PROJECT REPORT

On

Blockchain Based Secure IoT Networks for Smart Cities

Submitted in Partial Fulfillment of Award of

BACHELOR OF TECHNOLOGY
In
Computer Science and Engineering in Cybersecurity

By

Richard Roy - 2022BCSE07AED772

Karthik Rakesh – 2022BCSE07AED775

Joel Kochukunju – 2022BCSE07AED780

Under the Supervision of

Dr. Viji C, Associate Professor, Computer Science Engineering

ALLIANCE SCHOOL OF ADVANCED COMPUTING
ALLIANCE UNIVERSITY
BENGALURU

NOVEMBER 2025

COMPUTER SCIENCE AND ENGINEERING (CYBERSECURITY)

ALLIANCE SCHOOL OF ADVANCED COMPUTING

CERTIFICATE

This is to certify that the project work entitled **"Blockchain based secure IOT networks for smart cities"** submitted by **Richard Roy** [2022BCSE07AED772], **Karthik Rakesh** [2022BCSE07AED775] and **Joel Kochukunju** [2022BCSE07AED780] in partial fulfillment for the award of the degree of Bachelor of Technology in Computer Science Engineering of Alliance University, is a bonafide work accomplished under our supervision and guidance during the academic year 2025-2026. This thesis report embodies the results of original work and studies conducted by students and the contents do not form the basis for the award of any other degree to the candidate or anybody else.

Dr. Viji C	**K Ramalakhmi**
Associate Professor	HOD & Director COE
(Supervisor)	(Head of Department)
	All Specializations

External Examiners

SL. No.	Name	Signature
1.		
2.		

COMPUTER SCIENCE AND ENGINEERING (CYBERSECURITY)

ALLIANCE SCHOOL OF ADVANCED COMPUTING

DECLARATION

We hereby declare that the project entitled **"Blockchain based secure IOT networks for smart cities"** submitted by us in the partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science Engineering of ASAC, Alliance University, is a record of our work carried under the supervision and guidance of Dr. Viji C, Associate Professor.

We confirm that this report truly represents the work undertaken as a part of our project. This work is not a replication of work done previously by any other person. We also confirm that the contents of the report and the views contained therein have been discussed and deliberated with the faculty guide.

STUDENT NAME	REGISTRATION No.	SIGNATURE
Richard Roy	2022BCSE07AED772	
Karthik Rakesh	2022BCSE07AED775	
Joel Kochukunju	2022BCSE07AED780	

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all those who supported and guided me throughout the completion of this project. This final year project has been a significant learning experience, and I am deeply thankful to everyone who contributed to its success.

First and foremost, I extend my heartfelt thanks to my project guide, **Dr. Viji C,** for their invaluable guidance, constant support, and insightful feedback at every stage of this project. Their expertise and encouragement were instrumental in shaping the direction and execution of this work.

I am also grateful to the Dy. Director, **Dr. V. Vivek** for his leadership and for fostering an academic environment that encourages innovation and learning. Additionally, I would like to thank the Head of Department, **Dr. K Ramalakshmi,** Program Co- ordinators and all the faculty members of the **Computer Science Engineering** department at **Alliance University** for providing a supportive learning environment and necessary resources.

A special note of thanks to my teammates and friends for their collaboration, ideas, and motivation during challenging times. I also appreciate the support and encouragement from my family, who have always been a source of strength and inspiration.

Lastly, I would like to acknowledge all the authors and researchers whose work I referred to while carrying out this project.

Richard Roy	2022BCSE07AED772
Karthik Rakesh	2022BCSE07AED775
Joel Kochukunju	2022BCSE07AED780

PREFACE

The diffusion of digital technologies into the infrastructural setting of urban space has enhanced the evolution of smart city paradigm, i.e. Internet of Things (IoT) enables smooth device-to-device, device-to-system, and citizen-centered communication. As such networks continue to grow in size, the need to ensure a high standard of security and trust management also increases, thus hindering the sustainability of innovation and dependability. This project recognizes this need and examines the ways the blockchain technology can be combined with IoT to design and implement a decentralized, energy-saving system that ensures communication protection in the environment of smart cities.

The report gives extensive research regarding the design and development of solutions to the critical issues associated with network security, privacy and scalability within the IoT environments. It suggests a hybrid architecture, which is a combination of the Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) consensus mechanisms, further reinforced with advanced cryptography and AI-based anomaly detection sequences to allow autonomous threat mitigation. This strategy is proven to be effective with the help of hardware prototypes and performance analysis and provides an overview of future upgrades in resilient smart city systems.

