ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

How AI can Improve Identity Verification and Access Control Processes

Srikanth Mandru

USA

ABSTRACT

Artificial intelligence (AI) is recognized as the driving force responsible for reinventing a wide range of industries, among them IAM. This paper, therefore, looks for the potential for advancement in AI systems with respect to IAM, focusing on identity verification and access control within IAM systems. IAM systems face really difficult problems nowadays: management of user identity, real-time access control, and protection from modern threats. Traditional approaches have proven to be inefficient worldwide because of the static nature of the approaches and the lack of human intervention. In this way, this work provides a discussion on how these IAM challenges are to be effectively managed with the application of AI technologies. AI empowers strong tools of advanced data analytics, machine learning mechanisms, and automation. Equipped with all these capabilities, IAM systems can monitor user activity and behavior continuously, identify emerging anomalies in real time, and dynamically enforce policies to greatly enhance security and efficiency. Research has shown that AI brings better results in terms of security and productivity and offers scalable solutions in light of current and future needs for identity management. AI integration can streamline the process of verification of identity, offer mechanisms of authentication that are enhanced, and deliver precise and dynamic access control methods. Meanwhile, resonant incorporation of AI in IAM definitively gives the systems the ability to learn and change and to learn firm protection along with operational resilience against threats that constantly change over time. In this light, IAM systems based on AI will be able to properly satisfy the growing demands of modern organizations in terms of proper security, optimum performance, and user satisfaction.

***Corresponding author**
Srikanth Mandru, USA.

Received: November 04, 2022; **Accepted:** November 15, 2022; **Published:** November 20, 2022

Keywords: Artificial Intelligence, Identity and Access Management, Identity Verification, Access Control, Security, Machine Learning, Biometrics, Cybersecurity.

Introduction

In a relatively short time, technological developments have led companies to re-look at how to manage access to systems and data. This change is significant because IAM determines who in the organization can access what resources, thus protecting the network and its systems against unauthorized access. Traditional means, characterized by static rules and manual processes, are proving ineffective in dealing with evolving cyber threats. AI is a promising solution, harnessing its capability in big data analytics, pattern recognition, and intelligent decision-making. The problems associated with the traditional IAM in terms of scalability and rapid response problems call for the new ways. This paper tends to explore the aspect, in detail focusing on how AI will tackle such problems through adaptive learning and advance analysis methods. Further, tacking AI in IAM gives rise to important consideration of privacy, legal compliance, and ethical practices. It is against this backdrop that the paper finds it crucial to examine the implications that can be derived from the practice so that AI-driven IAM systems traverse these complexities in consonance with both security and ethical integrity in the processes of identity verification and access control. In this light, AI is best viewed as a two-edged sword—full of transforming potential for IAM, while at the same time demanding careful, responsible use.

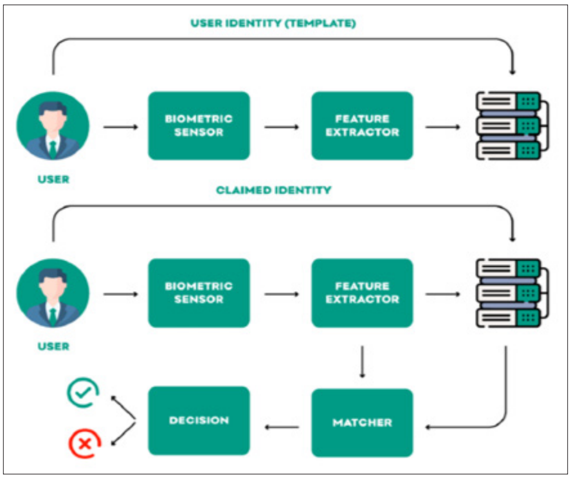
Problem Statement

Traditional IAM systems are based on traditional credential methods, which are passwords and simple verification processes, viewed as mediocre at their best. IAM systems based on these methods become highly vulnerable to hacking, identity theft, and human errors famously called 'blonde moments' colloquially. The many vulnerabilities identified with these systems carry with them portentous flaws in the current security architectures. In fact, it is a given that these systems will fail to provide the much-needed safeguarding during the threat scenarios of emerging and evolving. Another serious predicament that plagues the traditional IAM is the issue of scalability. As an organization grows, over time, more and more user identities are managed, and the number of entry points becomes greater. It is becoming imperative to support SSO across platforms and devices, which leads to cumbersome and less efficient IAM processes. Organizations are finding it difficult to balance usability with strong security measures and most often shift focus from one to the other. The shortcomings brought about by the issues of the traditional IAM models clearly underline the need to adopt new flexible and innovative approaches. Advanced solutions such as those integrating artificial intelligence offer the possibility of more robust and changeable IAM. AI can provide security through constant monitoring and adaptability in real-time with the change in threats. Second, the AI-based IAM systems are better in the sense that these streamlined processes provide an enhanced user experience and offer ready-to-deploy scalable solutions that are capable of growing with the organization. Transitioning to these more advanced IAM approaches is thus support for a proactive response to the ever-changing threat landscape while being able to execute secure and efficient IAM.

