media. Due to Identity Fraud, consumers, organizations, and governments, are losing billions of dollars discussed in [17]. Identity management and its impact on socio-economic inclusion are discussed in [18]. Also, the authors propose a theoretical framework for digital identification.

Criminals focused on new unethical business when a fraudster uses a victim's name or other private information stolen from a credit card and other claims. Identity and Access Management (IAM) formalizes the use and management of the same identity for all application domains while ensuring security. Identity management plays an important role in cloud security. Data protection and compatibility are the main issues with current identity management solutions, especially in public cloud environments. The impact of security standards and their influence on the performance of organizations are discussed in [19,20].

Identity and access management systems effectively reduce cloud-based risks, they provide a secure password and digital certificate management [21]. A large number of studies have focused on IAM methods, IAM policies and their execution and overarching access control models in recent years. For example, RBAC has become a standalone standard for controlling access to information in hundreds of organizations. Permissions are grouped into positions that are eventually assigned to employees based on this principle. This reduces bureaucratic overhead and contributes to a creeping increase in the number of roles, thus offering little flexibility regarding changing scenarios (*e.g.*, government personnel changes) [12,13].

In [16] discuss a more detailed consideration of ABAC. The identity management approach can handle passwords, compliance control, data access management, access requests, automated provisioning, and single sign-on. Purpose of effective web access requests, the provider ensures multifactor authentication, single sign-on enterprise, privileged identity & access control, and user activity compliance [11,22–24].

3 Proposed Hybrid Approach of IAM and PAM

The concept behind IAM and PAM's integration or hybrid approach is to enable a secure ecosystem over the end-user inside the organization or outside the organization.

Nowadays, there are so many malicious adversarial threads in the world that can easily destroy the organization by stealing credentials and information data. The main goal of this project is to highlight that identity management and governance are central to good cybersecurity, and role-based access control is one of the essential functions of identity and access management (RBAC) [12]. It enables device users to delegate positions and permissions required to perform specific functions across these roles. Organizations minimize both the effort required to assign user access rights and the associated costs through role-based access management.

3.1 Privileged Access Management (PAM)

A layered architecture with privileged access management is shown in Fig. 1. It illustrates the role of Active Directory services in both authenticating and providing privileged access. However, privileged access includes Active Directory as a subset in the identity access management scenario.