This effort is owed to the shared direction and resources that have aided in the pursuit of this report, and the report hopes to bring something of value and practical solutions to the developing area of urban technological transformation.

ABSTRACT

The structured process of integrating the Internet of Things (IoT) into the smart city structures has made the interconnectivity more feasible but has also created significant security and privacy issues. Centralized security designs which do not scale are characterized by latency limitations and do not provide the required scalability, making them inappropriate in heterogeneous and large-scale IoT environments of modern cities. In this paper, a secure communication system based on blockchain technology has been outlined, with AI-assisted anomaly detection performed to promote confidence and resilience in the IoT-based smart city systems. The two-tier blockchain system proposed utilizes Proof-of-Authority (PoA) on the end-device level to support the process of lightweight verification and Practical Byzantine Fault Tolerance (PBFT) on the city level to enable high-quality consensus. Advanced cryptographic protection mechanisms such as combining elliptic-curve cryptography with AES-256 encryption deliver a high level of security in terms of authenticity and confidentiality and introduce minimal computational burden on network nodes. Threat intelligence supported by AI facilitates real-time detection and mitigation of abnormal network behavior that supplements autonomous defense. The tenfold simulation of performance appraisals with Raspberry Pi nodes and federated learning-inspired architectures show that there is less latency, higher detection rates, and minimal computational overhead, which makes the whole structure of IoT communication secure, adaptable, and scalable to serve the smart cities of tomorrow.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND SYMBOLS

IoT	Internet of Things
PoA	Proof of Authority
UDP	User Datagram Protocol
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
AES	Advanced Encryption System
DoS	Denial of Service
DDoS	Distributed Denial of Service

TABLE OF CONTENTS

CHAPTER - 1

INTRODUCTION

Modern digital technologies have resulted in modern infrastructures where many interconnected smart technologies come together to increase efficiency, safety, and sustainability. The Internet of Things (IoT) is a key aspect of this development and it connects devices, sensors and platforms to enable the exchange of data and automated processes. Nevertheless, with the spread of IoT, it faces ubiquitous threats, namely, security, privacy, and scalability. Traditional systems are also susceptible such as when one system fails or is breached by a malicious attacker, and it affects the whole network. It has been proposed that blockchain technology has been used as a solution with mitigatory value, offering a decentralized paradigm with tamper-restraint, which guarantees trust, transparency, and integrity during the processing of transactions by IoT.

1.1 INTRODUCTION TO BLOCKCHAIN BASED IoT NETWORKS

IoT networks based on blockchain combine decentralized blockchain ledger features with the connectivity provided by IoT devices. Such symbiosis improves the level of data security, checks the integrity of inter-device communication, and eliminates the necessity of centralised control. Information sent via central servers can be lost, attacked and inflexible; on the contrary, blockchain stores user transactions in a common and irrevocable registry. This results in the creation of trust and accountability between the devices despite the lack of inter- device trust. PoA and Practical Byzantine Fault Tolerance (PBFT) are used to support fast and reliable interaction, and smart contracts allow the exchange of validated information automatically, which makes the IoT systems self-managed in the context of healthcare, manufacturing, and logistics.

1.2 INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Blockchain is a decentralised distributed system that distributes information over various nodes. Transactions, a time, and a cryptographic hash are contained in each block and connect it to the previous block, which makes it virtually impossible to modify historical data. The fundamental features of blockchain are the permanence of data, common control, openness and shared consensus. It guarantees integrity of the data within the system with all users possessing the same copy. In the context of the IoT, blockchain provides a level of trust where the interactions between devices are logically documented; smart contracts allow the device to independently perform tasks as required once the predefined conditions are met. Consensus algorithms that consume less energy also make blockchain useful to low-power IoT-based devices, like sensors.

1.3 INTRODUCTION TO INTERNET OF THINGS (IoT)

Internet of things (IoT) is a set of interconnected devices that have sensors, controls and communication modules, which collect and transfer data via the internet. Examples are smart meters, cameras and traffic sensors that enable the real world system automation and optimisation. The IoT has wide applications in automated control and early fault detection as well as data-based decision making. The integration of blockchain and IoT allows decentralizing the verification of any data, which increases the level of security, privacy, and trust without reducing efficiency. Edge computing also increases the utility of blockchain-IoT convergences in large-scale deployments in smart cities.

