

A Blockchain-Based Architecture and Framework for Cybersecure Smart Cities

Devarapalli Sreenivasa Reddy¹, Dr. K. V. Srinivasa Rao²

*PG scholar, Department of Computer Science & Engineering, Prakasam Engineering College, Kandukur,
Associate Professor, Department of Computer Science & Engineering, Prakasam Engineering College,
Kandukur.*

Abstract : A smart city is one that lowers the cost of municipal services while simultaneously enhancing the quality of life for its residents via the use of digital technology and other strategies. In order to monitor municipal assets and community developments in real time, enhance operational efficiency, and proactively address any issues and obstacles, smart cities largely employ IoT to gather and analyze data. These days, one of the biggest issues confronting smart cities is cyber security. The cyber security research community has given this problem a lot of attention in recent years. Blockchain is starting to emerge as a technology that may help with this difficulty. It provides the data security and secrecy that are necessary to bolster the security of smart cities. In order to enhance the cyber security of smart cities, we provide in this article a thorough framework and architecture based on big data, blockchain, and artificial intelligence. We give simulation results together with analysis and testing to provide a detailed picture of the suggested system. The UCI Machine Learning Repository's smart grid dataset served as the basis for these simulations. The results clearly show the potential and efficacy of the suggested methodology for handling cyber security issues in smart cities. These outcomes support the framework's applicability and usefulness in a practical setting.

Index Terms--- Smart city, smart grid, cyber security, framework, IoT, blockchain, big data, artificial intelligence

1. Introduction

As part of the expanding and quickening digital transformation of contemporary society, which encompasses a wide range of industries and human endeavors including healthcare, education, the economy, energy, and so on, everything is linked in the digital age. The tools and solutions made possible by the digital revolution are helping urban communities—and some rural ones, too—engage in a variety of smart city projects that support inclusive, resilient, and sustainable socioeconomic growth. By integrating technology, a smart city increases productivity, encourages sustainability, and enhances the quality of life for its citizens. Bringing the Internet of Things (IoT) to scale is the fundamental component of smart city planning. The Web 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. Giovanni Merlino was the associate editor in charge of organizing the review of this manuscript and approving it for publication. IoT and ICT are the key pillars of smart cities, driven by the increasing urban population, to enhance both the efficiency and quality of life of their residents [1], [2]. Technological efficiency is required in a smart city in a variety of domains, including services, citizen interactions, communication, security, and mobility and transportation. Cities may optimize a variety of processes by implementing IoT-based applications, including garbage disposal, street furniture management, energy control, building performance, and mobility. Local governments, businesses, individuals, and consumers all gain from this [3]. As smart cities provide more and more digitalized services, they link people and increase their vulnerability to cyberattacks and other threats. IoT-based services and apps that are regarded as vital resources for managing and monitoring smart cities depend on data collecting. Because of the many linked devices and their various designs, managing data throughout the smart city infrastructure is thus quite difficult. Additionally, urban data has to be safeguarded at every stage of its existence. Nonetheless, the primary obstacle is in safeguarding IoT infrastructures throughout their implementation [4]. In this instance, a crucial query emerges: how can all data