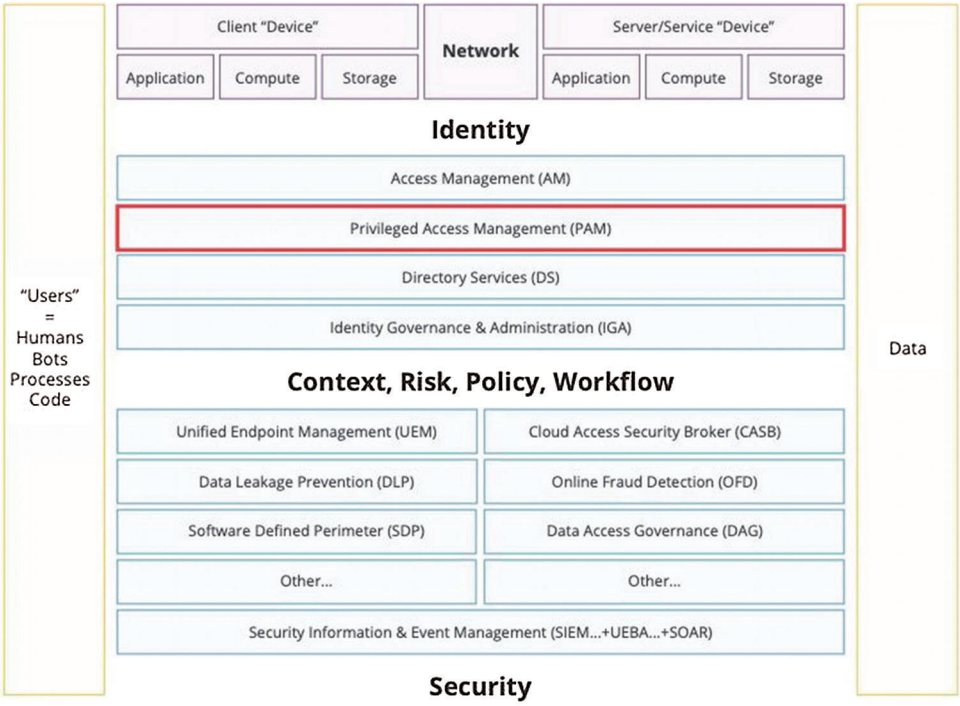

Figure 1: A layered architecture using privileged access management

A productive PAM architectural design must ensure privileges for all users, sessions, and assets. A computerized enterprise privilege technology platform is the first important part of a PAM solution that provides secure access control, inspection, alerting, and documentation for each pampered session. Lower privilege management, as well as wireless network management, are other major components of PAM. All these three solutions must be embedded and work together for the rest of the privileged universe. Tracking privileged authentication issues is required to accommodate a shared administrator account in the neighborhood or directory, a user's government account, privilege escalation, application-related accounts, network devices, credential databases, and computerization accounts, whether they are

on-premises or in the cloud. IT institutions can eliminate privileged threats and achieve compliance goals by monitoring and regulating over-privileged passwords [25].

3.2 Integration of IAM and PAM Such as Active Directory

Modern cybersecurity threats are becoming more common, yet organizations need both IAM and PAM to protect their sensitive data. Organizations implement a coordinated approach to identity access with an integrated IAM and PAM solution. The integration of IAM and PAM is shown in Fig. 2. The two most important components in a system are PAM and IAM. To achieve security goals, organizations rely on digital information to operate, manage, and compete. This includes migration to the cloud, surveillance and the ever-growing Internet of Things, the use of more developers, and the increasing reliance on them. Companies are in a constant battle to stay ahead in the ever-growing digital ecosystem. To maintain their competitive edge, they must transform their identity management programs to prevent and respond to cybersecurity threats.

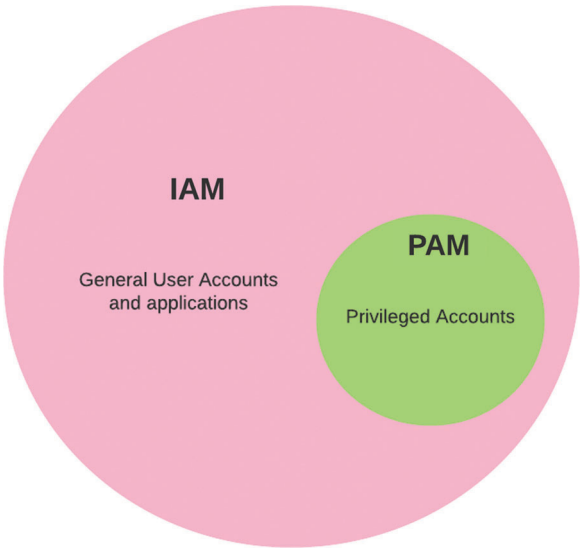

Figure 2: The Conceptual integration of the IAM and PAM

Integration of IDM and PAM is necessary for almost all applications and contexts to which IDM (with PAM) systems can adapt within and across applications, systems, and boundaries. For example, IDM (with PAM) can be applied. One of the main problems to solve is uncertainty. If an IDM (with PAM) framework is limited or expensive, developing trusted environments through appropriate security and privacy policies and practices, a user-friendly interface, and a commitment to user education and knowledge is another significant challenge to a successful implementation. In addition, a critical component of such an operation is digital identity management (IDM) with privileged access management (PAM). Finally, protection and privacy are enhanced by minimizing the data flow in transactions.

3.3 Active Directory Approach for the Integration

Digital identity management initiatives and processes have been developed in many organizations to address identity-related risk, compliance, and operational gaps. With the increasing number of password breaches, IAM access rights have become even more critical.

