Integration of Identity Governance and Management Framework within Universities for Privileged Users

Shadma Parveen[1]
School of Management and
Economics, University of Electronic
Science and Technology of China
Chengdu, 611731, China

Sultan Ahmad*[2]
Department of Computer Science,
College of Computer Engineering
and Sciences, Prince Sattam Bin
Abdulaziz University, Alkharj
11942, Saudi Arabia

Mohammad Ahmar Khan[3]
College of Commerce and Business
Administration, Dhofar University
Oman

***Abstract*—The development of high-tech progression around the world, with the attentions of governance body and private companies towards well-organized setup access control measures within the organization. The importance of these exceedingly essential perception, this article is proposing an integrated approach with the assimilation of IAM (identity access management) as an authentication tool and PAM (privilegd access management) as a restricting accessing control measure in terms of an active directory. Originally the experimental setup organized within the Prince Sattam Bin Abdulaziz University, and it is analyzed using the real-time data which is available within the university database. We found that the proposed mechanism can be a vital method for protecting governance data or key business-oriented data from the unauthorized or adversarial attack. We also reviewed and compared other access control methods and find that the integrated method is relatively have an advantage to deal accessing task in any premier organization.**

Keywords—Identity management; governance framework; privileged access management; security; privacy

I. Introduction

These days, propagation of the communication within the organization or outside world is very common. It is also very necessity to engage proper protocol to address effective and innovative things to manage secure access control over the system. The covid-19 disease outbreak has led to an inevitable rise with the use of digital technology nationwide subject to socioeconomic distancing requirements including territorial lockdowns, individuals and organizations now have to adjust a changing method of working as well as residing[1]–[5]. A rise in digitalization is leading industries as well as educational institutions to switch to work online. Governance and the management of identity will become relevant. They will require design and regulatory analysis. Online workers will likely increase in size, rising job distribution issues, teamwork, motivation, work overload, and present aspects. With rapid intensification in digital occurrence, tracking among the workplace and technostress problem will turn out to be prevalent[6]–[8]. Information technology (IT) improves companies' ability to compete in the 21st century's intensely competitive global marketplace has become increasingly evident. However, the actual practice of information technology count on profoundly on efficient and adequate IT governance. The flow of communication within the organization and outside is inviting many security and privacy challenges among the user. The restriction of the adversarial attack is highly required and build such type of mechanism which can deal to provide a framework and use proper access among the authorized user[9]–[11]. To ensuring such type of mechanism our intension to encourage to develop an essential tool or any type of integration approach, concerning these technological enhancements, this article is going to optimized with the integration of the identity access management framework (IAM) and privileged access management (PAM) as an active directory which is demonstrated on the Fig 1. The architecture of the system incorporates as a managerial way such as life cycle manager, compliance manager, password manager and the layout of the system demonstrated such as identity intelligence, dashboards, reporting console, analysis console. This system is performed governance console including policy model, identity warehouse, role model, workflow engine, risk model, IT security, 3rd party provisioning, IT services management and mobile device management with the fronted communication in terms of external world.

Integrating as an active directory is necessary for almost all applications and contexts to organizations which can adapt within and across applications, systems, and boundaries. For instance, active directory can apply. One of the principal problems to be tackled is uncertainty. If an integrated framework is restricted or expensive, the development of trustworthy environments through adequate security and privacy policies and practices, a user-friendly interface, and commitment to user education and knowledge is another significant challenge for its successful implementation. Due to the organization's rapid growth and the application that they are using, the user will have to memorize all his credentials for each application[12]. Moreover, a crucial component of such an operation is digital identity management with privileged access management. Today public and private sector organizations vary dramatically in their approach to active directory designing their means of generating, checking, sorting, and using digital identities through their network and the internet. In our increasingly interconnected economies, the lack of shared policies and methods creates privacy, protection, and efficiency problems and hampers an organization's ability to deliver convenient service to customers. Besides, improving user conveniences is one of the

*Corresponding Author

significant advantages of active directory. Effective integration may reduce the inconveniences and inefficiencies caused by the need to keep track of various identities, passwords, and authentication requirements when used through organizations. Similarly, more functional user interfaces will boost accessibility and increase online services for registration and log-in processes. Finally, protection and privacy enhancement by minimizing the flow of data during transactions, only requesting, transferring, and storing what is needed, security and privacy are improved, and effective integrated approach can minimize the transactional details needed by multiple device users and reduce the security and privacy risks.