Solution

Identity Verification

AI increases the efficiency of biometric authentication systems by increasing the speed, accuracy, and effectiveness of fingerprint, facial, voice, and iris recognition. Despite the efficiency of such systems in personal identification, traditional biometric systems have some problems concerning high accuracy under different circumstances and counteraction to other types of spoofing [1,2]. AI solves these issues through machine-learning techniques, which can process intricate biometric signals and differentiate between small changes and variations that manual methods might discount; for example, AI can enhance facial recognition accuracy due to lighting changes, angles, and facial expressions. Likewise, AI can improve the discriminability between real and fake inputs regarding minutiae points and complex fingerprint and iris recognition patterns. Another advantage of using AI is its ability to learn different accents, tones, or impediments in the speaker's voice, thus offering even more reliable identification [3]. AI-based biometric systems generally provide efficient and complex identity recognition, increasing security and convenience by lessening false positive and negative rates and making it difficult for intruders to circumvent security protocols.



Biometric enrollment and verification. The enrollment phase produces an association between a biometric characteristic and its identity. In the verification phase, an enrolled user claims an identity, which the system verifies on the basis of the user's biometric feature set [4].

AI helps identity verification enhance behavioural analysis by tracking user patterns like typing speed, mouse dynamics, and usage history. Compared to the conventional credentials prone to attacks, behavioral biometrics offers an ever-changing and constantly updating approach to security. Machine learning algorithms are instrumental in this process as they generate individual behavioral patterns for every user [5]. For instance, an AI system can learn how a user types, such as the speed, rhythm, and pressure of keys. It can also monitor the movement of the mouse, its movement pattern, and the intervals between each click made by the user. These traits create a package over time that a pretender or an imposter cannot easily imitate. Whenever a user tries to get into a system, the AI checks the current behavior against the stored profile to determine the user's identity. This continuous authentication method guarantees that even if the user's static credentials are disclosed, access should not be granted to unauthorized persons [6]. Behavioral analysis improves the protection and is user-friendly since the process takes place behind the scenes without additional actions from the user.

Technologies such as OCR and NLP have enhanced the effectiveness and reliability of document validation procedures through machine learning algorithms. Conventional techniques of verifying documents like passports, driver's licenses, and utility bills have always been manual, thus they are prone to human errors and fraud triggers [7]. This process is also accelerated through OCR technology, which is AI-driven and is capable of converting every piece of text from scanned documents, either in a different language or in a different format. Since this step is automated, the verification process is hastened, and the chances of errors arising from interference are greatly minimized. AI also utilizes natural language processing to understand and analyze obtained information, thereby ascertaining the fact that the content is real and meets required standards. Artificial intelligence can, for instance, help in, therefore, enabling one to know whether a document is forged and where there are disparities. This way, by automation of the verification process for documents, AI not only increases the efficiency and reliability of the verification process but decreases the demand on time and operating resources for verification purposes as well [8]. Particularly, such technology is more beneficial in domains such as finance, healthcare, or government services, where prompt verification of documents is of crucial importance with respect to compliance and safety.

Access Control

AI fits into a security strategy through adaptive authentication implementations. These mechanisms change the security controls depending on the context of the access request and the associated risk. This approach, called second-factor authentication, consists of MFA and contextual authentication and considers features such as geographical location, device type, and user activity [9]. It also uses the dynamics of authentication requirements, thus increasing the application's security level while still delivering a desirable user experience. It provides an optimal security level by minimizing the probability of unauthorized access while maintaining the corresponding usability levels to the lowest possible minimum.