be sent swiftly, safely, and without the need for middlemen? By reclaiming personal data that would no longer be in the hands of middlemen, the implementation of blockchain technology in smart cities would enable more regulated government. It provides the option to secure and encrypt the data being sent, all the while guaranteeing its traceability and anonymity. Furthermore, it maximizes the interconnectivity of all the city's services while offering real-time data on energy, waste management, mobility (such as the cars utilized and the routes traveled), etc. [5], [6]. The blockchain is a distributed system that enables data transfer and storage. It is built on a series of blocks. The capacity to track every transaction and the fact that blockchain technology operates independently, securely, and transparently without the need for a central authority are two of its benefits. By assisting users in validating information, cryptography ensures its legitimacy [7]. The individuals selected inside the blockchain to oversee the technical framework of the implementation get compensation for their duties in examining, confirming, and authenticating the accuracy of the data in relation to other records within the blockchain. The block is time-stamped and posted to the blockchain when it has been confirmed and approved. At that point, anybody may access and read this data, but they cannot edit it. If a mistake occurs, a fresh transaction will fix it [8]. Smart contracts are the digital counterpart of paper contracts; they are often implemented on a blockchain and relate to irreversible computer programs that carry out certain commands that have to be complied with. All verification procedures taken during the smart contract's execution are documented on the blockchain, which guards and secures all data by preventing post-event change or deletion [9]. Machines that are equipped with artificial intelligence (AI) may mimic human cognitive functions including language, reasoning, perception, and so on. It also describes the capacity of robots and computers to carry out intelligent activities devoid of human assistance. While AI organizes information and learns to solve issues using machine learning (ML) techniques, humans build rule-based or logic-based systems to solve problems. Smart cities powered by data-intensive apps are being constructed using blockchain and artificial intelligence. Because of this, they may assist smart cities in achieving "data sovereignty" and enhancing data security via traceable and secure transactions, averting circumstances like data leaks and abuse [10]. Spark's Mllib is one of the ML libraries that has been successful in simplifying and scaling ML. It's a machine learning package that makes it possible to analyze algorithms quickly and well. Among the many tools it offers are: machine learning algorithms, which include traditional machine learning techniques including clustering, collaborative filtering, regression, and classification.

2. Literature Survey

K. Christidis and M. Devetsikiotis [1] Driven by the current surge in interest in block chains, we investigate whether they are a suitable match for the Internet of Things (IoT) industry. Block chains enable the creation of dispersed peer-to-peer networks in which members who lack trust may communicate with one another in an authenticated way without the need for a trusted middleman. We go over the operation of this mechanism and investigate smart contracts, which are blockchain-based scripts that enable the automation of multi-step procedures. After that, we go to the Internet of Things and explain how a blockchain-IoT combo can: 1) makes it easier for devices to share resources and services, creating a marketplace for services; and 2) enables us to automate a number of laborious, current processes in a way that can be verified cryptographically. Additionally, we highlight a few concerns that need to be taken into account prior to implementing a blockchain network in an Internet of Things context, ranging from transaction privacy to the anticipated worth of the digital assets transacted on the network. We provide workarounds and solutions when appropriate. We conclude that the marriage of blockchain and IoT is strong and has the potential to significantly disrupt a number of sectors, opening the door for new business models and creative distributed applications.

D. Bruneo, S. Distefano, F. Longo, G. Merlino, A. Puliafito, V. D'Amico, M. Sapienza, and G. Torrisi [2] According to fog computing, computer logic will be shifted to the edge of the Internet, where choices, actions, and data processing must happen rapidly. It may not be very effective to transfer all of the application load to the cloud, especially when there are spikes in demand. This is particularly true in the context of IoT and Smart Cities, where thousands of smart devices, including cars, phones, and people, communicate with one another to provide cutting-edge services. Thus, we created Stack4Things as an Open Stack-based architecture that spans the levels of Platform-as-a-Service and Infrastructure-as-a-Service. Through the implementation of a

provisioning model for Cyber-Physical Systems, it allows developers and users to remotely operate nodes, virtualize their functions, and create network overlays among them, all while managing an Internet of Things infrastructure. Additionally, it offers tools to distribute the application logic among the many smart objects involved and to precisely choose which particular duties to assign to centralized cloud infrastructure. The main Stack4Things techniques that create a fog computing approach toward a run-time "rewireable" Smart City paradigm are shown in this work. We demonstrate its efficacy in a smart mobility scenario where end users get extremely responsive geolocalized services from automobiles interacting with smart objects at the city level.

D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das [3] In addition to completely changing the banking sector, the introduction of the blockchain as the basis for the first decentralized cryptocurrency in 2008 allowed for peer-to-peer (P2P) information exchange that was very safe, effective, and transparent. The blockchain is a publicly accessible ledger that functions similarly to a log by recording every transaction in chronological order, giving an immutable record, and being safeguarded by a suitable consensus technique. Immutability, irreversibility, decentralization, persistence, and anonymity are some of its remarkable qualities.