CHAPTER - 2
LITERATURE SURVEY

Urban infrastructures have become interconnected ecologies due to the fast development of IoT technologies over the recent years. This enhanced interconnectivity poses huge challenges in terms of security, privacy and trust. As a result, a number of blockchain-based approaches have been considered that can be utilised to enhance security in smart cities by making use of decentralisation, immutability, and cryptographic guarantees. The next section will discuss relevant literature in the area, discuss the methodologies, strengths and limitations to give a thorough understanding of the solutions available and be able to pinpoint the research gap that this study is going to fill.

2.1 LITERATURE REVIEW

S.No	Methodology	Performance Metrics	Disadvantages
1	The architecture substitutes central authorization with a blockchain system, hence allowing Internet of Things (IoT) nodes to communicate and authenticate safely. It makes use of cryptographic keys, the Vigenere cipher, and hash algorithm (SHA256) in an encrypted version of a Python implementation of VPN in Debian (except on 64-bit processors).	In configuration, the blockchain files within the nodes would initially be empty and they are only filled during synchronization. The UDP packet encryption would significantly increase the level of privacy, and the general scheme of the blockchain is effective regarding authentication.	However, the UDP protocol is also unsecured and prone to packet sniffing, there is also the issue of synchronization in case the nodes disconnect and reconnect. The comparatively weak Vigenere cipher also makes security weak, and updates of blockchain are susceptible to latency on restarting nodes.
2	The system takes the form of a multi-layered architecture that combines the IoT devices and a private Hyperledger Fabric blockchain and thus	Empirical findings suggest that all nodes consume little resources in terms of CPU usage, RAM usage, and network usage and that the time spent responding to	As the size of systems grows, Hyperledger Fabric is subject to more transaction latency and response times, which may negatively affect user

	provides a secure and transparent system of transport data. Users engage each other using graphical user interfaces and REST APIs, registration of devices is performed using Certificate Authority in fabrics, and privacy is protected by using multi-channel configurations. Hyperledger Caliper facilitates the achievement of performance optimization and its implementation is provided on Ubuntu with Docker and Node.js support.	individual transactions grows progressively with more users per node (220ms with 200 users to 460ms with 600 users) although the response time rates off at higher usage levels. In general, throughput, system and user presence remain reliable even with increasing concurrency.	experience in large networks. The deployment and configuration requires, and are still characterized by, heavy technical knowledge, and explorable security issues at the endpoint, trust of devices, and the difficulty of integration with the existing infrastructure in smart cities.
3	LightGBM is used to detect intrusion accurately with a minimal amount of LightGBM to support the architecture, which attempts to use elliptic-curve cryptography (ECC) and principal component analysis (PCA)-based privacy to achieve IoT data authentication and transfer. It works on a built-in system of blockchain-IPFS integrated fog-and-cloud network, which transfers intensive calculations off-the-shelf off the IoT and grants secure registration and management of devices	As IoT devices and transactions evolve, the processing time and IPFS storage requirement are growing yet they are scalable due to the off-chain layer design; meanwhile, the Ethereum prices of gas directly correlate with the volume of transactions. The LightGBM-based intrusion detection system achieves good performance which is 98.38 per cent, 95.32 per cent, 94.35 per cent and 94.80 per cent accuracy, precision, recall and F1 score respectively, and	The system also faces high costs in computational costs posed by the increased Proof-of-Work and cryptographic functions and performs poorly as the number of IoT devices and transactions grow. Its multi-stage and expensive authentication and fog-cloud connectivity require stringent secure key and trusted-parties management in order to prevent single points of failures when on boarding the device.