To better manage user access requests, permissions, accreditations, provisioning, and recovery for privileged and non-privileged users, organizations should implement Identity Governance and PAM. The significance of the proposed approach, shown in Fig. 3, using the cloud identity platform component is that it enables the integration and management of a wide range of enterprise applications and directories, whether they are in the cloud, on-premises, or a combination of both. It typically requires creating a service account that must be set up for each application to gain access to identity information. While these service accounts are typically granted administrative access to create, modify, and delete accounts in the target applications, they are rarely granted broader privileges. As critical enterprise applications are increasingly integrated into the IAM platform, it is not a difficult task for attackers to gain access to high-value targets.

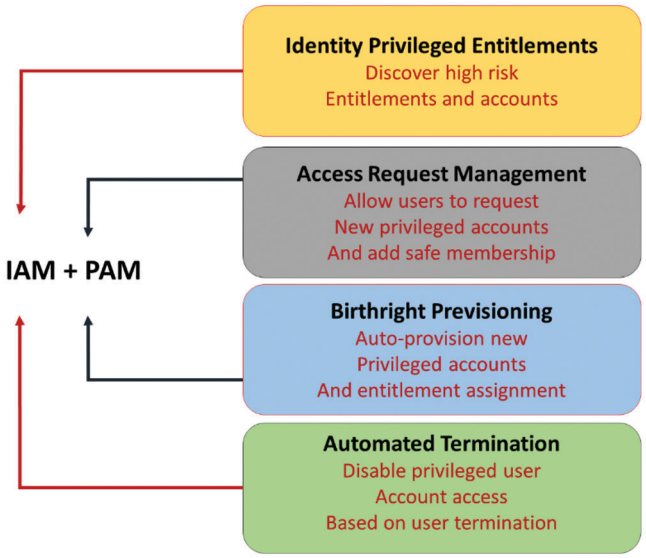

Figure 3: Proposed integrated approach using IAM and PAM as an active directory

4 Implementation of Hybrid Approach (Active Directory)

The advent of technological advancement all over the world focuses on well-organized government as well as business-oriented intelligent control measures within the organization. This paper proposes an integrated approach with the inclusion of IAM as an authentication tool and PAM as a restrictive access control measure to an Active Directory. This method extends the secure access policies between the government and business organizations to know every activity and record the adversarial attack from the proposed system. The entire experimental setup has been implemented in Shaqra University, Saudi Arabia, and is analyzed using the real-time data available in the university database. The basis for careful planning that can successfully deploy an application using the proposed Active Directory hybrid mechanism. It enables automated deployment and protection that streamlines onboarding and reduces the time required for efficient deployment. This blend means that the framework can be seamlessly customized and reduce downtime for your end-users.

4.1 Identifying Test User

To verify provisioning, use this segment to define a collection of users or groups of users. The configurations in the preconstruction phase, define the users for each item, as shown in Tab. 1.

Table 1: Define the test users to check that perhaps the roles' settings function

Test role	Test user
<Role name>	<User testing role>
<Role name>	<User testing role>

After the test users are marked, use this procedure to customize protected multifactor authentication for the test users. The graphical interface supports certain processes allowed in the Unified Communications.

4.2 Configure Hybrid Approach (Active Directory) for Roles

1. Set the portal function as planned.
2. Traverse to the post roles, select the roles and then select the installation location.
3. If the test users are already permanent admins, people can be searched and converted from permanent to qualifying by clicking on the three dots in their rows. They can create a good qualifying assignment if they don't have position responsibilities yet.
4. Try numbers 1–3 for all positions to be tested.
5. Once the test users are set up, give them a connection to activate the role.

This step can also be used to maximize contact with existing participants. Tab. 2 shows the steps required to test the expected result in terms of the activation behavior.

Table 2: Steps involved to test expected outcome in terms of the behavior of activation

Role	Expected behavior during activation	Actual results
Global admin	Requirement MFA, Require permission, The approver is notified and authorized to accept, Function expired after the preset period.	
Individual subscription	The qualifying assignment requires MFA, expired after the span of time set.	

4.3 Communicate Hybrid Method (Active Directory) about Affected Stakeholders

Implementing Advanced Multifactor Authentication would impose specific requirements on users with protected roles. Although Protected Information Governance addresses the security concerns associated with protected identification, the transition must be effectively communicated to the organization prior to implementation.