The significant contribution of the proposed study is provided a hybrid approach between the identity and access management and privileged access management to protect highly confidential access data within the organization or outside world. The incorporating this mechanism is validated that using these types of hybrid mechanism can be a better option to handle things and restrict some adversarial attacks into the entire system. The adjustment between IAM and PAM, by describing a general project management methodology for IAM environments, we attempt at shutting down this research gap. It not only provides a generic high ranking research method, but also incorporates specific methods for the handling of attributes of quality. This fulfills the demand for the measurement of ABAC's quality evaluation and at the same time provides an interconnected process-oriented approach which is applicable to large-scale IAM scenarios.

The organization of the articles is as follows: Section 2 highlights literature background of the hybrid approach as a well-defined context about access control, Section 3 proposed an integrated methodology which provides a highly trusted architecture to deal with control access about the user within the organizations, Section 4 discussing optimization of proposed mechanism with advantages as well as disadvantages and finally Section 5 concludes with future work.

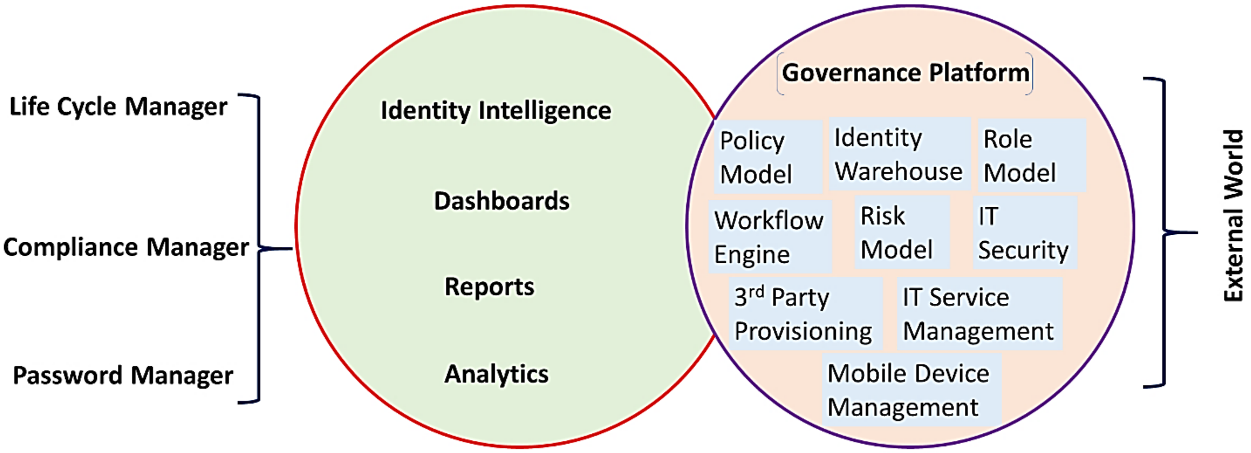

Fig. 1. Integrated Conceptual Design.

II. Preliminaries

The intention of the governance and organizational setup is to improve control access methodologies within the institution from the external world. This requires due to day-by-day new threads coming to unauthorized access within the organization and stealing valuable secret data to destroy business as well as economic consequences around the world. Concerning these thread and new epidemical policies during covid-19, its hand to mouth to control adversarial data theft about the organization. So, it is required to provide an architecture to address these shortcomings, the adaptation of the identity and access management with integration of privileged access management is quite favorable option to adjust governance as well as business companies to fight back and control these valuable data and any miss happening things within the organization or institution. Identity management (IdM) is in a position to perform such functions as management, maintenance, discovery, management, enforcement of policies, exchange of information and substantiation. Identity and access management (IAM) formalizes the use and management of the same identity for all application areas and guarantees simultaneous security[13]. The software is being utilised to validate devices, users or services as well as deny or allow access to data or other infrastructure components. In the event that the application is accessed, the system or service does not have to authenticate all its identity shops or authentication mechanism. Rather, the identity checking process can be customized such reliable identity provider, which actually decreases the volume of work among application. Management of identity and access simplifies management of transmitted distributed projects. IAM are utilised in whole business (B to B) or even amongst a private innovativeness with cloud provider within a company or outside the enterprise[14]. IAM has a broader organizational area to identify entities, cloud objects and manage admittance to resources oriented predetermined policies [15], [16]. Identity and access management are a number of functioning zones. Identity managing and provision, federated identity management, validation administration, compliance management and authorization management [17] are all functioning zones. These functioning zones ensure the secure and effective integration of authorized users at clouds. The service provisioning markup language (SPML) is an XMLrelated framework which is used to manage identity. It enables communication on resources, users and services amongst officialdoms. One of SPML's failings, this employs multiple symmetric cryptography from innumerable providers which lead to a range of marginal applications (APIs). Since APIs not the identical provider, interacting with each other is difficult. Authentication management is the second industries application of IAM. This ensures secure management of credentials including passwords as well as digital documentations [18].