	through a Trusted Party.	outperforms several traditional classifiers in the ToN-IoT and BoT-IoT datasets.	
4	The architecture suggested has integrated IoT nodes, cognitive base stations as well as a fusion center execution coordinated by a blockchain which will utilize encryption to provide safe communication. The fusion center actively chooses credible nodes by measuring trust and energy, and adaptive smart contracts are used to distribute spectrum and energy, thus, decentralizing energy trading and optimizing security and energy efficiency because of trust-based organization and energy efficiency by the use of spectrum sensing.	The detection probability, false alarm probability, missed detection probability, sensing performance gain, total error probability, number of selected sensing nodes, average network performance and energy efficiency are the key performance metrics.	The overheads of computation and communication of low-power IoT devices can be increased with blockchain consensus mechanisms and cryptography. The ability to scale smart cities to large systems has to be further verified. The need to have constant improvement to gain transaction validation, resist collusion attack, and avoid fraud in trading of energy requires continuous enhancement. Also, integration problems with prevailing wireless standards (5G, LPWAN) should be considered.
5	The continual updates of the firmware implementation is developed then persisted using blockchain smart-contracts, maintaining an unalterable audit trail and broadcasting the encrypted updates to the endpoint devices via the management nodes. The system uses dynamic cryptography	Integrity check To verify the integrity, the consistent application of monitoring messages on the blockchain is used with variable intervals that manage the trade off between the latency and resource usage. The system has resilience against various attacks, has transparency and	Although with lightweight optimisations lightweight devices witness escalated computation overflow and latency caused by the blockchain consensus. Handling of multiple cryptographic keys and the reliance on trusted nodes to achieve secure onboarding has brought a

	protocols and proof-of-stake consensus to loop-achieve optimised security and energy efficiency, by means of heterogeneous per-capability device capacity.	auditability through extensive history of immutable logs, and scales protocols to the capabilities of various devices to reduce cryptographic overhead.	problem of scalability to scaling up heterogeneous networks.
6	Blockchain protocols, permissioned ledgers and consensus mechanisms by the system secure data on physical, communication, database and interface layers to overcome attacks and guarantee integrity and privacy during real-time smart application.	The blockchain decentralisation, use of the private ledges to provide scalability, and the secure confirmation of transactions via the majority voting ensures the resilience of smart-city security threats, whereas the real-time performance is supported with integrated communication devices and optimisation of blockchains.	Nevertheless, achieving the combination of blockchain and various communication standards is complicated, and open ledgers will be lost in favor of performance. The lack of standardisation in communication is a considerable barrier to adoption, scalability, interoperability with existing systems, and cryptographic overhead on the limited IoT devices.
7	Participant anonymity is ensured with SHA 256 hashed identifiers, secure enrollment expects hashed passwords, one-time passwords and multi step checkups. AES-128 encryption and Chebyshev poly interpolation increase the level of data confidentiality, which is backed up by the multi-level authentication process and encrypted and verified data exchange through the	The system of SecPrivPreserve exhibits both effective authentication and data processing with the time to compute growing slightly between 50 and 62 seconds with an increase in the number of users between 100 to 500. Similarity scores are increased to 0.88, and the legitimate user verification rates are increased to 90 percent and low latency and high	Handling of multiple cryptography operations and processes makes the design more complicated and the overhead higher; the current assessment is mainly based on simulation and the actual implementation is still to come. The permissioned blockchain must also be administered by trusted parties, which somewhat limits the aspect of decentralisation, and an

	blockchain by the use of smart contracts.	request acceptance are maintained at increasing loads.	increment in the number of users may lead to an increase in the number of computations hence the optimization of fog/cloud homogenisation is needed in future.
8	The current paper presents a stack architecture of a blockchain platform based on Internet of Things (IoT) systems, including physical, data, network, consensus, incentive, smart contract, and application layers. This architecture is synergistically linked with the cloud computing and artificial intelligence modalities. Authentication and privacy is achieved by implementing smart contracts and fog-edge cloud is used to notify the computing loads on resource-constrained IoT endpoints, which enhances energy efficiency.	In turn, the suggested setup will help reduce energy usage, increase the security and privacy capabilities, and enable scalable and efficient management of large IoT data streams. It also incorporates incentive systems that facilitate blockchain mining.	Nevertheless, the architecture can be characterized by considerable computational and bandwidth requirements that can be attributed to AI and blockchain functionality, which increases the energy usage and raises the development of possible environmental implications. IoT in resources constrained can consider only the integration of blockchain and AI layers to be prohibitively expensive, and scalability in ultra large smart cities deployments remains a daunting challenge.
9	The framework suggests a combination of IoT information acquisition, the transparency of nodes protected by an immutable blockchain and computed at the edges to obtain fast data	Some such key performance measures will be the length of the queue, variance between the actual and expected arrival times of packet, end-to-end latency, average resource	As the scope of the IoT data and blockchain transactions grows, scaling issues become apparent due to high initial costs and the additional expenses of operation, the