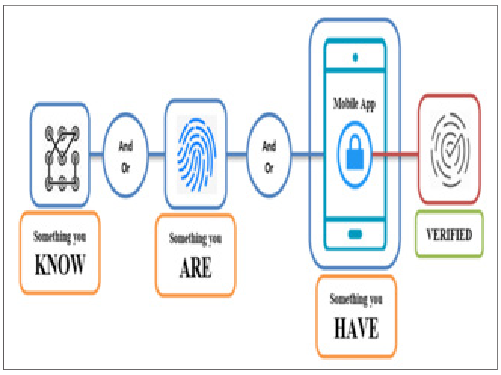
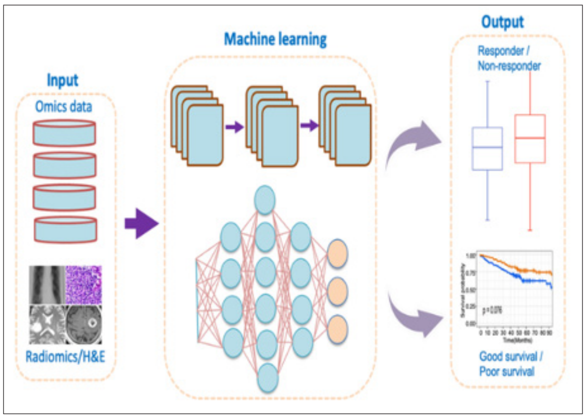


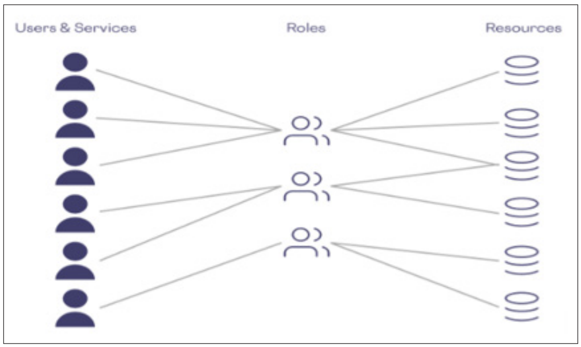
Figure 2: Multi-factor authentication.," ResearchGate, 2020 [9].

AI-based machine learning models can effectively enable the routine analysis of access patterns for the observation of early signs of an intrusion or even a potential security breach. This proactive approach analyses the user's behavior in real-time and looks for significant changes compared to the baseline. This is particularly important in case of anomalies when the actions that the system suggests can include alerts or immediate responses to the noted risks [10]. It also ensures a continuous and dynamic approach to analyzing threats, strengthening an organization's capacity to counter suspicious activities and mitigate security threats before they escalate.



Artificial intelligence-based machine learning model for predicting CAR-T cell therapy outcome [11].

AI can enhance role-based access control (RBAC) and attribute-based access control (ABAC), where an AI tool can study users' roles, attributes, and access behavior patterns to assign correct rights. Through AI, an organization can automate its capability to change a team member's access level depending on variables and data received at any given time. This ensures that users on the system have the right level of privilege to perform required tasks without having privileged access that can be misused, leading to insecure compromises. RBAC and ABAC systems based on artificial intelligence contribute to the more efficient security of an organization as they contain automated and accurate access control mechanisms that are more appropriate to suit users' behaviors within an organization.



“RBAC vs ABAC: Access Control for Sensitive Data - Skyflow,” www.google.com, 2021 [12].

Uses

Artificial intelligence makes a contribution to identity and access management (IAM) in the realm of business security by enhancing the access rights of employees, safeguarding vital corporate information, and avoiding hostile activities by employees within the organization [13]. Traditional techniques of identity and access management (IAM) are troublesome because they include static credentials and conventional methodologies that need human labor. Artificial intelligence (AI) solutions take advantage of behavioral biometrics, anomaly detection, and machine learning to perform real-time monitoring of users' activities. These solutions are both current and versatile. Besides, they allow the identification and prevention of risks as they pop up, hence increasing the level of unwanted access and data loss. AI therefore improves security and amplifies operational effectiveness, as companies no longer need to spend much time on tactical considerations. An example is the use of automated processes in identification and authorization. Thus, AI use in corporate security ultimately establishes a robust and highly flexible defense to new cybercrimes, which are popping up almost daily.

AI plays a crucial role in transforming IAM in financial services by protecting consumer transactions, preventing fraud, and adhering to regulatory requirements. The other security challenge that they have to brace for is consumer information protection and their systems' integrity maintenance. Other security improvements from AI-powered identity and access management solutions include Utilizing improved authentication technologies such as biometric, behavioral, and real-time analysis of transactional activities [14]. As a financial transaction safety net, they help identify and avert fraud in real-time. Moreover, AI may also help to smoothen compliance procedures by integrating identification verification and tracking of regulatory updates. This will enhance compliance with the highest standards for the involved financial institutions. With AI, the financial services industry can enhance the safety and efficiency of IAM positively affecting trust from the clients.