Federated identity management is the third operational field of IAM. The said identity management validates cloud facilities using the selected ID provider of the organization. Management of federated identities guarantees privacy, integrity as well as non-repudiation. It therefore ensures the confidence here between mobile application as well as the identity provider by transferring certified public keys from public key infrastructure (PKI). The fourth main activity is the management of authorizations. After authentication process, authorization management decides whether such an authenticated entity is permitted to perform an application. Compliance management is the last functioning zone of IAM. This ensures that the resources of an association are secured and accessible under the current policies and regulations [19]. In the field of cloud security, Identity management plays an important role. Privacy as well as compatibility are the major problems with current solutions to identity management, particularly in public cloud environments [10], [11], [18]. Currently, IAM systems are effective mechanisms for reducing cloud-based risks. Many institutions provide an IAM system to ensure information through the influence of each user's access authorization [20]–[22]. SailPoint, IBM, Oracle, RSA as well as Core security are the most popular IAM system providers. SailPoint's identity management approach is capable of handling passwords, compliance control, data access management, requests for access, automated delivery, as well as Single Sign-On [9]. Purpose of effective in web access requesting, providers to ensure, single sign-on company, multi-factor authentications, access control, privileged identity, and compliance of user-activity are available through the IBM identity and access management Suite. Oracle identity & access management offer four keys cloud security mechanisms. [23] explained an identity management system, and its functions, including security roles to prevent various scams and instances of identity theft. A distinction is presented between the conventional and new scope of identity management. As a prerequisite for the current IT period, an identity management framework is given. [24] reported that most emphasis on identity security has centered on securing customer information in the area of virtualization. However, as they use cloud services, users usually leave a trail, as well as the subsequent verification of accounts can potentially contribute to the leakage of confidential personal information. In the meantime, cyber criminals can do damage to cloud service providers by the use of fake identities. The author is introducing a credibility framework and developing a prestige identity management model for information computing to address these issues. Throughout the model, anonymous sources are created based on a credibility identity to ensure that aliases are untraceable, as well as a framework is suggested to measure user credibility, that enables cloud providers recognize malicious users. Investigation verifies that perhaps the template will guarantee that data centers are accessed anonymously by consumers and also that cloud providers efficiently determine the reputation of users thereby infringing consumer privacy. [25] addressed and offers the efficient assessment model of IT administration that could be used in specific, by organizational management throughout the HEI. In addition, this research identifies the variables that lead to successful IT accomplish a specific objective upon that domain's published studies. The suggested model needs to be evaluated in future projects by someone else by empirical research.

Privileged access management offers an automatic credential managing as well as sessions managing solution for secure accessing control, audit, notification with logging for all privileged accounts. The methods are intended to control localized or domains shared admin privileges; a client's account and admin account, a customer's service, network device, operating system, application (A2DB) accounts and database. IT businesses can reduce privileged risks and meet assessment of progress by increasing the authority and ownership over authorized credentials. The benefit of approach, although, requires on all such situations of usage and even on the presence of resources on site, virtualized or cloud environments. Ecosystems also require to take account of advance reliability, breaking glass, disaster recoveries, as well as stint to recover when the application itself faults or underlying equipment part from connections to web access which could trigger a breakdown happens. Privileged information security used as a Saas platform (software as a service) can only run in the clouds or allow special supervision nodes to drive as well as combine policies as well as events. These systems are fully maintained by PAM manufacturer as well as share data centers at multi-tenant installation with other PAM customers. Although nearby few PAM implementations at cloud utilizing SaaS at the moment, the trend implies that companies acquire assurance in the storage of PAM cloud credentials, administration tools and policies. This approach is determined by personal suppliers and system integrators, who offer economic services related on financial PAM capabilities as well as with no required skills by consumers.[26] explained in his article, amongst the most complex issues for device integration of 4G generation communication. Which is very complex in terms of safe multimedia delivery in current and future networks. This incorporation implies that in order to deliver their facilities to users, multiple service and network providers would have to collaborate. Such multi-domain setting poses a major threat to the consumer that has an agreement with the consumer and even just a restricted numeral of carriers and service providers confidence. [27] suggested about the model of digital identities. Confidence management should create and check the confidence to provide lead to increased results for online transactions such as reactants between the purchase and sale of products and services, improved retention and loyalty, expanded credibility, etc. Author discusses the need and value of confidence managing in the digital world, along with the different models and strategies required to mitigate confidence. For the existing options, a qualitative analysis was presented. In view of the large-scale emergence of the digital world and electronic firms, the research seems to have a lot of significance. [28] Characterizes a case of developing a stable identity management system as well as its organizational structure in accordance with the VAHTI protection guidelines of the Finnish government. The construction project was about to be conducted in compliance with the directives for government protection, while adopting the management structure of the supplier itself. [29] referred the goal of his article is to examine how or when integrated knowledge management of a seaport terminal operation can be efficiently shared between the most advantageous and cost-effective great skills, to potentially boost their access control, a road haulier as well as a rail operator. The automated exchanging of characteristics depends on the standardization of the participating actors among information technology. In this analysis, compatibility is accomplished through an existing simple object access protocol. His research paper adds to previous studies by creating a cost comparison that identifies the characteristics affecting four principles (from low advantage/low cost to high advantage/high cost) data cultivation, committed sharing of data, opportunistic exchange of information, as well as preventing sharing of information.

