International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Artificial Intelligence Based Anomaly Detection for Secure E-Government Transaction: A Review

[1]Muskan Sharma, [2]Dr. P. K. Sharma

[1,2]Department of Computer Science Engineering

[1,2]NRI Institute of Research and Technology, Bhopal (M.P.) -462021

ABSTRACT

The high pace of e-government platforms has revolutionized the way of delivering public services because it has facilitated massive online transactions in authentication, finance, welfare disbursement, land management, and citizen-government interfaces. The growing reliance on digital governance has however demonstrated vulnerability of systems to advanced cyber threats such as data manipulation, identity fraud, access without authorization, malware infiltration and huge-scale coordinated attacks that are beyond the ability of traditional rule based security mechanisms to manage. The present review article explores why the use of Artificial Intelligence (AI)-based anomaly detection is critical in increasing the security, reliability, and resilience of e-government transactions. Through examination of advanced machine learning and deep learning frameworks, including LSTM, autoencoders, graph neural networks, and unsupervised clustering models, the researcher can point out that AI systems are able to learn a behavioral pattern, identify anomalies in real-time, and detect threats pretending to be unknown or zero-day threats with high levels of precision. The literature also indicates that there are new frameworks in the emerging of combining blockchain and artificial immune system, federated learning and hybrid cloud and edge architecture to enhance data integrity and privacy. The results indicate that AI-based anomaly detection offers a scalable, adaptive, and proactive protection mechanism that is necessary in the protection of the modern e-government ecosystems. The paper ends by arguing why ongoing innovation and cross-functional integration are necessary towards developing safe, reliable, and future intensive digital governance structures.

Keywords: Artificial Intelligence, Anomaly Detection, E-Government Security, Cybersecurity, Machine Learning

1. INTRODUCTION

The quick digitalization of the systems of public governance in the world has catapulted the e-government platforms to the center of the modernization of the administrative system, and with the online system, the citizens, businesses and government agencies can communicate effectively through online channels.[1] The volume, speed, and sophistication of electronic transactions have been increasing exponentially as more countries are implementing electronic interfaces to deliver the most basic services including identity verification, taxation, welfare transfer, land registration, online payments, and redressing of grievances. Though this digital transformation makes e-government services more accessible, transparent, and efficient, it leaves the e-government infrastructures vulnerable to an expanding range of cyber threats, data manipulations, financial frauds, unauthorized access, identity theft, and failure of services.[2] Conventional security measures that followed a rule-based and manual auditing system are no longer enough to protect such large and dynamic environments due to advanced attackers that are continuously advancing their methods to avoid predisposed rules. Artificial intelligence (AI) is presented in this respect as a new force that can analyze large amounts of data, be trained to behave in certain ways, identify subtle anomalies, and react to any new threat promptly.[3] AI-powered anomaly detection, specifically, is a paradigm shift in digital security since it does not rely on some fixed signature, or past occurrence of attacks, but instead, it continuously learns about the normal behavior of transactions and detects anomalies that can be signs of fraud, intrusion, or attack on the system. The intelligence of AI-driven anomaly detection is indispensable in securing the most vital e-government systems, where millions of sensitive user interactions are made on a daily basis, due to its adaptability, scalability, and predictive power.[4]

The explosion in the uptake of e-government has accelerated cybersecurity issues with malicious parties actively taking advantage of vulnerabilities in digital authentication systems, API, and outdated government databases and the platform of cloud-based services.[5] The need to integrate different modules, including Aadhaar-linked services, e-payment gateways, digital lockers, online municipal services, e-tendering systems, and e-courts require a well-built security architecture that will be able to identify irregular patterns at both granular and system-wide scales.[6] The traditional anomaly models are generally based on rule-sets that are not scalable in dynamic ecosystems where users can behave differently in different regions, service types, time time, and demographics.[7] Alternatively, machine learning (ML), deep learning (DL), natural language processing (NLP), graph-based intelligence, and reinforcement learning methods that are driven by AI have proven to be very useful in identifying anomalies like unusual login behavior, abnormal transaction frequency, access location variations, unusual data-sharing requests and suspicious patterns of communication.[8] These sophisticated models employ statistical learning, pattern recognition, time-series forecasting, clustering analysis and probabilistic reasoning to establish full behavioral baselines and are therefore well able to detect fraud even in the absence of explicit attack signature knowledge.[9]