AI quickly elevates IAM for healthcare by securing patient data, keeping in line with healthcare regulations, and providing authentic access to medical information, but security, in the realm of patient information because of privacy, has to be increased; hence, traditional IAM is generally not competent enough to fulfill requirements. To ensure that patient information is accessed by only the concerned and privileged ones, AI-powered solutions have implemented advanced measures that map to identity and location. Built-in machine learning engines keep an eye over user activities and their access patterns and try to pinpoint potential security threats. By taking this proactive approach, organizations prevent undesirable access and unwanted data breaches, which makes it quite easy to protect patient information. In fact, compliance activities can also be conducted through AI, by which health firms maintain compliance with strict regulations. Moving in this realm of identity and access management by harnessing the service of artificial intelligence integration can therefore enable the healthcare industry to maintain data security, access control, and elevate the general confidence of, and security to, the patients.

By using IAM, artificial intelligence is reshaping how the e-commerce industry continues to protect customers' details, prevent unwanted account takeovers, and ensure a safe transaction. As one of the industries that has seen massive growth in recent years, the e-commerce platforms are under ferocious pressure from hackers looking for possible ways to gain customer data and breach their accounts. Among many security components that are built with the help of artificial intelligence in determining the IAM solutions include the use of biometrics and behavior analysis in authenticating an individual's account. This makes sure that only the right individuals can get into their accounts from the right places.

Impact

AI implementation in IAM dramatically enhances the level of protection with a particular focus on unauthorized access and data leakage. Early IAM systems require static credentials and may involve a lot of paperwork; they are prone to many cyber risks [15]. AI-based IAM solutions address advanced technologies like machine learning, biometrics and behavioural analysis to deliver progressive and intelligent authentications. These technologies always observe the users' activities, identify suspicious events, and address security threats in real time. Through AI, an organization can design security measures that mitigate the rising threat of cybercrime by denying unauthorized access to such information. It safeguards essential data and increases the organization's IT security system's defence mechanism against all sorts of illicit activities.

Implementing AI in IAM results in a marked enhancement of the organization's performance since identity proofing and authorization are automated. Many traditional approaches can be time-consuming and cumbersome, involving significant human intervention [16]. AI solutions facilitate these tasks by using automated processes and intelligent algorithms that decrease the need for manual operation. This automation increases the speed of identity verification while increasing efficiency and reducing the likelihood of fraud and mistakes. In addition, AI can easily handle innumerable requests for access, authentication, and authorization at the same time. The execution allows an organization to achieve extremely high productivity with minimal resources, since it will free personnel who could attend to more sensitive duties other than administrative work. In better-managed IAM enhanced by employing AI, the results are better in the management of resources and higher overall performance.

AI-driven IAM solutions offer unique privileges in the provision of solutions for businesses in handling a large number of users and devices. This is an addition to the overall scalability as the AI-powered IAM solution is specially developed so that it can be scalable, meeting the developing needs of the enterprise without harm to productivity or security. The system performs well in handling the addition of new users, devices, and applications effectively to ensure a seamless integration. Additionally, AI algorithms learn and adapt with time, meaning they will meet the growth of the IAM system with the growth of the organization. This kind of scalability is important for having strong security and productive continuous operation in changing environments. AI allows the organization to be flexible in its IAM solutions in anticipation of future developments.

Moreover, the use of AI in IAM positively affects the user experience because it accelerates access procedures and retains the high security of information while doing this. Traditional IAM solutions often have slow-going authentication procedures that may irritate users. AI-driven solutions provide more convenient and intuitive authentication mechanisms, such as biometric access and adaptive authentication, which results in a user-friendly and smooth experience. AI can easily improve the user experience through making access control more flexible and user-tailored, based on the behavior and preferences of users. This will reduce friction in the authentication process and again increase customer satisfaction and efficiency. All in all, AI-driven IAM solutions maintain a high level of security, ensuring that the data of the users will remain secure. By the use of AI in IAM, a balance of security and ease of use will be gained, providing the best experience for the user.