	processing. It integrates a service controller that is controlled by a received optimization of queuing model that is calibrated through the RFpo algorithm of resource allocation and scheduling. At the same time, secure automated supply-chain management capabilities are built upon smart contracts running on Hyperledger Fabric.	usage, and the exact arrival times. Also, the study determines the convergence of cost-functions and compares the suggested methodology to other proposed blockchain and optimization algorithms.	complexity of interoperability between the heterogeneous platforms, and the latency caused by the consensus mechanisms and the massive volume of data.
10	By recording authenticated IoTs communicate to the Gateway and running anomaly detection and traffic analysis, Gateways secure the blockchain ledger. Regularly updating this data to a cloud-based blockchain allows carrying out massive analytics, making it possible to identify the threat in real time and carry out operational indicators of actions in response to it. Besides, IoT services are automated on Ethereum-based smart contracts, which control them and enforce them decently.	Security and privacy protection are reinforced by features helpful to withstand data manipulation and computer attacks. Scalability of the network that is provided by the decentralized deployment is also reviewed. Trustworthiness validation processes such as authentication, authorization and anomaly checking are outlined. As well, transaction latency and throughput of various consensus mechanisms are measured.	The public blockchain platforms are not only affected by latency and low throughput but also consumes a significant amount of energy, thus limiting the use of IoT devices that are constrained by resources. Smart contracts can fall prey to code bugs, require trusted oracles, and there is a problem of interoperability and privacy, which makes their widespread applications in the real world unfeasible.

Table 2.1 Literature Survey

2.2 LIMITATIONS OF THE EXISTING SYSTEM

Despite the existence of a rather large field of research on the implementation of blockchain technology and the Internet of Things (IoT) into the context of smart cities, the currently existing systems have vital problems with scalability and performance. First, blockchain applications rely on any form of consensus mechanism, such as Proof of Work or Proof of Stake, which puts a considerable burden of computation and communication upon its resources which are not highly compatible with the constraints of the IoT ecosystem. According to this, the greater the number of linked devices the longer the time to authenticate the transaction and then push it out to the network and acute bottlenecks develop under the latency and throughput. Weaknesses of such scale cannot support real-time responsiveness, which applications such as traffic monitoring or emergency response, such as using communication with low latency require. Moreover, the need to maintain complete blockchain records introduces prohibitive overheads to the IoT nodes with bandwidth and storage constraints, hence requiring attention into lightweight or selective ledger duplication.

The other shortcoming has to do with the interoperability and heterogeneity of the IoT devices and platforms too. Smart-city systems are not only complex systems but also contain numerous sensors, actuators and communication technologies so that their computational requirements and security needs can differ. The existing blockchain-based solutions have a low probability of helping this diversity but offer generic architectures that do not best integrate with legacy infrastructures or cross-domain services. The resultant interoperability trade-off undermines a consistent policy implementation as well as access control in the absence of a standard structure of data communication between the vendors. Moreover, most of the current systems that rely on fixed trust configurations cannot support dynamic network behaviour or mobile nodes and hence introduce inconsistency in trust as well as vulnerability of multi-domain environment.

Other than scalability and interoperability, energy efficiency, privacy protection, and complexity of implementation, are also major barriers to practical implementation. Cryptographic operations, smart-contract functioning and validation of consent usage in the IoT consume a great deal of energy and cannot run on battery-powered devices. Despite the fact that the operation of privacy-preservation mechanisms is of vital importance in securing sensitive information of the citizens, additional latencies and storage costs are commonly

introduced, and, therefore, diminish the overall system performance. Most blockchain -IoT prototypes are not tested on large scale, but under a controlled environment, which casts their effectiveness and reliability in a large-scale smart city setting in doubt. All this shows the necessity to possess lightweight and versatile and scalable blockchain architectures capable of achieving the optimal balance between security, energy efficiency and interoperability in the heterogeneous IoT context.

2.3 SCOPE OF THE PROJECT

The proposed project defines a secure, scalable and energy-efficient blockchain system that is specifically implemented to be operated by the IoT-inspired smart-city applications. In contrast to modern, centralized, resource-sensitive designs, the design has lightweight consensus engines, adaptive authentication patterns, and a meeting on-chain off-chain data-management paradigm. These architectural choices are aimed at ensuring the end-to-end data integrity, ensuring communication between the devices, as well as ensuring strong trust management among the heterogeneous IoT entities. Access control and data validation and event-driven operations are automated, and transparent, and thus enhance the efficiency of municipal operations, such as traffic control, energy distribution, and environmental monitoring with the implementation of smart contracts.

