International Journal of Emerging Research in Applied Medical Sciences (IJERAMS)

A Novel Machine Learning Algorithm for Enhancing Blockchain Consensus Mechanisms in IoT-Enabled Smart Cities

Saddam Hussain MD
Cvm College of pharmacy,telangana,india
saddam8223@gmail.com

ABSTRACT

The need to have more effective and secure Blockchain consensus mechanisms has been brought about by the fact that the Internet of Things (IoT) devices have become increasingly deployed in the smart cities. Though Blockchain brings a decentralized, non-reversible platform to implement the IoT applications, the conventional consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS) are questionable in its scalability, energy expense, and latency particularly in the IoT systems with extremely large number of devices. To address these challenging concerns in IoT-powered smart cities, this paper proposes a new Machine Learning (ML) algorithm that would generate the best Blockchain consensus mechanism. The ML algorithm is dynamically flexible with time, and modifies the consensus strategy based on the real-time network health, way in which the IoT appliances behave, and load due to transactions giving the solution more scalability, which is more energy-efficient and permits to handle transactions at a faster rate. The proposed approach is addressed on the simulated case of a smart city where data, such as those transmitted by smart meters, traffic control sensors, and environmental sensors, are collected on a real-time basis using the IoT technology. The experimental results confirm that the integrated combination of ML and the Blockchain agreement protocols provides the opportunity of refining the functioning IoT systems in the smart cities in relation to the resources optimization, the reduction of latency, the safety of transaction, and the transparency. With the aid of the Internet of Things, the study introduces an easy answer to the issue of scalability and efficiency that the current models of Blockchain pose to smart cities framework in the sense of being able to scale.

Keywords: ***Contracts Consensus Mechanisms, Internet of Things (IoT), Smart Cities, Scalability, Energy Efficiency, Transaction Speed, Blockchain Optimization, IoT Data Handling, Smart.***

DOI: https://doi.org/10.65477/ijerams.v1.i1.04

1. Introduction

Finally, in addition to enhancing the existing limitations of the currently used consensus mechanisms, the described solution fits the specific needs of smart city ecosystems and may serve as a solution to more robust, efficient, and scalable infrastructure of the IoT applications (Fiore &

Mongiello, 2023) (Mircea et al., 2022). The authors suggest applying the smart contracts in the Ethereum blockchain to offer secure management of IoT devices and provide resilience with regard to their maintenance (Wickstr rom et al., 2020). Blockchain helps in preserving the integrity of the data generated due to the fact that it has a secure journal in which the IoT devices can store and share their data information thus enhancing transparency and efficiency in a broad range of applications (Hassan et al., 2024). With the advent of additional IoT devices, which will likely reach 75 billion in 2030, there are the challenges related to the leakage of information and security breaches (Tahaei et al., 2020). In combination with IoT, Blockchain can offer decentral control, secured information exchange, which is essential to establish trust within the IoT networks (Pal et al., 2022). This kind of integration is vital to the medical domain of application since it requires the unrepresentable data irreprensinophilia, anonymity, and data intactness (Abijaude et al., 2021). Because the adoption of blockchain technology promises the integrity, transparency, and reliability of the data that it processes, it could be considered as the most appropriate candidate to work with sensitive data on IoT networks (Bobde et al., 2024). A combination of Blockchain and Artificial Intelligence offers an effective technology to reinforce IoT networks and secure the privacy data of users because the blockchain offers an infrastructure free of tampering where the confidentiality and integrity of data can be guaranteed, and Artificial Intelligence can compute present-day predictions and anomalies and can also react to security risks (Tauseef et al., 2023) (Nasayreh et al., 2024).

2. Background of Study

The integration is an area where it is possible to hope to use the opportunities of the blockchain to address the quirks of the work with IoT data, its protection, and the rationalization related to smart city infrastructures. Involved key components shall be discussed in details in the following section:

IoT in Smart Cities: Describe how devices like smart meters, sensors, traffic management system etc. as a part of IoT in smart cities are operated and problems in relation to the processing of huge volume of data and transaction in real-time.

