ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 12, Issue.2 April 2024

BLOCK CHAIN BASED ARCHITECTURE AND FRAMEWORK FOR CYBERSECURITY SMART CITIES

Sama Sai Ram [1], B. Nikhil [2],
K Sai Shiva [3], Dr. K. Niranjan Reddy[4]
[1,2,3] UG Student, Dept. of ECE, CMR Institute of Technology, Hyderabad
[4] Associate Professor, Dept. of ECE,
CMR Institute of Technology, Hyderabad

ABSTRACT

A smart city is one that uses digital technologies and other means to improve the quality of life of its citizens and reduce the cost of municipal services. Smart cities primarily use IoT to collect and analyze data to interact directly with the city's infrastructure and monitor city assets and community developments in real time to improve operational efficiency and proactively respond to potential problems and challenges. Today, cybersecurity is considered one of the main challenges facing smart cities. Over the past few years, the cybersecurity research community has devoted a great deal of attention to this challenge. Among the various technologies being considered to meet this challenge, Blockchain is emerging as a solution offering the data security and confidentiality essential for strengthening the security of smart cities. In this paper, we propose a comprehensive framework and architecture based on Blockchain, big data and artificial intelligence to improve smart cities cybersecurity. To illustrate the proposed framework in detail, we present simulation results accompanied by analyses and tests. These simulations were carried out on a smart grid dataset from the UCI Machine Learning Repository. The results convincingly demonstrate the potential and effectiveness of the proposed framework for addressing cybersecurity challenges in smart cities. These results reinforce the relevance and applicability of the framework in a real-world context.

INTRODUCTION

In the digital age, everything is connected as part of the growing and accelerating digital transformation of modern societies, which involves all kinds of sectors and human activities such as education, healthcare, economy, energy, etc. Urban communities, and even some villages, are benefiting from the technologies and solutions available through digital transformation to engage in all kinds of smart city initiatives to put them at the service of sustainable, resilient and inclusive socio-economic development.

The smart city achieves efficiencies, promotes sustainability, and improves the quality of life for its residents through the integration of technology. Planning for a smart city is essentially about bringing the Internet of Things (IoT) to scale. The Internet of Things (IOT) is the network of physical terminals, objects, incorporating software, connectivity, sensors, etc., to connect to other systems on the internet and exchange data to provide proper management and monitoring of city infrastructure and operations. Driven by the growing urban population, IOT and ICT are the main pillars of smart cities to improve their efficiency as well as the lives of their citizens [1], [2]. A smart city needs technological efficiency in areas as diverse as transportation and mobility, services, communication, security, citizen relations, etc. The implementation of IOT-based applications within cities allows for the optimization of: energy control, building performance, street furniture management, waste disposal, mobility, etc. The beneficiaries are citizens, consumers, private companies and local authorities [3]. By offering increasingly digitized services, smart cities are becoming ever more connected but also more exposed to cyber risks and cyber-attacks. Data collection is essential in IOT-based applications and services that are considered key assets for monitoring and operating smart cities. Therefore, managing data across the smart city infrastructure is a big challenge given all the connected devices involved and their different architectures and urban data must be protected throughout its lifecycle. However, the main challenge is to protect IoT infrastructures throughout their deployment [4]. In this case, an important question arises, namely: how to transfer all data quickly, securely and without third-party intermediaries?

LITERATURE REVIEW

IN "SUSTAINABLE SMART CITIES: CONVERGENCE OF ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN" In the digital era, the smart city can become an intelligent society by utilizing advances in emerging technologies. Specifically, the rapid adoption of blockchain technology has led a paradigm shift to a new digital smart city ecosystem. A broad spectrum of blockchain applications promise solutions for problems in areas ranging from risk management and financial services to cryptocurrency, and from the Internet of Things (IoT) to public and social services. Furthermore, the convergence of Artificial Intelligence (AI) and blockchain technology is revolutionizing the smart city network architecture to build sustainable ecosystems. However, these advancements