The significance of anomaly detection in e-government security is further enhanced by the fact that digital services to the population are characterized by very heterogeneous data that can be highly imbalanced, noisy, with missing values, and non-stationary trends.[10] The government dealings include basic OTP-based authentication to very sensitive two or more step operations that involve inter-departmental data transfer, document verification, and money release. Attackers take advantage of these variations by adding fake requests, impersonating authorized users, automated scripts, bot-based attacks, or even time variations to prevent being detected. Conventional approaches to cyberdefense fail to effectively cope with such dynamic environments when it comes to attacks by insiders, compromised accounts, or a multi-vector attack. The AIs-based anomaly detection solves these problems by continually updating the boundaries of decision making, automatically classifying suspicious activities, adjusting to environmental changes, and learning the previous results of the attacks.[11] Deep neural networks (RNN), long short-term memory networks (LSTM), gated recurrent units (GRU), autoencoders, graph neural networks (GNN), and transformer-based models have the ability to learn contextual and temporal dependencies, and thus detect anomalies with high accuracy that cannot be detected by traditional methods. Unsupervised learning methods, e.g., DBSCAN, isolation forests, one-class SVM, self-organizing maps, as well as clustering algorithms, are especially useful in e-government settings where there is a shortage of labeled attack examples or where they are changing.[12]

It is also the growing use of cloud platforms, hybrid data centers, mobile governance applications and multi-device authentication mechanisms which pose a significant increase in the attack surface that is another major concern by e-government systems. Government services have turned into ecosystems consisting of smartphones, biometric devices, IoT-enabled governmental infrastructure, service delivery through GPS, and verification systems based on blockchains.[13] Every interrelated element will be able to bring anomalies or weaknesses that will affect the overall integrity of transactions. With the assistance of AI-based anomaly detection, the end-to-end transactional security can be guaranteed by assessing data on several levels: network traffic, application logs, database access patterns, user-device fingerprinting, real-time biometric authentication, and even environmental indicators like location metadata.[14] Through the correlation of anomalies in these layers, AI models may identify multi-stage attacks that have existed in isolated monitoring systems. Also, current e-governments systems have to implement fraud detection in the online banking, online subsidy, online pension, online land registration, online KYC, and online procurement system. Anomaly detection using Artificial Intelligence increases the confidence of the use of these vital services since suspicious transactions are promptly detected and blocked before incurring massive financial or administrative harm.[15]

In addition to external cyber threats, AI-based anomaly detection is also used to assist governments deal with internal threats such as unauthorized access to data by the employees, abuse of privileges, tampering with the citizen records, deliberate data leakage and mistakes in the automated decision-making systems. The AI models are able to monitor employee behavioral patterns, irregular database queries, unauthorized alterations on records and misaligned outputs of algorithms in automated governance systems.[16] This in-house surveillance system has been critical since the contemporary e-government systems are based on the need to make various agencies cooperate among themselves, each having its own data-sharing standards and access control privileges among its employees. With the ability to detect anomalies across domains, AI systems make institutions more accountable and make sure that confidentiality, integrity, and availability principles are secured in all the digital governance processes.[17]

The issue of cyber-attacks on government systems globally: ransomware, phishing, credential stuffing, identity spoofing, DDoS attacks, API exploitation, and supply-chain attacks are further reasons why AI-driven anomaly detection frameworks are necessary. The vulnerabilities of the e-government platforms in the high-profile security breaches of a number of countries have revealed that national security can be undermined, interrupt service delivery, erode trust amongst the people and the vulnerabilities can lead to significant financial losses.[18] The use of AI-assisted tools to find vulnerabilities, automate attacks, and mount attacks at large scale continue to rise among attackers. Thus, the governments need to implement the equally progressive AI-based defensive systems that will be able to detect the threats proactively, perform predictive analytics, automated reaction to the incidents, as well as make decisions in real-time.[19] The AI-driven anomaly detection system has the potential to drastically decrease the response time in case of cyber-based incident, provide early warnings, detect the anomalies prior to their development, and suggest mitigation measures. This is a strong benefit over traditional security solutions, especially the ability to identify zero-day threats and new attack vectors.[20]

