International Journal of Engineering Innovation & Research
Volume 13, Issue 4, ISSN: 2277 – 5668

Integrating Smart Services in Smart Cities using Blockchain

Dr. Pradeep Chouksey, Dr. Praveen Sadotra, Mayank Chopra, Abhishek Sharma and Onkar Srivastava*
Department of Computer Science & Informatics, Central University Himachal Pradesh, India.
*Corresponding author email id: imonkar29@gmail.com

Date of publication (dd/mm/yyyy): 21/07/2024

Abstract **– The emergence of smart cities, once a visionary concept, has now become a tangible reality, elevating our living standards through the adoption of IoT, cloud computing, and advanced information and communication technology tools. However, this increasing reliance on technology has given rise to a surge in cyber threats, posing the risk of substantial data breaches and unprecedented economic losses for entire cities. To mitigate these risks, it is essential to explore and implement innovative technologies that can reduce the susceptibility to cyber-attacks and secure the storage of data in smart cities. Blockchain presents itself as a fitting alternative, providing a robust solution for safeguarding user data and fortifying the overall cyber security of smart cities. Blockchain based technologies such as BITS (Blockchain based Intelligent transportation system) and Block SIEM have been integrated into different sectors of smart city, ensuring safety of citizen data. Additionally, this study delves into the potential applications of blockchain across various facets of smart cities, including transportation, governance, and security. A transition toward more secure alternatives is imperative for the future trajectory of smart cities, ensuring our smart cities to be cyber secure.**

Keywords **– Blockchain, Cyber-Security, IOT (Internet of things), Smart City.**

I. INTRODUCTION

Since the advent of digitally driven era brought in the 21st century, there has been an ever-growing urge to connect different systems to improve the efficiency and convenience in our daily task. Government around the world have been making rapid strides in the race to provide its citizens at large scale a better living standard through technological advances.

Such a society having interconnected systems and smart delivery of goods and services has aptly led to such urban areas being termed as Smart Cities [1]. The term smart cities can include conveniently portrayed as a collection of interconnected network-based system. Some common examples of such systems are smart healthcare system and transportation system [1]. Such system has to be connected on a vast scale in a sophisticated manner as it is an indispensable factor towards the success of a smart city [1]. Several models of smart city implementation have emerged around the world. Singapore launched its smart nation program in 2014 where in it laid down extensive surveillance throughout its jurisdiction. This was done to collect data on crowd density, cleanliness of public spaces and keep track of illegal activities. Such vast amount of data helps the government in anticipating and preventing mishaps in public space and predicting spread of any diseases [15].

In Dubai, under the Smart Dubai Initiative more than 50 smart services has been rolled out to provide citizen the ease of paying bills, registering vehicle and filling complaints from the comfort of their homes [15]. While being engaged in these nations, making quick progress are taking in the race to make their cities Smart, it is not important to not compromise on the cyber threats that come with such tech dependent systems.

When different services in a city are integrated to collect data, enhance services, and improve people's lives, it

brings about connectivity. However, this connectivity also opens 'Smart Cities' to various cyber threats. The large amount of citizen data stored in these systems become vulnerable to theft, and the city's technology-dependent smart. Infrastructure becomes a critical target for security issues. Therefore, cyber security is rightly considered an essential factor for the implementation for the smart city.

Cyber-attacks usually aim to gain unauthorized access to, change, or destroy confidential data. Several levels of protection must be implemented across computers, networks, courses, and data that has to be protected as part of a strong cyber security strategy. To create a strong defence against cyber-attacks, an organization must ensure that people, procedures, and technology are all working together in harmony [2].

Cyber security threats in smart cities -

- IOT vulnerabilities.
- Data privacy concerns.
- Critical infrastructure risks.

In addition to this, Smart cities are exposed to a large number of cyber threats making citizen data vulnerable. A tiny error at individual level may cover the whole city's data at risk. Hence, making a smart city secure is essential for successfully realizing the concept of smart city. Protection of privacy and citizens' interactions with the government are additional concerns in addition to cyber security [3].