in technologies bring both opportunities and challenges when it comes to achieving the goals of creating a sustainable smart cities. This paper provides a comprehensive literature review of the security issues and problems that impact the deployment of blockchain systems in smart cities. This work presents a detailed discussion of several key factors for the convergence of Blockchain and AI technologies that will help form a sustainable smart society. We discuss blockchain security enhancement solutions, summarizing the key points that can be used for developing various blockchain-AI based intelligent transportation systems. Also, we discuss the issues that remain open and our future research direction, this includes new security suggestions and future guidelines for a sustainable smart city ecosystem. Rapid urbanization of the world population causes many economic, environmental, and social problems that can affect the lifestyle and quality of life of many people significantly. Given the high density of people in urban areas, the concept of the smart city brings opportunities to solve these problems and provide a better lifestyle through high quality intelligent service. The sustainable smart cities concept hopes to help raise awareness and publicize green energy minimal consumption best practices. As forecasted by the United Nations, 66 % of the world population (United Nations, 2015) will soon live in big cities, which implies there will be significant challenges we have to face for social sustainability. Moreover, the form of the modern-day city is seen as a social and environmental problem. Around 70 % of the world's resources are consumed by municipalities, which brings significant challenges to the distribution of these resources through cutting edge technologies (Bibri & Krogstie, 2017).

IN "MIGRATING FROM TRADITIONAL GRID TO SMART GRID IN SMART CITIES PROMOTED IN DEVELOPING COUNTRY,'' Smart Grid is a term that encompasses the economic benefits of an intelligent and advanced power grid to reach changing responsibilities related directly to sustainability and energy efficiency. Considering the shortfall of alternative fuels in developed regions, the new smart grids, in order to have access to their environmental hazard, show that the average non-renewable and renewable energy sources can be integrated to reduce environmental disasters to improve production costs significantly. In order to provide reliable, secured, and cost-effective power grid functions, infrastructures can quickly and effectively co-ordinate power-

sharing between several renewable energy sources freely accessible and economically demand costs. This article reviews the conceptual model, goals, architecture, potential benefits, and power grid issues with a complete and accurate understanding of the different defenders and people involved in the worldwide region scenario. The article examined energy and transmission issues, including smart grids and grid barriers, comprehensively. A Smart City is a city atmosphere that uses many IoT sensors to collect data and then utilizes insights gained to manage the assets, services, and resources effectively. It includes information about people, equipment, buildings, and assets that are processed and examined for monitoring and management of transportation systems, Electric power stations, utilities, water distribution networks, waste management, criminal activity detection [6], information systems, school education, library system, healthcare, and other community-based services.

IN "DEPLOYMENT AND INTEGRATION OF SMART SENSORS WITH IOT DEVICES DETECTING FIRE DISASTERS IN HUGE FOREST ENVIRONMENT,'' Surveillance system applications are drastically growing from small buildings to a wide area of forest monitoring. Forests provide various important things to our daily lives like oxygen, honey. Living things like animals and birds are living in forests. Thus, it is essential to monitor and protect the forests and their assets. To do that, smart sensors have been deployed in the forest to monitor and record the environmental impacts. The abnormal events are identified and detected using the appropriate IoT devices to reduce the risk. Also, to improve the accuracy, the sensed data is analyzed, processed using a software module. Various existing approaches used for learning the data and object detection was good, but slow in the process, which fails in reducing risks. To overcome these issues, this paper utilizes one of the Deep Learning Algorithms such as the Convolution Neural Network (CNN) for Forest Monitoring and identifying the abnormality. The deep CNN has experimented with MATLAB software and the results are verified. The performance of deep CNN is evaluated by comparing the obtained results with the existing approaches and found that deep CNN outperforms the others