Moreover, it is possible to integrate anomaly detection models into e-government platforms without exposing sensitive citizen data to third parties because of the development of privacy-preserving AI models, including federated learning, homomorphic encryption, differential privacy, and secure multi-party computation.[21] These technologies also make sure that the AI systems can train on distributed datasets, and the AIs need to be very confidential, which is another critical need of the public sector use.[22] A number of nations have begun utilizing hybrid frameworks of edge AI and cloud-based intelligence to enhance the elasticity and responsiveness of anomaly detection models. Edge-based anomaly detection supports real-time processing on edges like biometric scanners, mobile applications, and IoT sensors, reduces edge latency and enhances decision speed and uses large-scale model training and aggregation on clouds.[23]

The AI based anomaly detection can be also used to facilitate the advanced governance processes like fraud analytics in social welfare programs, prediction of trends of tax evasion, detection of irregularities in government procurement, environment compliance monitoring, and surveillance of financial system of the public sector.[24] Combining information across departments, AI systems are able to detect cross-platform trends like redundant applications, ghost beneficiaries, forged documents, suspicious fund transfers, and abnormal timelines of activity by a citizen. Such an ability fosters transparency, reduces corruption, increases accuracy in administration and enhances the implementation of policy.[25]

To recap the discussion, the growing reliance on the digital platforms of governance requires advanced security features that can ensure the security of sensitive transactions of the populace against even more advanced cyber attacks. To provide an efficient solution to this challenge, AI-based anomaly detection integrates predictive modeling, adaptive learning, pattern recognition, and automated threat response to ensure the scale of e-government ecosystems.[26] With the complexity and frequency of the attacks, the application of AI in digital governance systems is necessary to increase the degree of cybersecurity, as well as improve the reliability, public trust, the ability to continue functioning, and the resilience of the nation. Hence, it is important to conduct a thorough analysis of the methods of artificial intelligence-based anomaly detection with the aim of comprehending the current situation in the field, pinpoint technological progress, assess challenges, and see the future prospects of constructing safe, smart, and sustainable e-government systems.[27]

2. Review Of Related Literature

Balamurali, A and Kartheeswari, B (2025)[28] Overview of e-Government E-Government emerged out of need, anticipating the use of electronic technologies by larger enterprises. However, existing frameworks are mostly centralized and vulnerable to data breaches and assaults. This study presents a blockchain-based decentralized e-Government system that incorporates an Artificial Immune System (AIS) to enhance security and privacy. The framework uses the blockchain network's encryptions, transaction validations, and immutability characteristics in addition to its AIS-driven anomaly detection system to defend itself against both internal and external attacks. Using publicly accessible datasets and the Ethereum-based VIBES simulator, we assess the suggested system's performance, confirming that safe e-Government functions are provided.

Alzu, Shadi et al., (2025)[29] Reliable and secure data handling has become essential to successful e-government operations in the digital transformation of public services. A symmetry-driven neural network architecture designed for safe, scalable, and energy-efficient data processing is presented in this paper. To improve robustness and efficiency, the model incorporates symmetrical layouts and weight-sharing. The proposed approach increases processing performance by up to 40% and strengthens adversarial resilience by keeping accuracy decreases below 2.5% under attack scenarios, according to experimental validation on three E-government datasets (95,000–230,000 records). The architecture outperforms baseline neural networks in terms of accuracy (up to 95.1%), security (up to 98% attack protection), and efficiency (up to 1600 records/sec). These findings support the model's suitability for large-scale, real-time e-government systems and provide a workable route toward safe and sustainable digital public administration.

Lakshmi, K et al., (2024)[30] E-governance is now crucial for providing government services, increasing transparency, and encouraging citizen participation in the modern digital age. However, integrating cutting-edge security measures is still difficult, especially when it comes to cloud computing. This study presents the E-GovShield concept, a cutting-edge e-governance architecture that incorporates reliable cloud security technologies to guarantee user privacy, data security, and effective service delivery. With success rates ranging from 94% to 99%, false positive rates under 3%, and quick detection and mitigation timeframes of 1 to 4 seconds, the model successfully counteracts a variety of cyberattacks. With response times of 150 ms, 100 ms, and 200 ms for document submissions, information retrievals, and transaction operations, respectively, under typical circumstances, it can accommodate up to 10,000 concurrent users and exhibits scalability and resilience even in the face of heavy traffic. These findings offer a benchmark for incorporating cutting-edge cloud security measures in digital governance frameworks and other sectors looking to secure their digital infrastructure, while also greatly improving the security and dependability of e-governance systems, promoting increased public trust and regulatory compliance.