4.4 Targeting Production of Hybrid Approach (Active Directory)

Once testing is complete and comprehensive, commit the allowed multifactor authentication to manufacture by running all test cases in their delegated information management framework for all users, including their defined roles. In the meantime, organizations typically test and implement an Azure subscription at Protected Unified Communications for the proposed platform.

4.5 Use Information Management Authorized Warnings to Protect User Special Access

Perceive security alerts for more details on using the built-in alerting features of authorized unified communications to protect the facility. These alerts include managers not using sensitive roles, roles being delegated beyond the protected unified communications, roles being activated more frequently, and more. To fully protect the user's facility, the user should review their notification list and address the issues regularly.

4.6 Create Frequent Authorization Reports to Constantly Monitor Privileged Identities in User Institution

Connect reviews are indeed the perfect way to express stakeholder or individual reviewer interests when each user needs a protected identity. Service recommendations are perfect when the threat landscape needs to be reduced and consistent. The portal role accessibility assessments included portal role accessibility assessments for even more details on how to begin an accessibility review. In certain cases, the portal role assessor is the consumer, and the portal role assessor is the participant where the role is to be played. Fortunately, companies also have protected identities that are not tied to a single person's email address. In these situations, no one investigates or verifies access.

5 Result & Discussion

The intent to optimize a hybrid approach such as an active directory within the organization is highly required to define each user's access controls for security and secure, transparent tracking against the targeted adversarial attacks in the organization. Despite the advancing cybersecurity threats, organizations still need Active Directory to combine of IAM and PAM to protect their sensitive data. Another motive for agencies to implement these solutions is to escape the unpredictable and confusing behaviors employees use to access and report on their data. Organizations develop a synchronized process for the uniqueness of access, which is done with a combined solution like Active Directory. IAM provides services by authenticating the particular user, and PAM includes their administrator controls with assigning the user's access control operation as a facility of Active Directory interface mechanism.

The proposed method is well organized to accomplish the task and well control the access by the global administrator using the methods and policies within the organization. The systems generate the expected results by incorporating different policies that define the proper setup in terms of access to each device and network within the access mechanism with user privileges. Tab. 3 illustrates the efficiency of the proposed work compared to the existing information security components. An integrated implementation of Identity and Access Management (IAM) and Privileged Access Management (PAM) can solve this problem and enable organizations to respond to incidents and facilitate compliance reliably. This can automate use cases that involve managing privileged accounts in the real world. The Proposed unified policy-driven approach to IAM for all users have the following benefits;

- Identify privileged accounts in addition to the passwords installed by the IAM solution in the PAM program.
- Implement a single policy-driven IAM solution for all users.
- Automatically provision fresh privileged accounts through role-based access provisioning or IAM application authorization policies.
- Leverage user profile characteristics, including title, consulting firm, and profile, to grant sufficient access to privileged accounts.
- Automate regular access audits on accounts.
- Automate and implement separation of duties policies (SOD) for privileged and non-privileged accounts.

- Modularizing privileged account terminations based on segregation of duties or termination incidents as per the Active Directory solution.
- Eliminating doubt about who is allowed to receive privileged or restricted information externally and within the organization.
- The efficiencies created by autonomous systems reduce costs, allowing organizations to focus on building and protecting their networks.
- Implementing a process that prevents hackers from getting in saves both time and money.
- Enforcing new and existing security policies is simplified by the system.