III. Material and Proposed Method

The idea behind to integration or hybrid approach of the IAM and PAM are to facilitate secure ecosystem about the end user within the organization or outside the organization. Nowadays, there are so many malicious, adversarial threads available in the world to make highly risk and easily destroy organization with stealing credential, informative data. The key objective of this project is to clarify that identity management and governance are central to good cybersecurity, and role-based access control is among the essential characteristics of identity and access management (RBAC). Role-based access control enables device users to delegate positions[30]. Moreover, permissions are required to execute specific functions across these roles. This implies that users are not explicitly granted authorizations but rather obtain them through their allocated profession function or responsibilities, meaning whether someone enters the business, switches offices, goes on leave, or leaves the company, their access rights are easy to handle and stay in charge. Instead of addressing user access rights at a granulated level, operator access rights are combined into several positions across different systems[31]. This means that you mechanically have one set (combination) of defined access rights if your effort in the Finance team, which is different from if you work in the marketing team. Organizations minimize both the difficulty of granting user access rights and the related costs by role-based access management. It offers the ability to evaluate access rights in order to ensure compliance with different legislation, as well as to refine processes such that new workers can be up as well as successively work from the beginning, as it is already defined that the new member of staff would access systems, all based on his or her position in the company. The market advantages are various. This also increases productivity, in addition to the apparent improvement in security across the company, resulting in smoother onboarding and off-boarding processes and enforcement, as an organization has a higher degree of control and understanding of who has access to what and why, as well as decreasing directorial work, IT care and creating price savings.

A. Integration Methods

In numerous systems of government, digital identity management initiatives and processes have been developed in order to deal with identity-related risks, compliance, and operational gaps. in order to stay one step ahead of the competition, companies must regularly evaluate their identity solutions' abilities. An increase in the number of password-related breaches has made the issue of IAM access rights even more critical. To safeguard data from internal and external threats, the several organizations still have yet to implement mature capabilities that enable them to effectively manage privileged access, even though the frequency of the compromise of privileged accounts has increased. Compounding the risk of compromise has been added to the equation. This type of organization has invested in a product, but it hasn't implemented the processes as well as governance to make it work. Other organizations may have well-established processes, but they are missing the necessary supporting technologies that would be required for addressing privileged access threats at an enterprise scale. Identity governance and PAM solutions have been implemented by some organizations, but few have combined the two. For many companies, this could lead to the inconsistent application of processes and policies across silos of tools, which would result in incorrect reporting and failed audits.

In order to better manage both privileged as well as nonprivileged user access requests, authorizations, accreditations, provisioning, and restoration, organizations should implement Identity Governance and PAM. The importance of the proposed approach as shown in the Fig. 2 using cloud identity platform's component is that it makes it possible to integrate with and govern a wide variety of enterprise applications as well as directories, whether they are in the cloud, on-premise, or a combination of both. Creating a service account is typically required, which must be set up for each application to gain access to identity information.

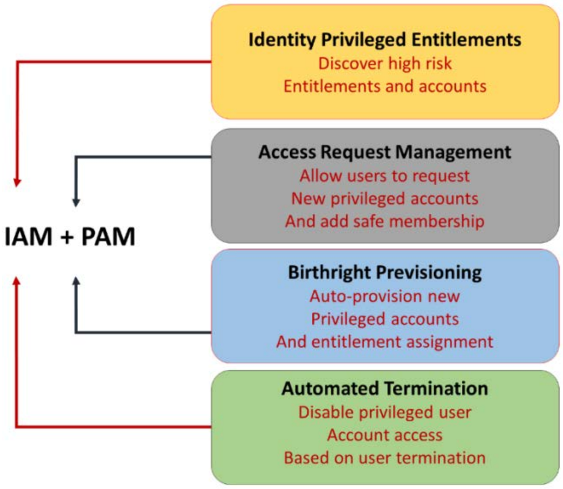

Fig. 2. Integrated Approach.