Scope

With AI integration in IAM, the blooming biometrics technology would have many applications. Integration of AI in biometric systems such as fingerprinting, facial recognition, voice, and iris recognition will definitely enhance the accuracy and reliability. These advancements will lessen the unabsorbed access and make the verification of identification a lot safer and efficient. Furthermore, AI skills allow biometric systems to adapt to the varying situations associated with such changes in facial features [17]. AI also has the ability to scour biometric data in a wider sense and might pick some subtle detail that is otherwise missed by traditional ways. AI integration with these biometric technologies will be some major steps in developing secure and user-friendly systems for authentication. The enhancement in the level of security with the performance of businesses would be incredible with AI integration.

As for IAM, AI-assisted zero-trust security frameworks are one of the most significant future developments. The zero trust architecture applies the general principle that no user or system, internal or external to a network, can be trusted at face value. This paradigm is enhanced by the use of artificial intelligence to constantly verify each access request, analyze behavioral patterns and detect suspicious behaviors as they occur. Using artificial intelligence, this technique helps determine and respond to suspicious activity, thereby limiting the threat of insiders and unauthorized entry. In this way, through Artificial Intelligence, organizations are able to ensure that the access to their networks is highly secured and all users and devices are well authenticated and authorized at every touch point. Artificial intelligence not only increases security measures within the zero-trust model but also generates a flexible model that is able to adjust according to threats and the needs of the company.

In the future, IAM may decentralize identity systems, and artificial intelligence could be needed to handle such systems. The one advantage of decentralized identity is that the user may have even greater control over their personal information, which then tends to enhance privacy and security. With the use of artificial intelligence, this switch can be made more comfortable by securely managing and verifying decentralized credentials to ensure identity data is correct and up-to-date [18]. Artificial intelligence will help the business to verify individuals without any need for centralized databases, so at a large scale, hacks are not possible. Moreover, artificial intelligence may make issuance and revocation of credentials efficient and decentralized identity systems more valuable and convenient for users. With the increasing awareness about privacy issues and data protection, decentralized identity enhanced with artificial intelligence will have a more critical role than it has today. Such solutions will be promising and given more focus than traditional identity and access management systems.

Certain standards of ethical and responsible application of artificial intelligence in IAM should be issued to manage the issue of privacy and reduce bias from AI programs. The use of AI should be transparent and applied fairly with increased AI use in IAM systems; certain governance structuring sets policies and standards on the development and application of AI in IAM. This guarantees the adherence to ethical values and legal requirements that would otherwise cause Grave. These include accountability and liability, discrimination in algorithms, and data privacy, among other things. Management can assure consumers and other stakeholders that the governance of AI is appropriate for the demonstration of responsibility in the practice of AI. This way, it makes the IAM system secure and effective and, at the same time, the digital space ethical and inclusive for all.

Conclusion

AI is set to transform the way IAM procedures are performed within the business environment. One of the key features of AI is its ability to deal with existing security concerns, improve operational performance, and solve issues with requirements for the future. AI makes IAM systems more robust and efficient by refining identification checks, security measures, and systems of control. Introducing AI in IAM will consolidate security in such a way that the procedures remain not only safe for organizations and clients but also affect the flow of procedures and user experience positively. AI will speed up and make the entire identity verification process more accurate, thus taking the burden off the IT staff and increasing the overall productivity. For instance, AI-driven systems are able to make quick analyses and verify different types of biometric data, such as fingerprints, facial recognition, voice patterns, and iris scans, performing a seamless and secure experience.

Further, learning and adapting with each experience, AI and IAM become foolproof. Such adaptability is vital for the design and construction of frameworks that will facilitate and resist IP-based, targeted, and complex cyberattacks, as well as dynamic IT environments. AI, as a technology, is growing in leaps and bounds with each day, which will make sure that applying AI in IAM provides a more secure and efficient user-friendly system. The future development of AI in IAM is designed to cater to the challenges of scalability, user convenience, and security. Organizations should expect better ways of managing identity and access controls in an environment that is more secure and operationally efficient. In other words, the role of AI in IAM is going to overhaul security practices, streamline operations, and enhance user satisfaction.