Table 3: Comparison between proposed work with other information security components

S. No.	Information security component	Proposed	[26]	[27]	[28]
1	Governance	Y	X	X	X
2	Security strategy	Y	Y	X	Y
3	Leadership	Y	Y	Y	Y
4	Security organization	Y	Y	Y	Y
5	Policies, standards, and guidelines	Y	Y	Y	Y
6	Measurement metrics & ROI	Y	X	Y	Y
7	Compliance and monitoring	Y	Y	Y	Y
8	User management	Y	Y	X	Y
9	Training & awareness	Y	Y	X	Y
10	Ethics	Y	Y	Y	X
11	Privacy	Y	Y	X	Y
12	Trust	Y	Y	X	X
13	Certification	X	X	Y	X
14	Best practice	Y	Y	Y	Y
15	Asset management	Y	Y	Y	X
16	Physical and environmental security	X	Y	Y	Y
17	Technical operations	Y	Y	Y	Y
18	System acquisition, development and maintenance policy	Y	Y	Y	Y
19	Incident management plan	Y	Y	X	Y
20	Business Continuity plan	Y	Y	X	Y
21	Disaster recovery plan	Y	X	X	Y
22	Risk assessment process and plan	Y	Y	Y	Y
Number of components with Y(Yes) %		86%	81%	64%	72%

Protecting the identity and limiting access control is the main reason for using an Active Directory. The system is controlled only by passwords. This means that the employee's access code only has value if they can influence it. Regardless of the company's size, installing and configuring an Active Directory can be expensive and time-consuming. For security reasons, it must be integrated with existing security systems. Where possible, many companies rely on the security experts at IT to develop and enforce comparatively

better frameworks, such as two- or three-factor authentication, to avoid disruption to employees and company operations.

6 Conclusion and Future Work

In this research, we have compared and identified all the access management parameters prescribed by different researchers in the past. The proposed framework includes Active Directory collaboration integrated with privileged access management. The ideology proposed in this paper was tested on a demonstration system in a data center network. The comparison between the framework proposed in this research and the previous frameworks enables understanding and realizing that the proposed framework is more stable and secure to provide proper access management for privileged users. The technique highlighted in this context is tested for authenticity and security parameters. The proposed framework provides 86% security as compared to the previously occurred results of various access management security frameworks. The framework is deployed for a generic data center environment using an Active Directory and provides more capabilities and features than those deployed without Active Directory. The advent of technological advancement all worldwide focuses on well-organized, both government and business-oriented intelligent control measures within the organization. This research proposes an integrated approach with the inclusion of IAM as an authentication tool and PAM as a restrictive access control measure to an Active Directory. This method extends the secure access policies between the government and business organizations to know every activity and record the adversary's attack from the proposed system. The proposed mechanism can be an important method to protect government data or important business oriented data from unauthorized or adversary attacks, which is always difficult in any leading organization. This research is just an initiative for a better-digitized system in terms of cybersecurity that can be used in both public and private organizations to create a trusted ecosystem for any organization. For future work, we are still thinking to integrating some cryptography-based strong authentication settings and combine them with effective privilege control measures that can provide very trustworthy and relatively better results for the government system or business-oriented institutions.

Acknowledgement: The authors sincerely acknowledge the support from Majmaah University, Saudi Arabia for this research.

Funding Statement: The authors would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project Number No. R-2021-150.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Sharma, S. B. Borah and A. C. Moses, "Responses to COVID-19: The role of governance, healthcare infrastructure, and learning from past pandemics," *Journal of Business Research*, vol. 122, no. 6, pp. 597–607, 2021.

[2] N. Pandey and A. Pal, "Impact of digital surge during COVID-19 pandemic: A viewpoint on research and practice," *International Journal of Information Management*, vol. 55, no. 1, pp. 1–5, 2020.

[3] Y. Cao, Z. Huang, Y. Yu, C. Ke and Z. Wang, "A topology and risk-aware access control framework for cyber-physical space," *Frontiers of Computer Science*, vol. 14, no. 4, pp. 1–16, 2020.

[4] S. Zareen, A. Akram and S. Ahmad Khan, "Security requirements engineering framework with BPMN 2.0. 2 extension model for development of information systems," *Applied Sciences*, vol. 10, no. 14, pp. 1–24, 2020.

[5] Y. Maleh, M. Zaydi, A. Sahid and A. Ezzati, "Building a maturity framework for information security governance through an empirical study in organizations," *Research Anthology on Artificial Intelligence Applications in Security*, vol. 1, pp. 143–173, 2021.

[6] S. AlGhamdi, K. T. Win and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Computers & Security*, vol. 99, no. 4, pp. 1–39, 2020.