B. Session Flow within the Optimised System

The proposed incorporation of the hybrid approach is significantly organized as shown in the Fig. 3. Where it is described the conceptual session flow within the organization. The implemented mechanism is targeting to achieve better connection-oriented way within the organization to tackle users accessing policies and its managing session to accomplishing the task. In the session flow operation, some sort of the protocol handler is incorporated to setup its goal and provide accessing things according to user's authorization skills. In which the used protocol handlers are listed as follows:

1) Secure connection: Communication lines prior among each node are optimised securely. This can be validated in the Fig. 3 where it is demonstrated very well how the transformation happen within the entire system. Our optimised system has taken care secure communication and tracing each activity with the monitoring capacity easily.

2) Launch application locally: Initially the optimised setup launched with locally installed server to administering each activity. The incorporated adjustment was quite well to reach desired outcomes.

3) Session recording: The additional process is inbuilt in the optimised setup which is known as session recording concept. This feature is enabling to monitoring task within the university setup and this can provide real proof about the adversarial attacks or miss use within the organization very well. Utilising this mechanism gives freedom to know who want to access our setup then it can be possible to take immediate action against the happened activities.

4) Terminating session: The administration of the entire setup can easily terminate suspected activity within the university accessing lines. The incorporation the whole process it can be easily seen that each process is providing distinguished outcomes to handle security a privacy within the system to integrate IAM and PAM.

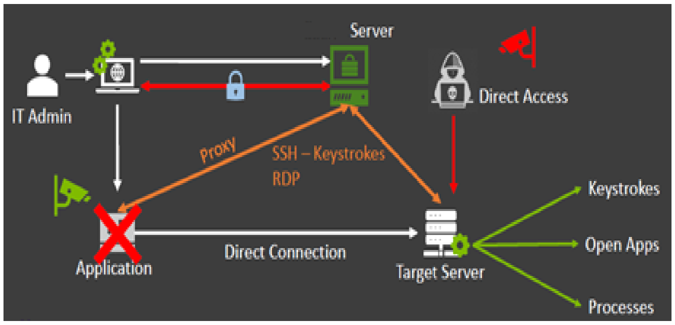

Fig. 3. Session Flow Diagram within the Applied Mechanism.

C. Implementation with Hardware and Software

The implementation of the integrated approach is needed appropriate hardware and supporting software utilities to successfully run proposed thought. The proposed integrated method is needed highly equipped hardware resources which are illustrated in Table 1 very well. The required supporting software is also defined very well in the Table 2. The collectively incorporation among the hardware and software utilities produced an integrated mechanism which can be easily used among the organizations as well as any universities for the security and safety from the external world or adversarial attacks.

TABLE I. HARDWARE SPECIFICATION FOR THE IMPLEMENT

VM Name	**CPUs >=2 GHz**	**RAM (GB) >=4 GB**	**Storage Space (GB) >=100 GB**	**OS Advance Version**	**Comments**
Server Node 1	8	16	500	Windows Server 12 or Higher	
Server Node 2	8	16	500	Windows Server 12 or Higher	
Database Cluster	8	16	1000		It entails if customer does not have present DB
Site Connector	2	4	100	Windows Server 12 or Higher	

TABLE II. COMMUNICATING PORT FOR THE IMPLEMENTATION USING SOFTWARE

Application/Process	**Traffic Types**	**Port**	**Sources**	**Destination**
Discovery	Microsoft DS SSH RPC Port Range Epmap	445 22 49152-65535 135	Secret Server IP	Work Stations
Web Server	HTTP HTTPs	80 443	IT Admin IP	Secret Server
Active Directory Syn	NTLM LDAP LDAPS Kerberos	445 389 636 88	Secret Server IP	Active Directory
Remote Changer password	Oracle Telnet NTLM LDAPS MS SQL SSH LDAP Sybase Kerberos	1521 23 445 636 1436 22 389 5000 88	Secret Server IP	Work Stations
Database	TCP/UDP SQL Connections	1433	Secret Server IP	Database Cluster
Load Balancer	HTTP HTTPs	80 443	Load Balancer IP	Secret Server IP
RADIUS Server	RADIUS	1812	Secret Server IP	RADIUS Server
Email	SMTP	25	Secret Server IP	Email Server
Rabbit MQ	MQTT	5672	Secret Server IP	Rabbit MQTT