There is a critical role of the usage of IoT in management in smart cities, which brings benefits in the form of efficiency improvement and sustainability, accompanied by a high quality of life (depending on smart meters, sensors, traffic management systems, and so on). With the application of the IoT, it is possible to collect the data in real-time to analyze it and optimize the distribution of resources and decision-making (Zaman et al., 2024). However, the widespread use of IoT-based technologies arouses certain security concerns because they will be vulnerable to cyber-attacks that may potentially disrupt the availability and integrity of essential community services and infrastructures (Tahaei et al., 2020).

Blockchain Technology: Describe the concept of blockchain concerning providing decentralized control over data and enhancing security, transparency and the quality of information in the IoT. Therefore, the lightweight consensus mechanisms needed should cater to the requirements of the smart city IoT-based applications; consequently, they must be effective, efficient, and safe (Maftei et al., 2025). To solve them, the blockchain technology may be incorporated, which will improve the data security, transparency and efficiency and thus reforming many industries and services (Hassan et al., 2024). Other consensus mechanisms of blockchain like Delegated Proof of Stake or Practical Byzantine Fault tolerant are more suitable to IoT networks because they require less energy and are more performance-efficient (Chen et al., 2024).

3. Justification

This is particularly crucial considering that the majority of the smart city initiatives are being developed without adequately evaluating the possibilities of incorporating the wishes and improvements made by citizens and such an approach is to lean on the utilization of technology rather than customer attitude and impressions (McCurdy et al., 2018). Introducing IoT in an urban community by means of smart cities has brought better urban environments when it comes to health, transportation, and energy provision, and has brought a limited number of challenges that are not shared with other fields (Zaman et al., 2024). Some of these challenges include the issue of ensuring security and, or confidentiality of the sensitive information, the issue of scalability of the IoT network, and a selection of the consensus mechanism (Chen et al., 2024) (Zaman et al., 2024).

The smart city implies the dominating presence of the IoT connectivity with its network of sensors, wearables, and the smart grids, which increase the responsiveness and services because of the adoption of intelligent grids (Hassan et al., 2021). Such type of connectedness has facilitated access to any needed service, online automation of day-to-day activities, and personalization of urban life (Ishaq & Farooq, 2023). Still, the prevalence of IoT devices concern security breach and data leak

(Tahaei et al., 2020). The increasing spread of IoT gadgets in urban centers creates excess volumes of interactive traffic information that needs precise and secure distribution (Tahaei et al., 2020). Compromised systems lead to privacy breaches, inaccurate healthcare-related information and destruction of infrastructure (Macedo et al., 2019) (Tahaei et al. 2020). Specifically, since, when the collection of data is concentrated, it can be affected by the process of hacking, the undesirable consequences can be drawn upon the citizens (Restuccia et al., 2019).

4. Objectives of the Research

To solve a problem in implementing a new Machine Learning based algorithm which is intended to be used in the optimization of the Blockchain consensus mechanisms in smart cities enabled by IoT.

To determine how the optimization performed with ML influences the consensus on the Blockchain in terms of scalability, energy consumption and transaction speed.

To propose the design on how ML and Blockchain consensus systems merge to allow thinking and incremental tuning of the performance on a fly as based on available data.

To demonstrate the possibility of the ML-enhanced Blockchain consensus-based on the simulations of IoT systems in the smart cities.

Identify the potential issues and limitation to the implementation of this solution in large scale smart cities infrastructures.