3. Existing System:

Blockchain is a technology that is rapidly gaining traction for a variety of uses. It may be thought of as a necklace, where each bead represents a record of an activity and the chain itself cannot be broken. As a result, the blockchain serves as an unbreakable digital transaction record. 76360 VOLUME 11, 2023 is revolutionized by this technology. In A. E. Bekkali et al.'s Blockchain-Based Architecture and Framework for Cybersecure Smart Cities, we discuss the ethical principles guiding the use of cryptography in data transmission. It provides a decentralized, transparent, and safe database that facilitates the exchange of any kind of data, including messages, products, and values. It permits building a database whose legitimacy the community can attest to. Digital assets are decentralized, enabling public access in real time, and dispersed, enabling the development of an unchangeable record of an asset. Blockchain will emerge as everyone's preferred technology and a decentralized worldwide source of trust [14], [15]. The three main components of the blockchain are as follows: the blocks that transactions provide. These blocks may be identified based on the quantity of data they contain thanks to a special code known as a "hash." The second component is the nodes, which stand in for the computers linked to the blockchain. These nodes store a copy of the database, which is downloaded immediately upon network connection and contains and permits all user trades. The last component is the miners, who play a crucial part in the blockchain by ensuring that newly generated blocks adhere to security guidelines. Thus, the legitimacy of the blocks and the chain as a whole may be guaranteed thanks to these miners.

4. Proposed System

The Blockchain is a highly competitive data transfer technology that can address a wide range of contemporary problems. By reclaiming personal data that would no longer be in the hands of middlemen, the implementation of blockchain technology in smart cities would enable more regulated government [36]. It provides the option to securely, traceably, and encrypt data transmissions while preserving anonymity. Additionally, it makes it possible to obtain real-time data on a variety of services, including energy, waste management, mobility (vehicles utilized, routes traveled, etc.), and trash management [1] [3]. It also enables the optimization of the connectivity of all the services provided in the Smart City. Additionally, blockchain technology may help Smart Cities accomplish a number of goals [9]:

- Simple and safe data transfer.
- Fostering cooperation amongst public authorities.
- To have a unified perspective of the supply chains in the Smart City.
- To curb fraud and expedite the verification of financial transactions.
- To design supply networks that are more intelligent and effective.
- To streamline procedures for resolving discrepancies in data for audit and legal compliance.

- To control population increase, urbanization, and energy use.

5. List Of Modules

- Service Provider
- View and Authorize Users
- Remote User

5.1 Module Description

5.1.1 Service Provider

The Service Provider must provide a valid user name and password to log in to this module. He can do some tasks after logging in successfully, such browsing insurance claim datasets and training and testing data sets. See the results of the trained and tested accuracy, the trained and tested accuracy in a bar chart, the predicted fraud in health insurance, the fraud in health insurance ratio, Acquire Forecasted Data Sets, View All Remote Users, View Fraud In Health Insurance Ratio Results,

5.1.2 View and Authorize Users

The administrator may see a list of all enrolled users in this module. In this, the administrator may see user information such name, email address, and address, and they can also approve people.

5.1.3 Remote User

There are n numbers of users present in this module. Prior to beginning any actions, the user must register. The user's information is saved in the database when they register. Upon successful registration, he must use his permitted user name and password to log in. Upon successful login, the user may do several actions such as registering and logging in, predicting fraud in health insurance status, and seeing their profile.