IV. Discussion Towards Optimization

The integrated mechanism for the optimization towards security and safety from external world within the organization and universities is very necessary. Discussing an integrated method which is the highly acceptable due to achievement of the various factors including major access controls mechanism incorporated with hybrid approach of IAM and PAM. The incorporation of this method reflected as a better mechanism which gives three-way access control mechanism as shown on Fig. 4. The first one is endpoint privilege managing. This managing administration gives very least privileged as well as credential theft protection within the organization to remain safe and protected towards external things. The second one is core privileged access security managing. This managing administration is provided remotely vendor access, risk-based credential security, protection of session management attacks and protection of least privilege server with domain controller. The third one is application access managing. This managing administration is illustrated tools, secret managing applications, containers and other develops. These all protection is coming from the optimization of IAM and PAM in a certain degree of integration methods as mentioned in the proposed section. During incorporating and implementation it seems some advantages to explore which is quite justifiable to integrate these applications.

A. *Benefit of the Integrated Methods*

One integrated identity and access management (IAM) and privilege access management (PAM) implementation can resolve this issue and make it possible for businesses to reliably respond to incidents and help facilitate regulatory compliance. When used, it can be used to automate use cases that involve the management of privileged accounts in the real world, proposing a unified, policy-driven approach to IAM across all users.

- Discover privileged accounts in addition passwords installed by the IAM solution in the PAM program.
- Implement a single, set of policies IAM solution for all users.
- Supplying fresh privileged accounts automatically by role-based access provisioning or IAM application authorization policies.
- Utilize user profile characteristics including title, consulting firm including profile to allow sufficient access to privileged accounts.
- Automation of periodic accounts access checks.
- Automation and implementation of duties segregation (SOD) strategies on privileged and non-privileged accounts.
- Modularizing privileged accounts abortions based on player separation or termination incidents as per the active directory solution.
- Excludes the doubt as to who is permitted to receive privileged or restricted information.
- We've developed better security on both the outside and inside of the organization.
- The efficiencies created by autonomous systems reduce costs, freeing companies to focus on building and protecting their networks.
- To stop the breach from happening, implement a process to avoid hackers from breaking in will save both time and money.
- Enforcing new and existing security policies with the system for the easiness.

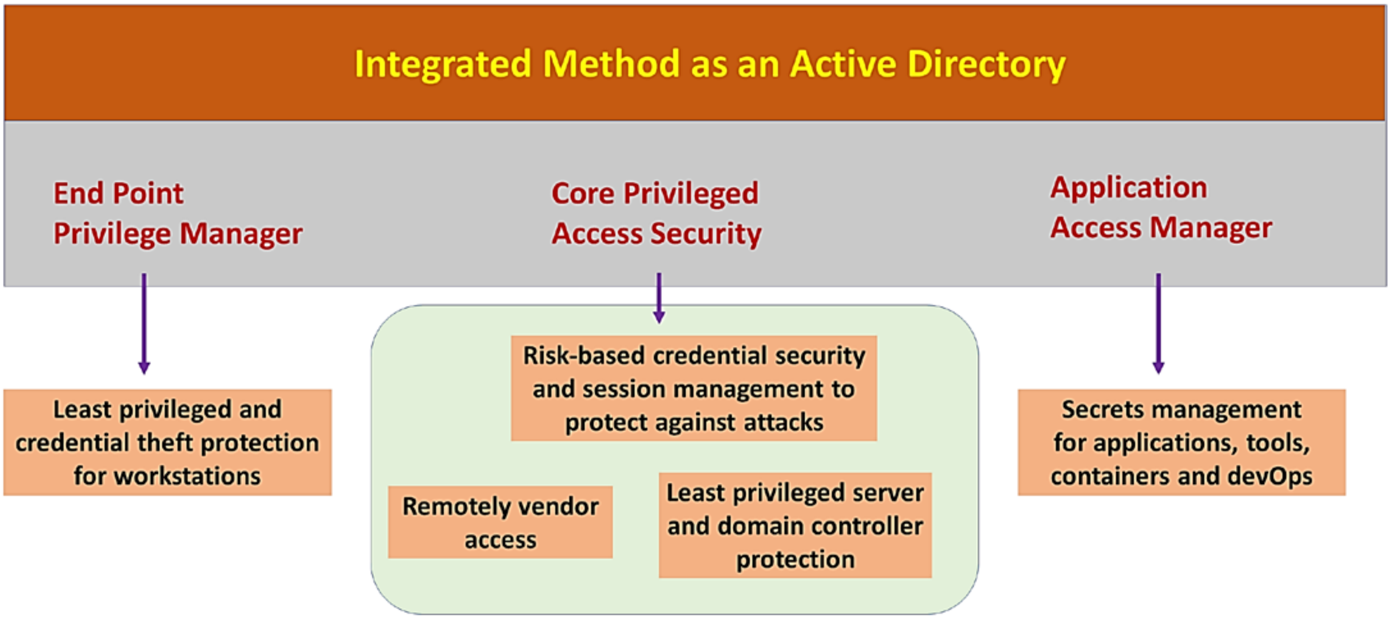
Integrated Method as an Active Directory
End Point Privilege Manager
Core Privileged Access Security
Application Access Manager
Least privileged and credential theft protection for workstations
Risk-based credential security and session management to protect against attacks
Remotely vendor access
Least privileged server and domain controller protection
Secrets management for applications, tools, containers and devOps