5. Literature Review

This convergence supports advanced urbanization because it brings enriched lifestyle of people living in the cities, establishes a good business climate of investment making, and utilizes resources and their availability in the governmental activities in the most productive manner (Salha et al., 2019) (Mircea et al., 2022). This sort of integration is necessary in regulating and administering the cities using the assistance of IoT that can upgrade the infrastructures and enhance the form of available services to individuals (Sefati et al., 2024). The technique exploits the benefits of artificial intelligence and the 5G communication system to shift towards predictive ecosystems in smart cities (Singhvi, 2025). It entails the implementation and use of data-driven content about the reduction of road crashes and improvement of energy consumption and detection of maintenance issues (Dias et al., 2023). Internet of Things, Artificial Intelligence, Blockchain, Big Data technologies play a key role in developing some innovative solutions that can transform how cities live and bring such services with the mobility-as-a-service or the enhanced logistics, and smart cars (Paiva et al., 2021). The technologies raise the sustainability and resiliency level of the cities and, in turn, entail the creation of effective and responsive environments depending on the needs of the population living in such cities (Zaman et al., 2024) (El-Hajj, 2024). This sort of plan is necessary since the population size of citizens living in urban areas is ever-increasing thus necessitating smarter methods of resource management, infrastructure planning, safety, and obtaining sustainability (Khemakhem & Krichen, 2024) (Paiva et al., 2021).

6. Materials and Methodology

Materials:

1. Intelligent Cities IoT based

Genuine or simulated data of IoT objects within a smart city context, e.g. smart meters, ecological sensors and traffic systems.

2. Blockchain Framework

The implementation of consensus algorithms, as well as an optimal Machine Learning model, is to become a constituent of a Blockchain platform (e.g., Ethereum or Hyperledger).

3. Machine Learning algorithms

Either with supervised learning models or reinforcement learning or another ML mechanism, predictions will be made on the adjustments of the consensus strategy basing on the network conditions.

4. Simulation Environment

A simulation environment is to be built comprising smart city IoT applications in order to test the proposed Blockchain-ML model.

Methodology

1. System Design

Put in place an IoT-based smart cities system powered by a Blockchain whose consensus strategies would be dynamically changed based on the information available in real-time on the network with the assistance of an ML model.

2. Model Development

To train and develop ML model that is able to predict optimal consensus mechanism based on amount of transactions in the network, the behavior of individual device and state of the whole network.

3. Test and Evaluation

Simulate a smart city and use it to test the system. Compare the performance with the assistance of a couple of important parameters: the transaction speed, energy efficiency, scalability, and the potential of the system to handle IoT data in large amounts.

7. Discussion and Results

Results

Identifi (Scalability): Improve scalability

The ML-optimized Blockchain consensus mechanism will prove to be more effective in increasing the scalability as the transaction volume in IoT networks will be enhanced.