Besides the cybersecurity, scalability, interoperability and real-time responsiveness, the project also deals with the different infrastructures that exist in the urban setting. Strong consensus check is to ensure that latency is minimised and bandwidth used better whereas edge/mog computing is integrated within blockchain systems. The modular structure permits the expansion in various municipal areas, which encourages the seamless interoperation between the government agencies, service providers, and IoT stakeholders. Therefore, the project would not be confined to the stage of theoretical modelling, but rather offer a sustainable and secure blockchain-IoT architecture that can withstand the scale of business demands that would be associated with smart-city projects.

CHAPTER 3
SYSTEM DESIGN

The system design presents the principles that shall be applied in the realisation of a blockchain-based secure IoT network in smart cities. It is also aware of the divide that exists between the theory and practice and endeavours to provide a solution that is secure, efficient, and decentralised communication between the devices. By using a hybrid blockchain architecture, the architecture is integrated using lightweight algorithms, where cryptographic security is provided. Within this section, the problem definition, system architecture and specifications required will be described and will be used to carry out the subsequent implementation.

3.1 PROBLEM DEFINITION

City smart-free devices respond to diverse areas of traffic control, energy management, and environmental surveillance through the generation of incredible amounts of data. Although they are essential, the systems are faced with massive challenges such as security risks, lack of trusts, inflexibility and excessive consumption of power. In most cases, IoT ecosystems are based on centralised identity validation and identity identification, which comprise single points of failure that increase the potential of data misuse and unauthorised consumption.

The suggested project uses hybrid blockchain architecture that consists of two levels of Proof-of-Authority (PoA) to validate lightweight devices and Practical Byzantine Fault Tolerance (PBFT) to find a consensus on a city-wide level. Through these mechanisms, encrypted communication, authentication, and threat detection are enabled with artificial intelligence support to increase the security, reliability, and scalability of resource-constrained IoT platforms.

3.2 SYSTEM ARCHITECTURE

The system will be subdivided into two great layers. The first layer is called the device layer. The lower layer embraces IoT devices e.g. sensors, gateways, actuators, which use the PoA to verify only the trusted devices, which conserves power and enhances communication. Secure DTLS over UDP used in communication with devices is compatible with IEEE 802.15.4.

The second layer is called the city layer. The top layer consolidates and authenticates information of clusters of equipment, integrating a secure and acceptable majority using PBFT. Also, AI can assist in threat detection based on federated learning where anomalies can be identified and separated in real time.