Main Building Block of Smart Cities:

- ICT - It is also known as Information and communication technology. It is used to enable smart buildings. It is used to provide enhanced quality of life to citizens, improved city resources utilization and better Sustainability [4].
- IOT - Also known as Internet of Things. Enables the detection and reporting of parameters pertaining to various municipal districts. Essential services such as healthcare, transport, waste management, agriculture etc. can be maintained using IOT [5].
- Cloud: - Cloud computing, which makes it possible to compute and store almost infinite amounts of data [6].
- Blockchain - Blockchain is a chain of blocks that keeps growing and can store all committed transactions using a public ledger. Every mining node sings and cryptographically verifies each transaction [7].

In this paper, we aim to study the components of a smart city and the cyber security threats that accompany them. We will also determine the cyber secure robustness of the smart systems and what can be done to improve them.

II. LITERATURE REVIEW

In [8] paper, to improve smart cities' security, the authors proposed a Blockchain based Intelligent Transportation System, or BITS. Coordinated attacks have the potential to alter data from cars and the transit system in smart cities. Furthermore, there can be bad actors attempting to alter the system or data to benefit themselves.

To ensure data availability, integrity, and immutability in the Intelligent Transportation System (ITS), the

authors suggested an architecture based on blockchain technology that includes outlier detection. This maintains the veracity of the information supplied while assisting in the prevention of dangerous vehicle actions. The proposed architecture can evaluate reputation based on input attributes and detect outliers in the BITS. The suggested approach seeks to better withstand abnormalities by fusing Blockchain technology, machine learning, and a distributed server configuration.

In [9] paper, authors have explained that smart city e-governance refers to the application of technology to enhance public service delivery by the government. It entails soliciting greater public involvement when formulating policy and making judgements. This promotes the government's transition to digital methods of operation and enhances governance. The e-Gov 2.0 smart city concept in India takes a broad approach to urban development and emphasizes the need of local self-government.

Globally, the number of smart cities is increasing, and they are addressing several issues including infrastructure, citizens, government, and the economy. Blockchain technology can enhance conventional business models by increasing traceability, security, and transparency. Information and communication technologies (ICT) includes e-governance. In smart cities, using blockchain for contracts improves efficiency. A blockchain-based smart city is not without its restrictions, though. It guarantees high integrity, but in the absence of an independent system to verify the data entering the blockchain, information dependability may be questionable. Blockchain is useful for e-governance in many areas, such as smart healthcare, energy trade, and electronic voting. It guarantees openness, confidence, and economic expansion by doing away with the need for middlemen. Blockchain has the potential to revolutionize supply chain and energy trading, bringing benefits to both private citizens and public institutions when integrated with smart cities. To put it simply, blockchain creates security, transparency, and trust between the public and the government. Additionally, it increases the automation of problem-solving and decision-making processes. The public participates more in decision-making.

In [10] paper, the authors talk about the problems with Internet of Things (IoT) devices. While these devices offer many useful services, making them popular also brings security risks. This is because there's not enough supervision, and these devices have limited computing resources. As more devices join an IoT network, the chances of a security breach increase. This could expose a lot of devices to attacks, turning them into a kind of army (botnet) that can launch large-scale attacks. An example is the Mirai attack, where around 50,000 IoT devices in 164 countries were infected and then used to carry out more attacks. To tackle these security issues, Block SIEM suggests a solution. It's a system that uses blockchain technology to securely detect, store, and analyze security events in IoT devices. This helps ensure that the information is trustworthy and cannot be denied or altered. Block SIEM can be used in different situations, providing a strong and reliable security system. By using blockchain, by controlling security events from IoT devices, it enhances the security of IoT ecosystems, preserving integrity and preventing denial. Block SIEM also has other good qualities like being resilient, trustworthy, auditable, and scalable, making it a robust security tool.