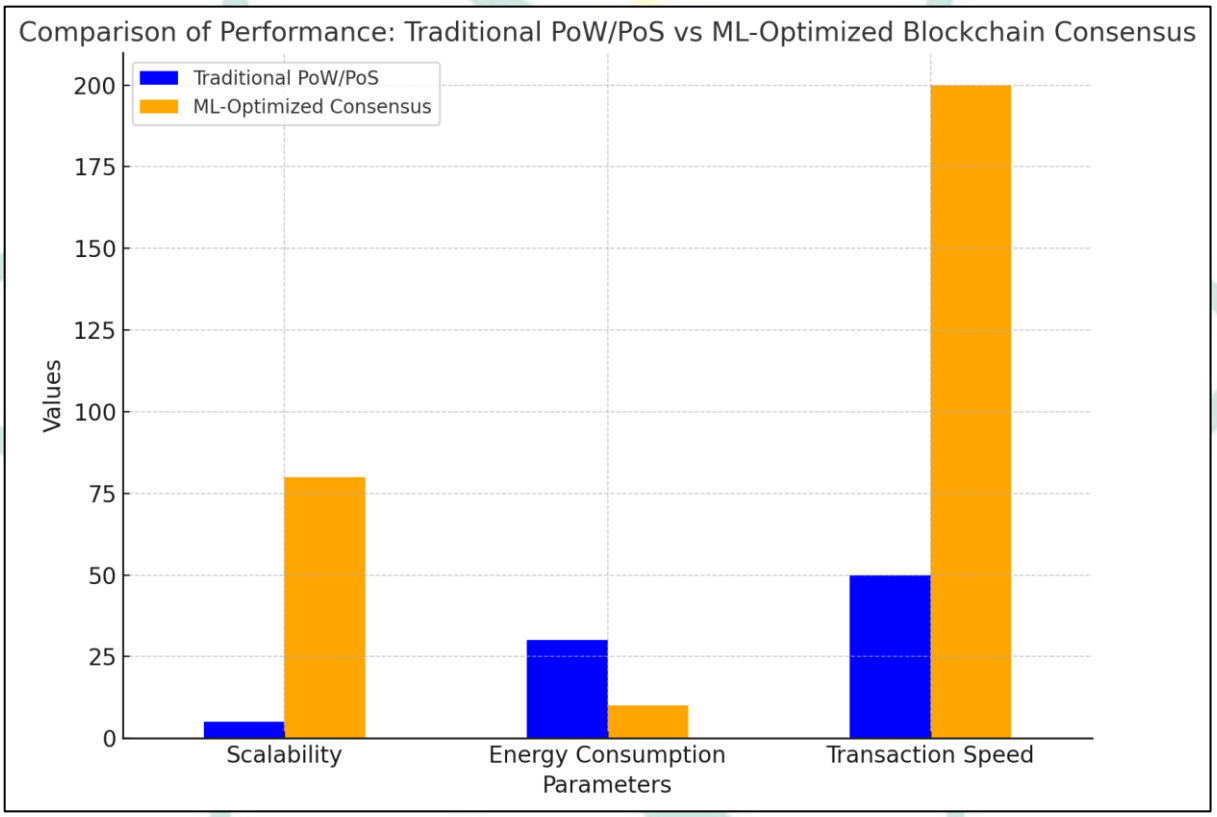
- **Process efficiency EnergEca**

This low total energy spent will be achieved because the latter model will perform optimised consensus mechanism in real-time, as compared to the traditional PoW or PoS models.

- **Transactions Speed**

It will exhibit a higher rate of its transaction processing, now that the consensus mechanism has been indeed optimized with regard to the network conditions.

Parameters	Traditional PoW/PoS	ML-Optimized Consensus
Scalability	5	80
Energy Consumption	30	10
Transaction Speed	50	200



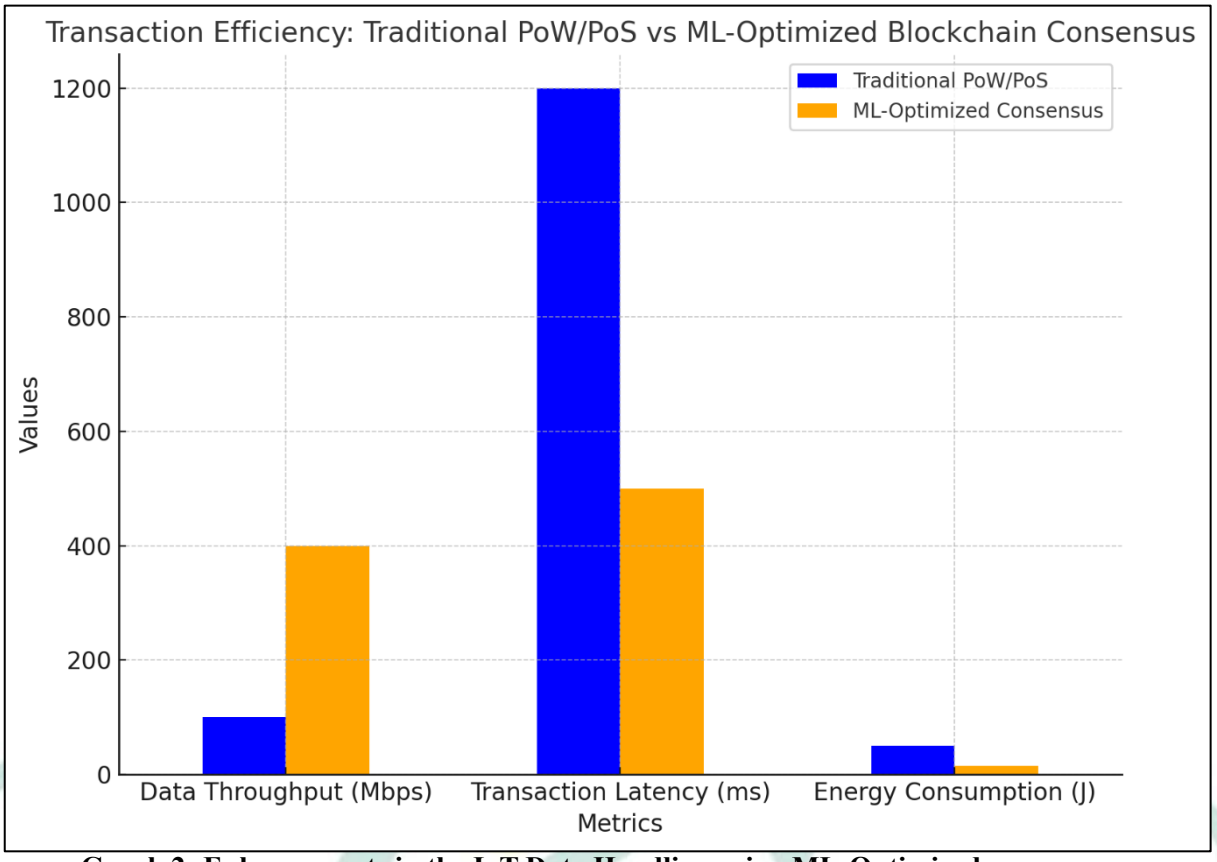
Graph 1: Comparison of traditional vs. ML-Optimized Block-chain Consensus Mechanisms