IN "BLOCKCHAIN-BASED BIG DATA ANALYTICS APPROACH FOR SMART CITIES" Nowadays, smart cities are using advanced technologies to control

and coordinate physical, social, and commercial enterprise systems to deliver high-quality services to their residents while guaranteeing the effective usage of available resources. Numerous major corporations, as well as government bodies, are involved in the construction of smart cities because smart city activities also need information that is obtained from organizations. Blockchain-based technology allows for peer-to-peer exchanges as a public ledger that maintains records of transactions, smart contracts, agreements, and shipments without third-party mediators. In the future, smart cities will be equipped with several innovative technologies, a huge amount of data, a lot of Internet of Things (IoT) devices, and a heterogeneous environment. However, data processing among IoT devices in futuristic smart cities is a challenging task. In this paper, the author proposed a blockchain-based big data integrity service framework for IoT devices data processing in smart cities. The author collected the necessary data from various resources and applied three experiments to evaluate the key performance indicators. K-mean algorithm was used to classify the data, and blockchain strategy was applied to ensure secure communication among IoT devices. The framework was simulated and tested using 100 devices. The proposed framework allowed IoT devices to efficiently use information collected from different resources to engage in operational processes and exchange information. The vast amount of research on big data analytics, blockchain, and the integration of both technologies provides many possibilities for smart city applications to thrive using these technologies (Karafiloski and Mishev, 2017). The acceptance of blockchains by companies across the globe keeps growing due to its success and the latest big data innovations have made data from different sources accessible besides investigation (Alam et al., 2020). Throughout the world, several cities are trying to become smart cities. Even so, its expertise and the system on its use of information by smart cities are still largely undefined (Alam and Benaida, 2018). Blockchain and big data growth have played a key role in the efficacy of smart city developments (Hassani et al., 2019). However, a pertinent question remains: Are the current technologies capable of achieving a security solution inside the smart cities that are massively establishing? Various steps should be considered, besides securing only sustainable development (Alam, 2020). Internet-connected gadgets like sensors, smart devices, and cameras making up the Internet of Things (IoT) keep rising exponentially (Alam, 2017). The

trends of big data, blockchain, and smart cities from January 2016 to January 2021, according to Google Trends, are shown in Figure 1 (Google Trends, n.d.). The objective of this study was to create a novel big-data- and blockchain-based integrated framework for IoT device data processing for futuristic smart cities. In this article, the author discussed such an integrated approach to assessing data exchange in smart cities, which helps to share resources across different unauthenticated environments. This integrated technology allows smart devices to efficiently use data collected from different resources to engage in operational processes without requiring access to the main information.

EXISTING SYSTEM

Internet of Things (IoT) is growing exponentially in research and industry. Although, many standard and conventional security solutions have been provided for IoT, it suffers from many privacy and security concerns. Standard security protocols are not suitable for majority of IoT devices because of its decentralized topology and resource-constraints. Blockchain (BC) finds its efficient application in IoT to preserve the five basic cryptographic primitives, such as confidentiality, authenticity, integrity, availability and non-repudiation. Adoption of conventional BC in IoT causes high energy consumption, delay and computational overheads which are not appropriate for various resource constrained IoT devices. To mitigate these problems, this work proposes a smart access control framework in a public and a private BC for a smart city application which makes it more efficient and secure as compared to the existing IoT applications.

IoT based smart city architecture adopts BC technology for preserving all the cryptographic security and privacy issues. Moreover, proposed BC has minimal overhead as well. This work investigates the existing threat models and critical access control issues which handle multiple permissions of various processing nodes of IoT environment and detects relevant inconsistencies. Comparison in terms of all security issues with existing literature shows that the proposed architecture is competitively efficient in terms of security access control. The primary goal of this research article is to explore the possibility of BC as an alternative to standard security solutions for low resource IoT applications.

DISADVANTAGES

• The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cybersecure Smart City.

• Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.

• Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

PROPOSED SYSTEM

we integrate machine learning. Preprocessing of data using machine learning is done because the collected data is in a raw format and it is not always possible to train/test the model using it. It is important to process this raw data in order to interpret it correctly and avoid any negative results in the prediction. In our case, we are dealing with too massive databases, which makes the computations too slow. We then decided to use PySpark DataFrame [10] which is one of the most optimized Machine Learning platforms for dealing with massive databases using distributed programming, and which consists of using multiple distributed computing units on multiple nodes to reduce the execution time of a query. Our algorithm uses the historical data of the Blockchain to build the model (training and testing), thus, after the end of the preprocessing and through PySpark the historical data of the Blockchain will be read in order to train/test the model, then, we use the linear regression model to predict the new records of the variable ‘‘stab’’, this prediction tool solves the binary classification problem (i.e.,stable or unstable).

ADVANTAGES

• Easy and secure data exchange.

• Promotion of collaboration among public administrations.

• To obtain a single view of the Smart City’s supply chains.

• To reduce fraud and verify financial transactions faster.

• To create smarter and more efficient supply chains.

• To simplify processes for reconciling data disputes for audit and regulatory compliance.

• To manage energy consumption, urban development and population growth.

MODULES

SERVICE PROVIDER

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Browse and Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View

Trained and Tested Accuracy Results, View Prediction Of Cyber secure Smart City Status, View Cyber secure Smart City Status Ratio, Download Trained Data Sets, View Cyber secure Smart City Status Ratio Results, View All Remote Users.

VIEW AND AUTHORIZE USERS In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

REMOTE USER

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT CYBERSECURE SMART CITY TYPE, VIEW YOUR PROFILE.

CONCLUSION

In this paper, we present a comprehensive and efficient approach for strengthening smart cities cyber security. Using block chain, big data and artificial intelligence algorithms, this approach offers a robust and a reliable framework for smart cities data security and privacy. This framework was illustrated using a real dataset on smart grid, demonstrating its efficiency and reliability. By focusing on data confidentiality, integrity and availability, our approach allows to guarantee a secure environment for smart cities, their infrastructures and services while improving their resilience to cyber-attacks. In addition, this approach fosters mutual trust among the smart cities stakeholders and strengthens citizens confidence and engagement in smart cities applications and services.

REFERENCES

[1] A. Sharma, E. Podoplelova, G. Shapovalov, A. Tselykh, and A. Tselykh, ''Sustainable smart cities: Convergence of artificial intelligence and blockchain,'' *Sustainability*, vol. 13, no. 23, p. 13076, Nov. 2021, doi: 10.3390/su132313076.

[2] O. S. Neffati, S. Sengan, K. D. Thangavelu, S. D. Kumar, R. Setiawan,

M. Elangovan, D. Mani, and P. Velayutham, ‘‘Migrating from traditional grid to smart grid in smart cities promoted in developing country,’’ *Sustain. Energy Technol. Assessments*, vol. 45, Jun. 2021, Art. no. 101125, doi: 10.1016/j.seta.2021.101125.

[3] F. Cui, ‘‘Deployment and integration of smart sensors with IoT devices detecting fire disasters in huge forest environment,’’ *Comput. Commun.*, vol. 150, pp. 818–827, Jan. 2020.

[4] T. Alam, ‘‘Blockchain-based big data analytics approach for smart cities,’’ Tech. Rep., Nov. 2020, doi: 10.36227/techrxiv.13054244.v2.

[5] T. Alam, ‘‘IoT-fog: A communication framework using blockchain in the Internet of Things,’’ *Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 1–10, 2019.

[6] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, ‘‘A blockchainbased trust system for the Internet of Things,’’ in *Proc. 23rd ACM Symp. Access Control Models Technol.*, Jun. 2018, pp. 77–83.

[7] D. Minoli and B. Occhiogrosso, ‘‘Blockchain mechanisms for IoT security,’’ *Internet Things*, vol. 1, pp. 1–13, Sep. 2018.