Elisa, N O et al., (2023)[31] With the help of advancements in information and communications technology, electronic government (e-Government) systems continuously provide more services to individuals, companies, organizations, and societies by providing new platforms, possibilities, and information. Stricter security and privacy protection measures are frequently required as a consequence of the increasing sensitivity and complexity of the system. Because most of the current e-Government systems are centralized, they have a single point of failure and are susceptible to security and privacy risks. To solve the aforementioned issues, this paper suggests a decentralized e-Government system with integrated threat detection features. Specifically, Blockchain's encryption, validation, and immutable processes provide the privacy and security of the proposed e-Government system. The use of an artificial immune system efficiently protects the integrity of the Blockchain by minimizing the external and internal dangers related to blockchain transactions. The Ethereum Visualisations of Interactive, Blockchain, Extended Simulations (eVIBES simulator) framework was used to test and assess the proposed e-Government system utilizing two publically accessible datasets. The experimental findings demonstrate the effectiveness of the suggested architecture in reducing both external and internal risks to e-Government systems while maintaining data privacy.

Pamisetty, Vamsee (2023)[32] Cloud computing has been extensively used in a variety of fields during the last several years, including business, scientific applications, and e-commerce. Cloud computing is also seen to be a key facilitator of e-Government because of its practicality. However, there haven't been many initiatives in this area. This study offers significant research on the fundamentals of cloud computing and uses them to investigate how cloud computing might be used to advance e-government. The core and fundamental components of six leading industries have been examined, and the findings support the suggested MASC framework. Additionally, it reveals a number of intriguing e-Government trends and identifies the real players that are essential to the creation, maintenance, and expansion of cloud-based e-Government systems.

Asad, Syed et al., (2023)[33] One crucial technology of the Fourth Industrial Revolution (Industry 4.0) is artificial intelligence (AI), which guards computer network systems against viruses, phishing, cyberattacks, damage, and unauthorized access. Through e-Government, AI has the ability to improve the cyber capabilities and security of nation-states, municipal governments, and non-state organizations. Research to date has shown a mixed link between cybersecurity, e-Government, and AI; however, this relationship is thought to be context-specific. Numerous stakeholders with diverse backgrounds and specialties in AI, e-Government, and cybersecurity impact and are influenced by these fields. This research examines the close connection between cybersecurity, e-Government, and AI in order to close this context-specific gap. Additionally, this research looks at how e-Government mediates the link between AI and cybersecurity as well as how stakeholder participation modifies that relationship. PLS-SEM route modeling research findings showed that e-Government has a partly mediating effect between cybersecurity and AI. The link between e-Government and cybersecurity, as well as between AI and e-Government, was found to be moderated by the engagement of stakeholders. Because all stakeholders are interested in a dynamic, transparent, and safe cyberspace while using e-services, it suggests that stakeholder participation is crucial to AI and e-Governance. This report offers useful recommendations for smart city governments looking to improve their cybersecurity protocols.

Al-besher, Abdulaziz and Kumar, Kailash (2022)[34] The suggested study will investigate and improve e-government services for all stakeholders using Internet of Things (IoT) technology powered by artificial intelligence (AI). Additionally, these AI methods will help reduce the danger of cyberattacks. All stakeholders will surely gain from factors influencing the adoption of e-government services, design, development, and implementation activities based on the suggested reference framework.

Al-mushayt, Omar Saeed (2019)[35] In an increasing number of fields, artificial intelligence (AI) has lately improved state-of-the-art outcomes. Nevertheless, there are still a number of obstacles that prevent it from being used in e-government applications, both to enhance e-government systems and citizen-government interactions. In order to automate and streamline e-government services, we examine the issues with e-government systems in this article and provide a framework that makes use of AI technology. In particular, we start by outlining a framework for e-government information resource management. Second, we create a collection of deep learning models with the goal of automating a number of e-government functions. Third, we suggest an intelligent e-government platform design that facilitates the creation and deployment of e-government AI applications. Our main objective is to advance the existing level of e-government services by using reliable AI approaches to save costs, shorten processing times, and increase public happiness.