Fig. 4. Outcomes of Applied Integrated Mechanism.

B. Limitation of the Integrated Methods

Protecting identity and restricting access control is the key reason for using an integrated method. The system is controlled by only passwords. This is to say that the employee access code is only has some value when they have the ability to affect it. Regardless of the size of the enterprise, installing and configuring an integrated method can be expensive and time-consuming. For security purposes, it needs to be incorporated with the current security systems. To the extent possible, many enterprises are depending on IT security experts to develop and enforce the relatively better framework such as two factor or three factor authentications to eliminate interruptions for staff and company operations.

V. Conclusion

The emergence of the technological advancement around the world a well-organized governmental as well as business oriented smart control measure focuses within the organization. The emphasis of these highly required concept, this article is proposed an integrated approach with the incorporation of IAM as an authentication tool and PAM as a restricting accessing control measure. This method is enhanced the secure accessing policies among the governance as well as business organization to know each activity and record the adversarial attack from the proposed system. The whole experimental setup implemented within the Prince Sattam Bin Abdulaziz University, Saudi Arabia and it is analyzed using the real-time data which is available within the university database. We found that the proposed mechanism can be a vital method for protecting governance data or key business-oriented data from the unauthorized or adversarial attack which is always a challenging task in any premier organization. Using this integrated method, we believe that there will be so many controls within the governance body or business companies which can help a lot to restrict any miss happening being a large company. This article is just an initiative towards the better digitized system in terms of cyber security to employ at public as well as private corporate system to enrich trusted ecosystem for the people of kingdom of Saudi Arabia.

For the future work, we are still thinking to incorporate some cryptographic based strong authentication setup and integrate with effective privilege access control measure which can give highly trusted and relatively better outcomes for the governance system or business-oriented institutions.

Acknowledgment

We thank the Deanship of Scientific Research, Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia for help and support.

References

[1] Y. Zhang, R. H. Deng, G. Han, and D. Zheng, “Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things,” J. Netw. Comput. Appl., vol. 123, pp. 89–100, Dec. 2018.

[2] L. Malina, P. Dzurenda, J. Hajny, and Z. Martinasek, “Secure and efficient two-factor zero-knowledge authentication solution for access control systems,” Comput. Secur., vol. 77, pp. 500–513, Aug. 2018.

[3] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, “BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0,” J. Netw. Comput. Appl., vol. 116, pp. 42–52, Aug. 2018.

[4] A. Sharma, S. B. Borah, and A. C. Moses, “Responses to COVID-19: The role of governance, healthcare infrastructure, and learning from past pandemics,” J. Bus. Res., vol. 122, pp. 597–607, Jan. 2021.

[5] U. Iqbal and A. H. Mir, “Secure and scalable access control protocol for IoT environment,” Internet of Things, vol. 12, p. 100291, Dec. 2020.

[6] Y. Inoue, “Indirect innovation management by platform ecosystem governance and positioning: Toward collective ambidexterity in the ecosystems,” Technol. Forecast. Soc. Change, vol. 166, p. 120652, May 2021.

[7] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, “Data governance: Organizing data for trustworthy Artificial Intelligence,” Gov. Inf. Q., vol. 37, no. 3, p. 101493, Jul. 2020.

[8] P. Ashley, M. Vandenwauver, and F. Siebenlist, “Applying authorization to intranets: architectures, issues and APIs,” Comput. Commun., vol. 23, no. 17, pp. 1613–1620, Nov. 2000.

[9] J. Khan, H. Abbas, and J. Al-Muhtadi, “Survey on Mobile User’s Data Privacy Threats and Defense Mechanisms,” Procedia Comput. Sci., vol. 56, pp. 376–383, 2015.