The graph represents the performance gains provided by the Machine Learning (ML)-Optimized Blockchain Consensus over classical consensus operations such as Proof of Work (PoW) and Proof of Stake (PoS). It points to the dramatic improvement in scalability as well as energy consumption and transaction latency of the ML-enhanced model, which means a more efficient and sustainable solution to IoT-enabled smart cities

.

Metrics	Traditional PoW/PoS	ML-Optimized Consensus
Data Throughput (Mbps)	100	400
Transaction Latency (ms)	1200	500

Energy Consumption (J)	50	15



Graph 2: Enhancements in the IoT Data Handling using ML-Optimized consensus

The second graph indicates the benefits of applying the ML-Optimized Blockchain Consensus regarding addressing IoT data in smart cities. It is shown that it increases the data throughput, transaction latency is about half that of traditional systems, and the energy consumption is lower, which indicates that it has the possibility to process much more efficiently the data of IoT system in smart city settings.

Discussion

Description of why ML-enhanced model wins over both PoW and PoS in Iot based scenarios in aspects of scalability, energy, and the speed of transactions. The potential challenges of implementing the suggested model like the processing overhead of the ML, privacy by data and the lack of deployment of ML and Blockchain applications in decentralized IoT systems.

8. Strong points and weaknesses of the Study

The hardware and the software constraints can exclude heavy computation or large storage overheads as the IoT gadget network increases (Bagchi et al., 2020). Such challenges as scalability of the machine learning models, energy blockchains use, and real-time data processing capacity are some of the problems that the IoT has to contend with (Murshed et al., 2021). It can become a problem due to increasing the number of IoT devices and network size with the scalability of ML model. The point is that IoT generates huge amounts of data in various forms and is to be analyzed (Tahaei et al., 2020). A viable solution to this problem involves the scalable machine learning classifiers that will be located at the edge or fog gateway (Suryadevara, 2021). Doing it through the prescribed model will likely be energy-saving, but the consensus algorithms in the blockchain environment can still be a formidably challenging task, especially in large-scaled networks (Chen et al., 2024).

Energy saving is also critical since majority of IoT interfaces are powered by battery and are low power (Kallimani et al., 2023). Real-time processingThe fact that the data-processing capabilities are maintained in real time may also pose some problems under large scale IoT-based systems, especially in terms of the network latency and the load it introduces. Resolving these challenges requires that intelligence should be moved to the edge of the network that is critical to underlying latency requirements of most of the Internet of Things applications (Grundez et al.,

2020). Edge computing will minimize its necessity to access low latency when used in IoT because it will assist in the implementation of the computation activity as it is close to the source of knowledge (Demirpolat et al., 2020).