3. Conclusion

The analysis of the artificial intelligence-assisted anomaly detection in order to ensure safe e-government transactions makes it quite obvious that AI is now an inseparable component of the cybersecurity stance of the contemporary digital-based governance ecosystems. The requirement of smart, response-based and real-time security mechanisms has never been as important as it is today because e-government platforms continue to grow in size, complexity, and interconnectedness; including cloud services, mobile governance apps, IoT-enabled infrastructure, and blockchain-based verification. The old rule-based security systems cannot protect against such swiftly emerging threats as identity spoofing, insider abuse of power, data manipulation, API abuse, bot-based attacks, and a massive orchestrated assault. Models powered by AI such as machine learning, deep learning, graph intelligence and privacy-preserving analytics have transformative properties by learning behavior patterns, detecting deviations, anticipating emergent risks and dynamically responding to unknown attack vectors. The reviewed literature proves that AI-based systems are more effective to identify anomalies, minimize false alarms, increase scalability, and provide security to multiple-layered digital infrastructures than the traditional approaches. In addition, research that discusses the use of blockchain, artificial immune systems, symmetry based neural architectures, and cloud-security models, underline the incremental approach of integrating AI in providing data confidentiality, system integrity, and continuous delivery of public service. Internal security is also an important aspect of AI whereby ongoing monitoring of employee activity, logs, and inter-departmental flows of data is important in enhancing institutional accountability. Federated learning privacy-preserving and hybrid edgecloud design also help to guarantee that data of citizens is not leaked and facilitate large-scale detection of threats. In general, the evidence highlights that AI-based anomaly detection is not an addition to the robust and transparent and reliable e-government systems but a prerequisite. In the wake of emerging cyber threats, countries need to prioritize the implementation of AI-driven security systems to ensure the protection of state resources, retain citizen trust, and create digital governance systems of tomorrow that can manage the pressures of the more interconnected world.

References

1. Drigas A, Koukianakis L. Government online: an e-government platform to improve public administration operations and services delivery to the citizen. InWorld Summit on Knowledge Society 2009 Sep 16 (pp. 523-532). Berlin, Heidelberg: Springer Berlin Heidelberg.
2. Raza A. A Review Of Cybersecurity Threats In E-Government Systems: Towards Secure Digital Governance. Multidisciplinary Research in Computing Information Systems. 2024 Jul 2;4(3):131-42.
3. Azaria A, Richardson A, Kraus S, Subrahmanian VS. Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data. IEEE Transactions on Computational Social Systems. 2015 Jan 15;1(2):135-55.
4. Ogunleye OS. Using Artificial Intelligence to Enhance E-Government Services Delivery Through Data Science and Machine Learning. InMachine Learning and Data Science Techniques for Effective Government Service Delivery 2024 (pp. 1-28). IGI Global Scientific Publishing.
5. Murray A, Begna G, Nwafor E, Blackstone J, Patterson W. Cloud service security & application vulnerability. InSoutheastCon 2015 2015 Apr 9 (pp. 1-8). IEEE.
6. Mohanty S, Prasanna VK, Neema S, Davis J. Rapid design space exploration of heterogeneous embedded systems using symbolic search and multi-granular simulation. ACM SIGPLAN Notices. 2002 Jun 19;37(7):18-27.
7. Kremen C. Managing ecosystem services: what do we need to know about their ecology?. Ecology letters. 2005 May;8(5):468-79.
8. Zubair M, Sabzevari M, Khatri V, Tarkoma S, Hätönen K. Access control for trusted data sharing. EURASIP Journal on Information Security. 2024 Sep 10;2024(1):30.
9. Edge ME, Sampaio PR. A survey of signature based methods for financial fraud detection. computers & security. 2009 Sep 1;28(6):381-94.
10. Palli AS, Jaafar J, Gilal AR, Alsughayyir A, Gomes HM, Alshanqiti A, Omar M. Online machine learning from non-stationary data streams in the presence of concept drift and class imbalance: A systematic review. Journal of Information and Communication Technology. 2024;23(1):105-39.