In [11] paper, Energy harvesting (EH) is a way to capture and use energy that is typically wasted in the environment. This energy is converted into usable power for devices that work on their own. For example, many items in a smart city are linked to the internet so they may communicate with each other or with people. In smart cities, web technology helps manage and access physical objects, making them "smart." However, a big

challenge is how to ensure that these connected devices always have the power they need to function. This is where energy harvesting comes in. Energy can be harvested from different sources like vibrations, sunlight, heat, wind, radio signals, and water, which are available in many places. This harvested energy can then be used to power the devices in the smart city. This approach has benefits like low maintenance costs and quick responses to the needs of different parts of the city. In simple terms, energy harvesting helps keep smart cities running smoothly by making sure connected devices always have the power they need.

In [12] paper, it has been explained that favors of a smart city come with possible risks. For e.g. one of the key components of a smart city is IOT devices, are most vulnerable and prone to cyber-attacks. So, we must oversee and control utility networks to shrink the chances such attacks on the regular bases. Area in which we must invest efficient smart utilities are: - networking and communication infrastructure, data collection and analysis, policies and regulation, and information security. In this era information technology infrastructure, traditional data management of smart services is routinely functioning on a centralized system. These centralized systems are inclined to security and privacy flaws. The Implementation of blockchain technology to enhance secure communication amongst smart utility devices is a compelling response to possible security breaches. A decentralized, safe data management plan with tamper proof consistency and verifiability can be achieved with the assistance of blockchain technology. Moreover, insecurities related with cloud and data are often linked with blockchain. The authors of this research presented a novel cyber security protocol based on the QHF (Quantum Hash Function), which was created using a quantum walk inspired by quantum mechanics. The provided protocol is used to create a blockchain that is motivated by quantum mechanics and allows for the safe exchange of data between smart devices. Also, QHF is used for connecting current block in relation to the chain's prior block. Hence making sure data is transferred b/t smart devices securely. The primary benefit of [] is that it gives a way of developing blockchain solutions made on model inspired by quantum mechanism that can survive assaults from both digital and quantum computers.

In [13] paper, Author gives attention on main component of smart cities, two deep learning ways and cyber security program as well as the connection among technology and smart cities are examined. Useful practical method for preserving user privacy and cyber security in smart cities are described. Acc. To author there are six main sectors in which cities can go with smartness. Although establishing smart cities have perks for business, citizen etc., these cities are prone to various cyber security risk. The defenseless a person's or an organization's action can create a position of risk of the whole city. The adoption of such technology by consumers will be placed into question due to the absence cyber security in smart cities.

This paper figures out and review the difficulties with cyberspace in smart cities and provide applicable and valid ways to deal with this problem or minimize the effects. Countless IOT sensors are located at various data gathering sites in smart city to acquire data of citizen, mobility, traffic, so that the feedback can be formed, and optimization of assets and resources can be done. Significant uses of deep learning in smart application are: - Urban Molding, Infrastructure, transportation, education, health, security, and privacy. Deep learning and related technology had proven successful in providing fruitful IOT based remedies for security breaches.

Summary Table 1.

Name of Paper	Technology Used	Future Scope	Objectives
“Software architecture	Internet of Nano Things,	Refining Software design and	To provide an assessment of the software