[7] I. S. Bianchi and R. D. Sousa, "IT governance mechanisms in higher education," *Procedia Computer Science*, vol. 100, no. 2, pp. 941–946, 2016.

[8] I. Indu, P. M. R. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574–588, 2018.

[9] M. Bradford, J. B. Earp and S. Grabski, "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*, vol. 15, no. 2, pp. 149–165, 2014.

[10] F. Alhaidari, A. Rahman and R. Zagrouba, "Cloud of things: Architecture, applications and challenges," *Journal of Ambient Intelligence and Humanized Computing*, vol. 3, no. 6, pp. 1–19, 2020.

[11] 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, pp. 1–16, 2016.

[12] S. T. Alshammari, A. Albeshri and K. Alsubhi, "Integrating a high-reliability multicriteria trust evaluation model with task role-based access control for cloud services," *Symmetry*, vol. 13, no. 3, pp. 1–27, 2021.

[13] A. Sathya and S. K. S. Raja, "Privacy preservation-based access control intelligence for cloud data storage in smart healthcare infrastructure," *Wireless Personal Communications*, vol. 118, pp. 1–20, 2021.

[14] R. Zhang, G. Liu, S. Li, Y. Wei and Q. Wang, "ABSAC: Attribute-based access control model supporting anonymous access for smart cities," *Security and Communication Networks*, vol. 2021, pp. 1–11, 2021.

[15] S. Rouhani, R. Belchior, R. S. Cruz and R. Deters, "Distributed attribute-based access control system using permissioned blockchain," *World Wide Web-internet and Web Information Systems*, vol. 24, pp. 1–28, 2021.

[16] Z. Wang, D. Huang, Y. Zhu, B. Li and C. J. Chung, "Efficient attribute-based comparable data access control," *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3430–3443, 2015.

[17] M. A. Ali, M. A. Azad, M. P. Centeno, F. Hao and A. V. Moorsel, "Consumer-facing technology fraud: Economics, attack methods and potential solutions," *Future Generation Computer Systems*, vol. 100, no. 11, pp. 408–427, 2019.

[18] A. Addo and P. K. Senyo, "Advancing e-governance for development: Digital identification and its link to socioeconomic inclusion," *Government Information Quarterly*, vol. 38, no. 2, pp. 1–15, 2021.

[19] S. Mishra, S. K. Sharma and M. A. Alowaidi, "Analysis of security issues of cloud-based web applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1–12, 2020.

[20] S. Mishra, M. A. Alowaidi and S. K. Sharma, "Impact of security standards and policies on the credibility of e-government," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1–12, 2021.

[21] M. Beltran, "Identifying, authenticating and authorizing smart objects and end users to cloud services in internet of things," *Computers & Security*, vol. 77, no. 2, pp. 595–611, 2018.

[22] M. Kunz, A. Puchta, S. Groll, L. Fuchs and G. Pernul, "Attribute quality management for dynamic identity and access management," *Journal of Information Security and Applications*, vol. 44, no. 1, pp. 64–79, 2019.

[23] M. Habiba, U. Masood, R. Shibli and M. A. Niazi, "Cloud identity management security issues & solutions: A taxonomy," *Complex Adaptive Systems Modeling*, vol. 1, pp. 1–37, 2014.

[24] D. H. Sharma, C. A. Dhote and M. M. Potey, "Identity and access management as security-as-a-service from clouds," *Procedia Computer Science*, vol. 79, no. 13-14, pp. 170–174, 2016.

[25] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi and A. S. Ghamdi, "Blockchain platforms and access control classification for IoT systems," *Symmetry*, vol. 12, no. 10, pp. 1–17, 2020.

[26] ISO/IEC 27000-2018, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.

[27] J. H. P. Eloff and M. M. Eloff, "Information security architecture," *Computer Fraud & Security*, vol. 11, no. 11, pp. 10–16, 2005.

[28] A. D. Veiga and J. H. Eloff, "An information security governance framework," *Information Systems Management*, vol. 24, no. 4, pp. 361–372, 2007.