11. Montasari R, Hosseinian-Far A, Hill R. Policies, innovative self-adaptive techniques and understanding psychology of cybersecurity to counter adversarial attacks in network and cyber environments. Cyber criminology. 2018 Nov 28:71-93.
12. Abdullayeva FJ. Distributed denial of service attack detection in E-government cloud via data clustering. Array. 2022 Sep 1;15:100229.
13. Khalil U, Malik OA, Hussain S. A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. IEEE Access. 2022 Jul 12;10:76805-23.
14. Alotaibi A, Aldawghan H, Aljughaiman A. A review of the authentication techniques for internet of things devices in smart cities: opportunities, challenges, and future directions. Sensors. 2025 Mar 7;25(6):1649.
15. Manchikanti L. Implications of fraud and abuse in interventional pain management. Pain Physician. 2002;5(3):320.
16. Das RA, Sirazy MR, Khan RS, Rahman SH. A collaborative intelligence (ci) framework for fraud detection in us federal relief programs. Applied Research in Artificial Intelligence and Cloud Computing. 2023;6(9):47-59.
17. Mustafa G, Rafiq W, Jhamat N, Arshad Z, Rana FA. Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. International Journal of Law and Management. 2025 Jan 2;67(1):37-55.
18. Mustafa G, Rafiq W, Jhamat N, Arshad Z, Rana FA. Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. International Journal of Law and Management. 2025 Jan 2;67(1):37-55.
19. Lorenz B, Parasuraman R. Automated and Interactive Real-Time Systems. Handbook of applied cognition. 2007 Jan 1:415-41.
20. Ahmad R, Alsmadi I, Alhamdani W, Tawalbeh LA. Zero-day attack detection: a systematic literature review. Artificial Intelligence Review. 2023 Oct;56(10):10733-811.
21. Singh JP, Aqsa A, Ghani I, Sonani R, Govindarajan V. Privacy-aware hierarchical federated learning in healthcare: integrating differential privacy and secure multi-party computation. Future Internet. 2025 Jul 31;17(8):345.
22. Laourou AB. The adoption and implementation of data mining in accounting information systems (AIS) within the public sector of Nigeria. IIARD Journals. https://doi. org/10.56201/jafm. 2025;11.
23. Kuchuk H, Malokhvii E. Integration of IoT with cloud, fog, and edge computing: a review. Advanced Information Systems. 2024 Jun 4;8(2):65-78.
24. Ball R. Infrastructure requirements for an economically efficient system of public financial reporting and disclosure. Brookings-Wharton papers on financial services. 2001;2001(1):127-69.
25. Lindstedt C, Naurin D. Transparency is not enough: Making transparency effective in reducing corruption. International political science review. 2010 Jun;31(3):301-22.

26. Al-Mushayt OS. Automating E-government services with artificial intelligence. IEEE Access. 2019 Oct 8;7:146821-9.
27. Ibrahim M, Al-Nasrawi S, El-Zaart A, Adams C. Challenges facing e-government and smart sustainable city: An Arab region perspective. In15th European Conference on e-Government, ECEG 2015 Jun 1 (pp. 396-402).
28. Balamurali A, Kartheeswari B. A Secure and Privacy-Preserving E-Government Framework using Blockchain and Artificial Immunity. (ICSICE 24). 2025;1(Icsice 24):1*8.
29. Alzu S, Quiam F, Al-zoubi AM, Almiani M. Neural Network Architectures for Secure and Sustainable Data Processing in E-Government Systems. Algorithms Artic. 2025;1(2):1–17.
30. Lakshmi K, Amarnath N, Farida S, Gowthami G. Enhancing E-Governance Security : The E-GovShield Model Integrating Advanced Cloud Technologies and Threat Mitigation Strategies. Macaw Int J Manag Stud Res. 2024;10(1):1–12.
31. Elisa NOE, Member S, Yang L, Member S. A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity. IEEE Access. 2023;11(November 2022):8773–89.
32. Pamisetty V. Leveraging AI , Big Data , and Cloud Computing for Enhanced Tax Compliance , Fraud Detection , and Fiscal Impact Analysis in Government Financial Management. Int J Sci Res. 2023;12(12):2216–29.
33. Asad S, Bokhari A, Myeong S. The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities : A Stakeholder ' s Perspective. IEEE Access. 2023;11(June):69783–97.
34. Al-besher A, Kumar K. Measurement : Sensors Use of artificial intelligence to enhance e-government services. Meas Sensors [Internet]. 2022;24(October):100484. Available from: https://doi.org/10.1016/j.measen.2022.100484
35. Al-mushayt OS. Automating E-Government Services With Artificial Intelligence. IEEE Access. 2019;7:146821–9.