[10] J. Khan et al., “Efficient secure surveillance on smart healthcare IoT system through cosine-transform encryption,” J. Intell. Fuzzy Syst., vol. 40, no. 1, pp. 1417–1442, Jan. 2021.

[11] J. Khan et al., “SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System With Probabilistic Image Encryption,” IEEE Access, vol. 8, pp. 15747–15767, 2020.

[12] P. White, “Identity Management Architecture: A new direction,” in 2008 8th IEEE International Conference on Computer and Information Technology, 2008, pp. 408–413.

[13] I. Indu, P. M. R. Anand, and V. Bhaskar, “Identity and access management in cloud environment: Mechanisms and challenges,” Eng. Sci. Technol. an Int. J., vol. 21, no. 4, pp. 574–588, 2018.

[14] I. Indu and P. M. Rubesh Anand, “Identity and access management for cloud web services,” in 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), 2015, pp. 406–410.

[15] P. M. Rubesh Anand and V. Bhaskar, “A unified trust management strategy for content sharing in Peer-to-Peer networks,” Appl. Math. Model., vol. 37, no. 4, pp. 1992–2007, Feb. 2013.

[16] S. Parveen, S. Yunfei, J. P. Li, J. Khan, A. U. Haq, and S. Ruinan, “E-waste Generation and Awareness on Managing Disposal Practices at Delhi National Capital Region in India,” in 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2019, pp. 109–113.

[17] Z. Wang, D. Huang, Y. Zhu, B. Li, and C.-J. Chung, “Efficient Attribute-Based Comparable Data Access Control,” IEEE Trans. Comput., vol. 64, no. 12, pp. 3430–3443, Dec. 2015.

[18] Z. Yan, M. Wang, Y. Li, and A. V. Vasilakos, “Encrypted Data Management with Deduplication in Cloud Computing,” IEEE Cloud Comput., vol. 3, no. 2, pp. 28–35, Mar. 2016.

[19] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, “Securely Outsourcing Attribute-Based Encryption with Checkability,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2014.

[20] J. Khan et al., “An Authentication Technique Based on Oauth 2.0 Protocol for Internet of Things (IoT) Network,” in 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2018, pp. 160–165.

[21] J. Khan et al., “Medical Image Encryption Into Smart Healthcare IOT System,” in 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2019, pp. 378–382.

[22] Q. Liu, G. Wang, and J. Wu, “Secure and privacy preserving keyword searching for cloud storage services,” J. Netw. Comput. Appl., vol. 35, no. 3, pp. 927–933, May 2012.

[23] A. Bhardwaj and V. Kumar, “Identity Management Services in the Present IT Era,” IPASJ Int. J. Inf. Technol., vol. 6, no. 4, pp. 6–11, 2018.

[24] L. Wu, S. Zhou, Z. Zhou, Z. Hong, and K. Huang, “A Reputation-Based Identity Management Model for Cloud Computing,” Math. Probl. Eng., vol. 2015, pp. 1–15, 2015.

[25] M. Q. Huda, M. C. Utami, N. A. Hidayah, and Q. Aini, “Effective IT Governance in Higher Education Institutions: The Conceptual Model,” vol. 149, no. Icosat 2017, pp. 148–151, 2018.

[26] G. Karopoulos, G. Kambourakis, S. Gritzalis, and E. Konstantinou, “A framework for identity privacy in SIP,” J. Netw. Comput. Appl., vol. 33, no. 1, pp. 16–28, Jan. 2010.

[27] P. Pradhan and V. Kumar, “Trust Management Models for Digital Identities,” Int. J. Virtual Communities Soc. Netw., vol. 8, no. 4, pp. 1–24, Oct. 2016.

[28] K. Rindell, S. Hyrynsalmi, and V. Leppanen, “Case Study of Security Development in an Agile Environment: Building Identity Management for a Government Agency,” in 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 556–563.

[29] S. Jacobsson, P. O. Arnäs, and G. Stefansson, “Automatic information exchange between interoperable information systems: Potential improvement of access management in a seaport terminal,” Res. Transp. Bus. Manag., vol. 35, p. 100429, Jun. 2020.

[30] M. umar Aftab, Z. Qin, Zakria, S. Ali, Pirah, and J. Khan, “The Evaluation and Comparative Analysis of Role Based Access Control and Attribute Based Access Control Model,” in 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2018, pp. 35–39.

[31] M. U. Aftab et al., “Negative Authorization by Implementing Negative Attributes in Attribute-Based Access Control Model for Internet of Medical Things,” in 2019 15th International Conference on Semantics, Knowledge and Grids (SKG), 2019, pp. 167–174.