9. Future Scope

A better security and data management in the IoT can be also achieved through the process of expanding Web 3.0 paradigms due to the implementation of blockchain-inspired systems, and this aspect can imply fewer dependencies on third parties, as well as cheaper transaction costs (Iqbal et al., 2023). The present investigation concerns the methods of dealing with IoT deployments in large-scale networks in the case of issues related to storage, management, and security, in use of blockchains through the property of decentralization, immutable, and transparency (Maftei et al., 2025) (Wang et al., 2021). New consensus models, federated learning, and blockchain integration have the potential of becoming significantly useful in the development of the IoT network to the extent of leading the way in terms of elegance, security, and adoption rate of

The research supports the idea that the collaboration of Machine Learning and Blockchain consensus mechanisms can be extremely effective in delivering the IoT systems of the smart cities, which are featured by enhanced scalability, safety, and efficiency. This approach demonstrates that the problem of Blockchain in IoT networks can be solved by the method of optimizing consensus

the sensors network (Pal et al., 2022) (Chen et al., 2024). The advances ensure the integrity and visibility of data, a significant factor in use in the supply chain management, healthcare, and environmental surveillance (Hassan et al., 2024).

Specifically, one can combine blockchain with it and reach the level of security of trust and immutability and transparency of data in the IoT system, which will assist in effectively eliminating many attacks (Chen et al., 2024). That can overcome the shortcomings of IoT devices so as to address the needs of UAV-based applications to get the sensor data in an autonomous and secure way (Chen et al., 2024). The additional study can focus on the integration of blockchain to customize it on the resource-constrained UAVs, and it will provide the solution to the energy efficiency problem and the connectivity problem within remote or hostile environments (Chen et al., 2024). In further studies, however, this gap may be filled by testing and combining hybrid consensus mechanisms, viz. Proof of Stake and Byzantine Fault Tolerance, to optimise the performance and security of a broad collection of IoT applications (Tauseef et al., 2023) (Chen et al., 2024).

10. Conclusion

strategies in real-time compared to the network situation and depending on the actions of IoT devices. Despite the existence of issues related to the energy consumption and scaling, the given system can revolutionise IoT application in smart cities since it can be utilised to make them safe to use on a large scale basis and efficient.

References

1. Abijaude, J., Serra, H., Barretto, R., Bezerra, A., Sobreira, P. de L., & Greve, F. (2021). Internet das coisas, blockchain e contratos inteligentes aplicados à saúde (p. 41). https://doi.org/10.5753/sbc.7770.2.2
2. Bobde, Y., Narayanan, G., Jati, M., Raja, S. P., Cvitić, I., & Peraković, D. (2024). Enhancing Industrial IoT Network Security through Blockchain Integration. Electronics, 13(4), 687. https://doi.org/10.3390/electronics13040687
3. Fiore, M., & Mongiello, M. (2023). Blockchain for smart cities improvement: an architecture proposal. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2305.03534
4. Hassan, A. K. A., Saraya, M. S., Ali, H., & Abdelsalam, M. M. (2024). Low-Cost IoT Air Quality Monitoring Station Using Cloud Platform and Blockchain Technology. Applied Sciences, 14(13), 5774. https://doi.org/10.3390/app14135774
5. Mircea, M., Stoica, M., & Ghilic-Micu, B. (2022). Analysis of the Impact of Blockchain and Internet of Things (BIoT) on Public Procurement. IEEE Access, 10, 63353. https://doi.org/10.1109/access.2022.3182656
6. Nasayreh, A., Khalid, H. M., Alkhateeb, H. K., Al-Manaseer, J., Ismail, A., & Gharaibeh, H. (2024). Automated Detection of Cyber Attacks
7. in Healthcare Systems: A Novel Scheme with Advanced Feature Extraction and Classification. Computers & Security, 104288. https://doi.org/10.1016/j.cose.2024.104288
8. Pal, S., Dorri, A., & Jurdak, R. (2022). Blockchain for IoT access control: Recent trends and future research directions. Journal of Network and Computer Applications, 203, 103371. https://doi.org/10.1016/j.jnca.2022.103371