6. System Architecture

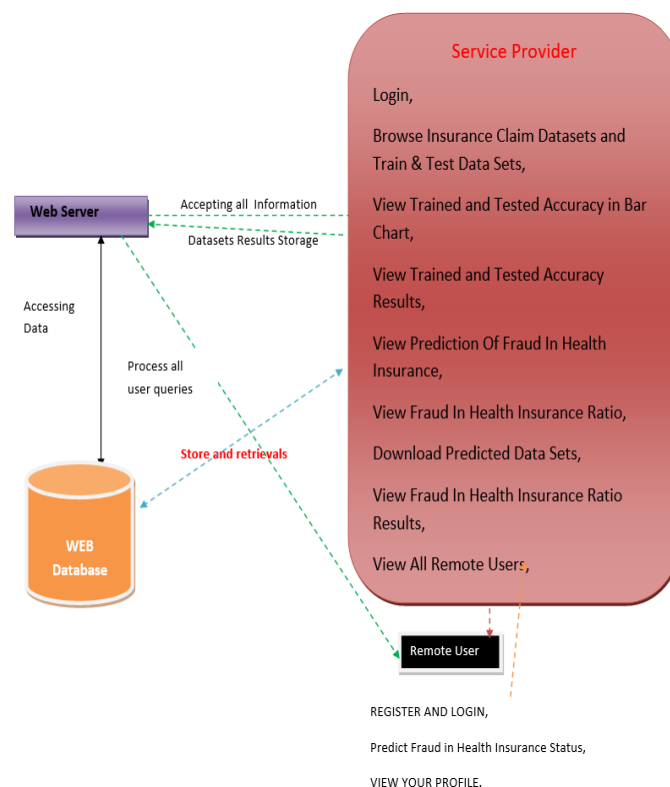
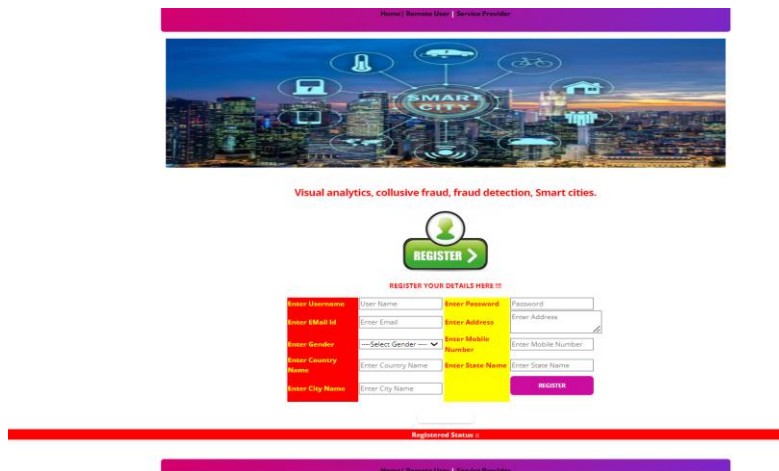


Fig.6.1 Architecture

7. Output Results



Home | Remote User | Service Provider

Visual analytics, collusive fraud, fraud detection, Smart cities.

REGISTER

REGISTER YOUR DETAILS HERE !!!

Enter Username	User Name	Enter Password	Password
Enter Email Id	Enter Email	Enter Address	Enter Address
Enter Gender	Select Gender	Enter Mobile Number	Enter Mobile Number
Enter Country Name	Enter Country Name	Enter State Name	Enter State Name
Enter City Name	Enter City Name		

REGISTER

Registered Status

Fig.7.1 User Registration page



Home | Remote User | Service Provider

Visual analytics, collusive fraud, fraud detection, Smart cities.

Login

Login Using Your Account:

User Name

Password

LOGIN

Fig.7.2.User Login page



Predict Fraud In Cyber Secure Smart City Status | View Your Profile | Logout

PREDICTION OF FRAUD IN CYBERSECURE SMART CITIES

ENTER DATASETS DETAILS HERE !!!