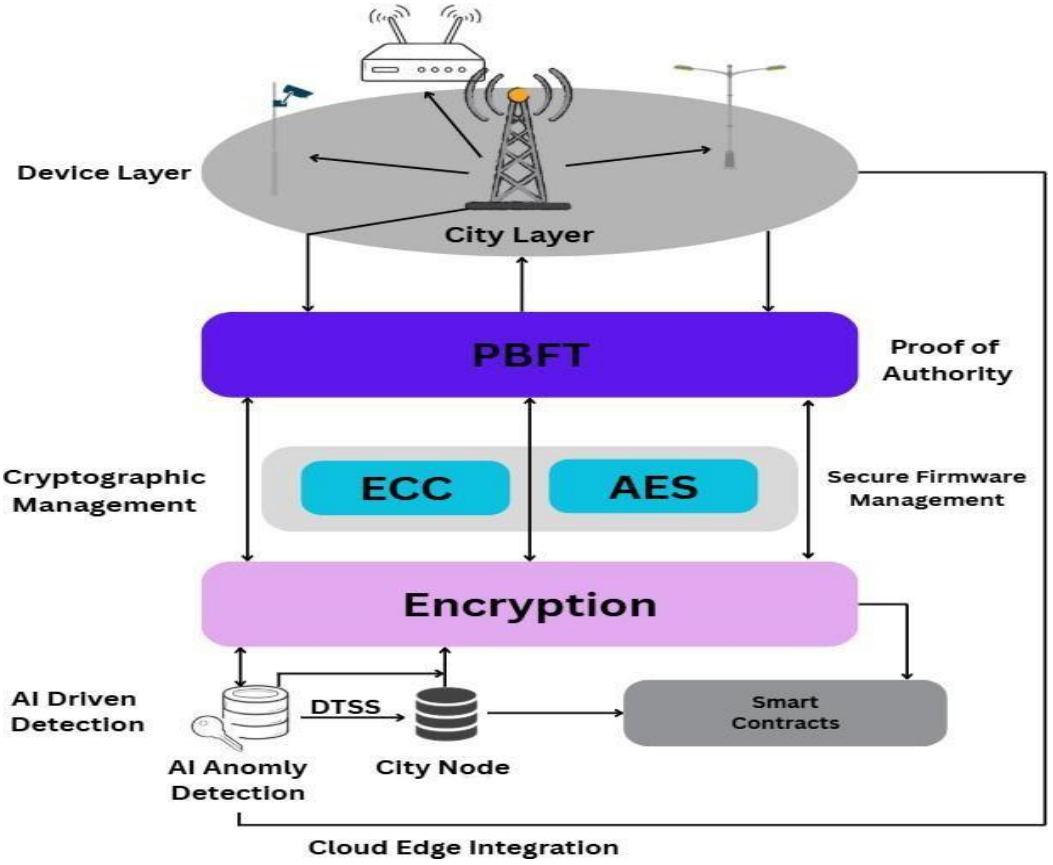

Figure 3.1 System Architecture

3.3 REQUIREMENT SPECIFICATIONS

1. Hardware Requirements

The processing unit of the system is a modern raspberry-pi, which can be used instead of model B or similar board. It has 4GB RAM to support city nodes and 1GB RAM to support device nodes, which provides an effective performance in various layers. Blockchain artifacts and datasets are stored in a 32GB SD card. Network connectivity is achieved using IEEE 802.15.4 (Zigbee) or Wi-Fi 802.11 to communicate with different devices and use Ethernet

or Gigabit LAN (Zigbee city) to connect the network nodes in the city. It uses a wide range of sensors, which are motion sensors, environmental sensors, humidity sensors, and temperature sensors, and is powered by a 3A 5V power backup to maintain continuous operation.

2. Software Requirements

The system runs on the Debian 11 operating system used on the nodes of the IoT system and Ubuntu 20.04 LTS used on the nodes of the server system, which offers a stable and healthy operating environment. The blockchain is developed based on Hyperledger Fabric 2.2 (PBFT) and a Proof-of-Authority (PoA) module developed in Python and implemented by Web Protocol. Python 3.10 is used in the implementation of blockchain logic, whereas Go has been used in the implementation of smart contracts. CouchDB or LevelDB is used as a database behind which the data management is performed. In the case of AI-based federated anomaly detection, the system uses TensorFlow Lite or PyTorch Edge, which is efficient in on-device training. Docker is used to package the deployment and communication environment and the integration and communication among system components is carried out using the Node.js.

CHAPTER 4

SYSTEM IMPLEMENTATION

The implementation stage puts the conceptual design into action and delivers the system of smart cities into a working blockchain-based Internet of Things. It includes hardware implementation, network setup, encryption implementation, implementation of blockchain protocols, and implementation of AI-advanced security procedures. The system has been built in a modular style, hence providing flexibility, scalability, low power consumption, and using structure that is highly secure.

4.1 OVERVIEW OF THE MODULES

The system is organized in two major modules. Module 1: Device-Level Blockchain Node uses a Proof-of-Authority (PoA) protocol that is based on lightweight implementation suitable to IoT devices, which allows to communicate with encrypted data, verify data authenticity, and store blockchain locally to provide efficiency and security at the device level. Module 2: City-Level Blockchain and AI Security manages the Practical Byzantine Fault Tolerance (PBFT) consensus of the city nodes and incorporates the AI-based anomaly detection using federated learning. This module provides secure data validation, automated response to threats with smart contracts, and stability of the whole network. The two modules will communicate safely and in an asynchronous manner, reducing the latency and ensuring high privacy levels within the entire system.

APPENDICES

Appendix A

Blockchain based secure IOT networks for smart cities.