[8] K. Christidis and M. Devetsikiotis, ‘‘Blockchains and smart contracts for the Internet of Things,’’ *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] T. Alam, ‘‘Blockchain and its role in the Internet of Things (IoT),’’ *Int. J. Sci. Res. Comput. Sci., Eng. Inf. Technol.*, vol. 5, no. 1, pp. 151–157, Jan. 2019, doi: 10.32628/CSEIT195137.

[10] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, and A. A. Abd El-Latif, ‘‘Convergence of blockchain and IoT for secure transportation systems in smart cities,’’ *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Apr. 2021.

[11] Reddy, Kallem Niranjan, and Pappu Venkata Yasoda Jayasree. "Low Power Strain and Dimension Aware SRAM Cell Design Using a New Tunnel FET and Domino Independent Logic." International Journal of Intelligent Engineering & Systems 11, no. 4 (2018).

[12] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Design of a Dual Doping Less Double Gate Tfet and Its Material Optimization Analysis on a 6t Sram Cells."

[13] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Low power process, voltage, and temperature (PVT) variations aware improved tunnel FET on 6T SRAM cells." Sustainable Computing: Informatics and Systems 21 (2019): 143-153.

[14] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Survey on improvement of PVT

aware variations in tunnel FET on SRAM cells." In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), pp. 703-705. IEEE, 2017

[15] Karne, R. K. ., & Sreeja, T. K. . (2023). PMLC- Predictions of Mobility and Transmission in a Lane-Based Cluster VANET Validated on Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5s), 477–483. https://doi.org/10.17762/ijritcc.v11i5s.7109

[16] Radha Krishna Karne and Dr. T. K. Sreeja (2022), A Novel Approach for Dynamic Stable Clustering in VANET Using Deep Learning (LSTM) Model. IJEER 10(4), 1092-1098. DOI: 10.37391/IJEER.100454.

[17] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, ‘‘Everything you wanted to know about the blockchain: Its promise, components, processes, and problems,’’ *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018, doi: 10.1109/MCE.2018.2816299.

[18] Q. Wang, H. Zhao, Q. Wang, H. Cao, G. S. Aujla, and H. Zhu, ‘‘Enabling secure wireless multimedia resource pricing using consortium blockchains,’’ *Future Gener. Comput. Syst.*, vol. 110, pp. 696–707, Sep. 2020, doi: 10.1016/j.future.2019.09.026.

[19] X. Huang, Y. Zhang, D. Li, and L. Han, ‘‘An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains,’’ *Future Gener. Comput. Syst.*, vol. 91, pp. 555–562, Feb. 2019, doi: 10.1016/j.future.2018.09.046.

[20] C. Yang, X. Chen, and Y. Xiang, ‘‘Blockchain-based publicly verifiable data deletion scheme for cloud storage,’’ *J. Netw. Comput. Appl.*, vol. 103, pp. 185–193, Feb. 2018, doi: 10.1016/j.jnca.2017.11.011.

[21] H. Chen and Y. Wang, ‘‘SSChain: A full sharding protocol for public blockchain without data migration overhead,’’ *Pervas. Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101055, doi: 10.1016/j.pmcj.2019.101055.

[22] A. K. Tripathi, K. Akul Krishnan, and A. C. Pandey, ‘‘A novel blockchain and Internet of Things-based food traceability system for smart cities,’’ *Wireless Pers. Commun.*, vol. 129, no. 3, pp. 2157–2180, Apr. 2023, doi: 10.1007/s11277-023-10230-9.

[23] J. Wu and N. Tran, ‘‘Application of blockchain technology in sustainable

energy systems: An overview,'' *Sustainability*, vol. 10, no. 9, p. 3067, Aug. 2018, doi: 10.3390/su10093067.

[24] N. Alasbali, ''Rules of smart IoT networks within smart cities towards blockchain standardization,'' *Mobile Inf. Syst.*, vol. 2022, Feb. 2022, Art. no. 9109300, doi: 10.1155/2022/9109300.

[25] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, ''A survey on consensus mechanisms and mining strategy management in blockchain networks,'' *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.