References

1. Ng Alex Chi Keung (2018) ed. "Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities: Emerging Research and Opportunities.". https://books.google.co.ke/books?hl=en&lr=&id=ipBFDwAAQBAJ&oi=fnd&pg=PR1&dq=Contemporary+Identity+and+Access+Management+Architectures:+Emerging+Research+and+Opportunities:+Emerging+Research+and+Opportunities&ots=04HYyTw2wI&sig=T8glvfCusbuh-hSdSGetS1X8ryQ&redir_esc=y#v=onepage&q=Contemporary%20Identity%20and%20Access%20Management%20Architectures%3A%20Emerging%20Research%20and%20Opportunities%3A%20Emerging%20Research%20and%20Opportunities&f=false.
2. Jain Anil K., Karthi Nandakumar, Arun Ross (2016) "50 years of biometric research: Accomplishments, challenges, and opportunities." Pattern Recognition Letters 79: 80-105.
3. Abdullah H, Warren K, Bindschaedler V, Papernot, Traynor P (2021) Sok: The faults in our answers: An overview of attacks against automatic speech recognition and speaker identification systems. In 2021 IEEE symposium on security and privacy (SP) IEEE 730-747.
4. Barbara M, Wojciech W, Anna Katarzyna Biometric enrollment and verification. https://www.researchgate.net/figure/Biometric-enrollment-and-verification-The-enrollment-phase-produces-an-association_fig2_362412868.
5. Balaji TK, Chandra Sekhara Rao Annavarapu, Annushree Bablani (2021) "Machine learning algorithms for social media analysis: A survey." Computer Science Review 40: 100395.
6. Al-Naji, Fatimah Hussain, Rachid Zagrouba (2020) "A survey on continuous authentication methods in Internet of Things environment." Computer Communications 163: 109-133.
7. Anand Nishant (2021) "New principles for governing Aadhaar: Improving access and inclusion, privacy, security, and identity management." Journal of Science Policy & Governance 18: 1-14.
8. Javaid Mohd, Abid Haleem, Ravi Pratap Singh, Rajiv Suman (2021) "Substantial capabilities of robotics in enhancing industry 4.0 implementation." Cognitive Robotics 1: 58-75.
9. Wu Hui, Haiting Han, Xiao Wang, Shengli Sun (2020) "Research on artificial intelligence enhancing internet of things security: A survey." Ieee Access 8: 153826-153848.
10. Alzahraa M, Ali adil Yassin (2020) “Figure 2. Multi-factor authentication.,” ResearchGate. https://www.researchgate.net/figure/Multi-factor-authentication_fig2_335709093.
11. Gunjan D, Ashna G, Tariq M, Sabah N (2019) Artificial intelligence-based machine learning model for predicting CAR-T cell therapy outcome. https://www.researchgate.net/figure/Artificial-intelligence-based-machine-learning-model-for-predicting-CAR-T-cell-therapy_fig3_372193225.
12. (2021) “RBAC vs ABAC: Access Control for Sensitive Data - Skyflow,” www.google.com, https://images.app.goo.gl/6gdZitK8QPiYGWcv9.
13. Haber Morey J, Darran Rolls (2019) Identity attack vectors: implementing an effective identity and access management solution. Apress, https://books.google.co.ke/books?hl=en&lr=&id=zfrEDwAAQBAJ&oi=fnd&pg=PR5&dq=Identity+attack+vectors:+implementing+an+effective+identity+and+access+management+solution&ots=4Zn5BR6VSD&sig=WVIj-JPbmpEtO4Qbhp8i0-ciZCA&redir_esc=y#v=onepage&q=Identity%20attack%20vectors%3A%20implementing%20an%20effective%20identity%20and%20access%20management%20solution&f=false.
14. Konstantinidis Giannis (2021) "Identity and access management for e-government services in the European Union–state of the art review." https://hellanicus.lib.aegean.gr/handle/11610/23968.
15. U Cali, Murat Kuzlu, Manisa Pipattanasomporn, J Kempf, L Bai (2021) “Introduction to Security for Smart Grid Systems,” Springer eBooks 59-85.
16. Azhar Ishaq (2018) "A literature review on the application of AI to Identity Access Management." Ishaq Azhar Mohammed," A literature review on the application of AI to Identity Access Management", International Journal of Emerging Technologies and Innovative Research (www. Jeter.org| UGC and ISSN Approved), ISSN: 2349-5162.
17. Razzano Gabriella (2021) "AI4D-Digital and Biometric Identity Systems." Research ICT Africa https://researchictafrica.net/wp/wp-content/uploads/2021/07/Final-Consolidated-Bio-ID-Thematic-Report.pdf.
18. Pöhn Daniela, Michael Grabatin, Wolfgang Hommel (2021) "eID and self-sovereign identity usage: an overview." Electronics 10: 2811.

Copyright: ©2022 Srikanth Mandru. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.