Dr.C.Viji, Associate Professor
Dept of Computer Science and Engineering
Alliance School of Advanced Computing,
Alliance University,Bangalore , India
Viji.c@alliance.edu.in

Richard Roy
Dept of Computer Science and Engineering
Alliance School of Advanced Computing
Alliance University, Bengaluru, India
rrichardbtech22@ced.allaince.edu.in

Karthik Rakesh
Dept of Computer Science and Engineering
Alliance School of Advanced Computing
Alliance University, Bengaluru,, India
rakarthikbtech22@ced.allaince.edu.in

Joel Kochukunju
Dept of Computer Science and Engineering
Alliance School of Advanced Computing
Alliance University, Bengaluru, India
kjoelbtech22@ced.allaince.edu.in

Abstract: Accelerated Internet of Things (IoT) deployment in smart cities has facilitated increased interconnectivity while introducing severe security and privacy risks. Scalable security measures based on centralized schemes suffer from latency and scalability issues and hence are inadequate to cater to large and heterogeneous IoT campuses. In this paper, we introduce a blockchain-based secure communication framework incorporating AI-assisted anomaly detection to improve confidence and resilience in IoT-based smart city infrastructures. A two-tier blockchain architecture using Proof-of-Authority (PoA) at the end device level to ensure lightweight verification and Practical Byzantine Fault Tolerance (PBFT) at the city level to ensure high-quality consensus is adopted in the proposed scheme. Advanced cryptographic measures that integrate elliptic curve cryptography (ECC) and AES-256 encryption ensure high authenticity and confidentiality efficiency with minimal computational power at the nodes. Incorporation of AI-assisted threat intelligence allows fast identification and elimination of network anomalies in real-time to enhance autonomous defense and mitigation capabilities. Simulation based performance analysis with Raspberry Pi nodes and federated learning-based models illustrate lower latency, high precision in anomaly detection, and minimal computational overhead in support of a secure, adaptive, and scalable IoT communication architecture in future-proof smart cities.

I. Introduction

These days the cities are becoming "SMART" because many things are connected through the internet,take for an example -Sensors, cameras, vehicles, and machines all send and receive data. This helps manage traffic, save energy, and improve public safety. But when everything

References & Bibliography

1. Ramazan Yetis and Ozgur Koray Sahingoz "Blockchain Based Secure Communication for IoT Devices in Smart Cities", IEEE, 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), 01 August 2019
2. Khizar Abbas, LoAi A. Tawalbeh, Ahsan Rafiq, Ammar Muthanna, Ibrahim A. Elgendy, Ahmed A. Abd El-Latif, "Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities ", Security and Communication Networks, Volume 2021, Article ID 5597679, 2021
3. Prabhat Kumar, Randhir Kumar, Gautam Srivastava, Govind P. Gupta, Rakesh Tripathi, Thippa Reddy Gadekallu, Neal N. Xiong, "PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities", IEEE, Transactions on Network Science and Engineering (Volume: 8, Issue: 3, 01 July-Sept. 2021)
4. Hamad Aldawsari, "A blockchain-based approach for secure energy-efficient IoT-based Wireless Sensor Networks for smart cities", Alexandria Engineering Journal, Volume 126, July 2025
5. Seonghyeon Gong, Erzhena Tcydenova, Jeonghoon Jo, Younghun Lee, Jong Hyuk Park, "Blockchain-Based Secure Device Management Framework for an Internet of Things Network in a Smart City", Sustainability 2019, 11(14), 3889, 27 May 2019
6. Kamanashis Biswas, Vallipuram Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology", 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 26 January 2017
7. Adla Padma, Mangayarkarasi Ramaiah, "Blockchain Based an Efficient and Secure Privacy Preserved Framework for Smart Cities", IEEE Access (Volume: 12), 07 February 2024
8. Imran Ahmed, Yulan Zhang, Gwanggil Jeon, Wenmin Lin, Mohammad R. Khosravi, Lianyong Qi, "A blockchain and artificial intelligence enabled smart IT framework for sustainable city", 16 February 2022
9. Ahmad Yahiya Ahmadad Bani Ahmad, Neha Verma, Nadia Mohamed Sarhan, Emad Mahrous Awwad, Amit Arora, Vincent Omollo Nyangaresi, "An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model", IEEE Access (Volume: 12), 18 March 2024

10. Rashid Ali, Yazdan Ahmad Qadri, Yousaf Bin Zikria, Fadi Al-Turjman, Byung-Seo Kim, Sung Won Kim, "A Blockchain Model for Trustworthiness in the Internet of Things (IoT)-Based Smart Cities.", Springer Nature Switzerland AG 2020, June 2020