Enter RID	192.229.163.180-10.42.8	Enter city	Tokyo
Enter city_ascii	Tokyo	Enter lat	35.6897
Enter lon	139.6922	Enter country	Japan
Enter iso2	JP	Enter iso3	JPN
Enter admin_name	TA-kyō	Enter capital	primary
Enter population	37977000		

Predict

Fig.7.3.This is the user page to predict the data. These are the parameters it will take from dataset

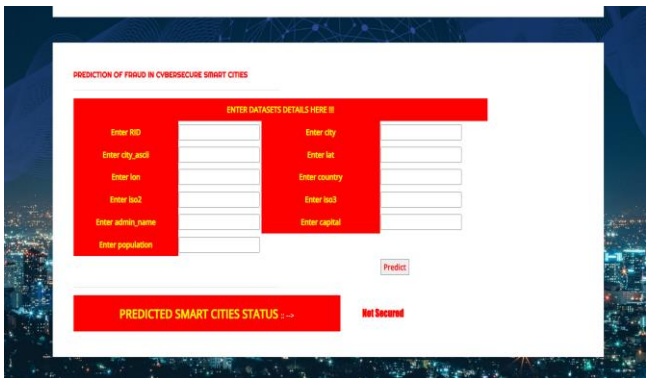


Fig.7.4. And it will predicted the results



Fig.7.5. this is the Admin login page



Fig.7.6. this is the admin page. These are the algorithms we have used in this project

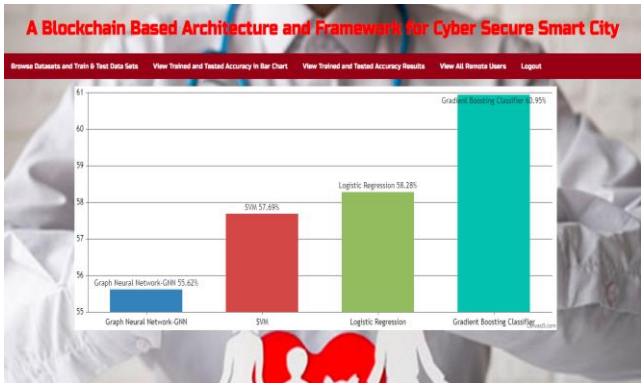


Fig.7.7. the algorithms are represented in bar chat

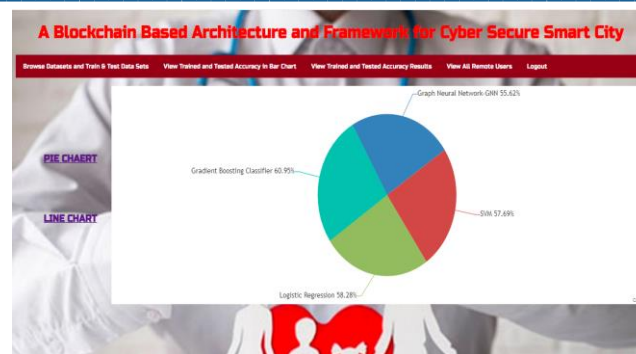


Fig.7.8. the algorithms are represented in pie chat

8. Conclusion

We provide a thorough and effective method for enhancing cyber security in smart cities in this project. This method provides a strong and dependable foundation for data security and privacy in smart cities by using blockchain, big data, and artificial intelligence algorithms. This framework's dependability and efficiency were shown using an actual smart grid dataset. Our method makes it possible to provide a safe environment for smart cities, their infrastructures, and services while enhancing their resistance to cyberattacks by concentrating on data confidentiality, integrity, and availability. Furthermore, this strategy increases public confidence and involvement with smart city apps and services while cultivating mutual trust between smart city stakeholders.

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. Elgandy, 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] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.
- [12] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, p. 1788, Apr. 2019.

- [13] D. Bruneo, S. Distefano, F. Longo, G. Merlino, A. Puliafito, V. D'Amico, M. Sapienza, and G. Torrisi, "Stack4Things as a fog computing platform for smart city applications," in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), San Francisco, CA, USA, Apr. 2016, pp. 848–853, doi: 10.1109/INFCOMW.2016.7562195.
- [14] N. Deepa, "A survey on blockchain for big data: Approaches, opportunities, and future directions," Future Gener. Comput. Syst., vol. 131, p. 209 226, juin 2022, doi: 10.1016/j.future.2022.01.017.
- [15] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges," Internet Things, vol. 8, Dec. 2019, Art. no. 100107, doi: 10.1016/j.iot.2019.100107.