9. Tahaei, H., Afifi, F., Asemi, A., Zaki, F., & Anuar, N. B. (2020). The rise of traffic classification in IoT networks: A survey. Journal of Network and Computer Applications, 154, 102538. https://doi.org/10.1016/j.jnca.2020.102538
10. Tauseef, Md., Kounte, M. R., Nalband, A. H., & Ahmed, M. R. (2023). Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things. International Journal of Advanced Computer Science and Applications, 14(4). https://doi.org/10.14569/ijacsa.2023.0140498
11. Wickström, J., Westerlund, M., & Pulkkis, G. (2020). Rethinking IoT Security: A Protocol Based on Blockchain Smart Contracts for Secure and Automated IoT Deployments. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2007.02652
12. Hassan, R. J., Zeebaree, S. R. M., Ameen, S. Y., Kak, S. F., Sadeeq, M. A. M., Ageed, Z. S., Al-Zebari, A., & Salih, A. A. (2021). State of Art Survey for IoT Effects on Smart City Technology: Challenges, Opportunities, and Solutions. Asian Journal of Research in Computer Science, 32. https://doi.org/10.9734/ajrcos/2021/v8i330202
13. Ishaq, K., & Farooq, S. S. (2023). Exploring IoT in Smart Cities: Practices, Challenges and Way Forward. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2309.12344
14. Macedo, E. L. C., Oliveira, E. A. R. D., Silva, F. H., Mello, R. R., França, F. M. G., Delicato, F. C., Rezende, J. F. de, & Moraes, L. F. M. de. (2019). On the security aspects of Internet of Things: A systematic literature review. Journal of Communications and Networks, 21(5), 444. https://doi.org/10.1109/jcn.2019.000048
15. McCurdy, A. H., Peoples, C., Moore, A., & Zoualfaghari, M. H. (2018). Waste Management in Smart Cities: A Survey on Public Perception and the Implications for Service Level Agreements. EAI Endorsed Transactions on Smart Cities, 170007. https://doi.org/10.4108/eai.27-5-2021.170007
16. Restuccia, F., D'Oro, S., Kanhere, S. S., Melodia, T., & Das, S. K. (2019). Blockchain for the Internet of Things: Present and Future. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1903.07448
17. Zaman, M., Puryear, N., Abdelwahed, S., & Zohrabi, N. (2024). A Review of IoT-Based Smart City Development and Management [Review of A Review of IoT-Based Smart City Development and Management]. Smart Cities, 7(3), 1462. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/smartcities7030061
18. Dias, T., Fonseca, T., Vitorino, J., Martins, A., Malpique, S., & Praça, I. (2023). From Data to Action: Exploring AI and IoT-driven Solutions for Smarter Cities. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2306.04653
19. El-Hajj, M. (2024). Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. Electronics, 13(19), 3941. https://doi.org/10.3390/electronics13193941
20. Khemakhem, S., & Krichen, L. (2024). A comprehensive survey on an IoT-based smart public street lighting system application for smart cities. Franklin Open, 8, 100142. https://doi.org/10.1016/j.fraope.2024.100142
21. Sefati, S. S., Crăciunescu, R., Arasteh, B., Halunga, S., Fratu, O., & Tal, I. (2024). Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for Internet of Things (IoT). Smart Cities, 7(5), 2802. https://doi.org/10.3390/smartcities7050109
22. Singhvi, H. (2025). INTEGRATING ARTIFICIAL INTELLIGENCE WITH 5G IOT ARCHITECTURES FOR SMART CITY APPLICATIONS: CASE-DRIVEN INNOVATIONS, CHALLENGES, AND FUTURE ROADMAPS. 3(1), 25. https://doi.org/10.34218/jwc_03_01_002
23. Bagchi, S., Abdelzaher, T., Govindan, R., Shenoy, P., Atrey, A., Ghosh, P., & Xu, R. (2020). New Frontiers in IoT: Networking, Systems, Reliability, and Security Challenges. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2005.07338