Name of Paper	Technology Used	Future Scope	Objectives
of the internet of things (IoT) for smart city, healthcare and agriculture: analysis and improvement directions"	Web Of Things, Radio Frequency Identification	resources managed by IOT	architecture applied in IoT systems to support agriculture and healthcare in smart city environments. Provide a model of software architecture for Internet of Things systems that is optimized for simplicity and performance, along with a comparative analysis of the suggested approach.
"LoRa based intelligent soil and weather condition monitoring with internet of things for precision agriculture in smart cities"	IOT, Machine Learning	Future research can be done to maximize system's functionality and inspect the possibilities of integration of techniques like blockchain and artificial intelligence.	To investigate possible applications of LoRa-based intelligent weather and soil monitoring systems for precision agriculture in smart city settings. By using IoT and ML technology to urban agriculture, it seeks to offer solutions for sustainable living and food security in urban areas.
"Cybersecurity and Privacy Solutions in Smart Cities"	Fuel Cell Technology, Building automation system, Industrial Control System	Public safety and privacy remain a central concern that can be achieved by giving legal, scientific and technological attentions such as by using blockchain, AI and ML.	to investigate the design principles and projects of smart cities, pinpoint security flaws and privacy concerns, and talk about standards, suggestions, and privacy and security solutions for smart cities and their services.
"Cyber Security Issues and Challenges for Smart Cities: A survey"	IOT (Internet of Things), Homomorphic encryption, Hash Link and Hash-Lock Method, Elliptic Curve Cryptography	Privacy and safety are the two key problems which are seen in the concept of smart cities which can be examined by giving a model to manage the security	The two main issues that smart cities face are privacy and safety. One way to solve these problems is to suggest a model for managing security in an efficient manner.
"Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects"	Artificial Intelligence	This paper only focusses on AI, in future we can embed AI with other technologies like ML, Blockchain.	To examine and emphasize the significance of cybersecurity in safeguarding smart cities from cyberattacks, data theft, and intrusion detection. The paper emphasizes artificial intelligence's function techniques in enhancing cybersecurity and promoting economic development in the digital environment.
"Smart city and cyber-security; technologies used, leading challenges and future recommendations"	Deep Learning	Research on privacy-preserving technologies to address the challenges of data privacy and security in smart cities, including the development of systems that ensure information integrity and prevent unauthorized access	The objective of this paper is to discuss the technologies employed, major issues, and upcoming for smart cities and cyber-security.
"Privacy and Security Aspects of E-Government in Smart Cities"	Blockchain, Artificial Intelligence	This paper only shows the challenges and solution in one sector, so we can use blockchain and AI in other sectors also.	To discuss the Aspects of e-government in smart cities related to security and privacy, including the challenges and opportunities they present. And also give guidance to use blockchain and AI as a solution.

III. Research Proposal

Cross-Chain:

A cross-chain bridge is a unique method using smart contracts over several blockchains. It securely transmits tokens from one blockchain to other by selling them on the origin and unzipping on the target. It works like a safe digital portal making the resources travel between blockchain in a supervised and authentic way. It works as a faithful interface between digital worlds that write the feature of transferring assets from one place to another in a safe and secure manner.

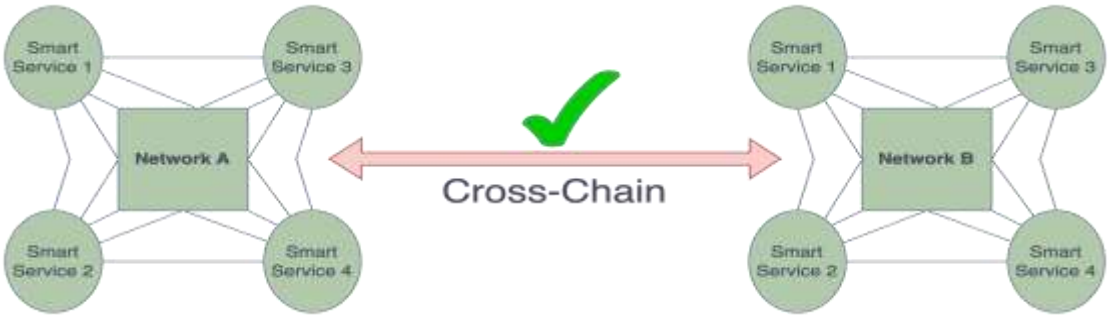

Fig. 1. Cross Chain Protocol to connect services across Smart cities.

In the field of blockchain a cross-chain bridge is a refined system. It provides safe transmission of tokens between distinct blockchains. On the starting point a user involves with a smart contract that deploys cryptographic function to see age or halt a particular number of tokens making sure that they transmitted securely. The cross-chain bridge works as safe and trusted gate, that uses cryptographic techniques and rules to transfer Siege tokens from the starting blockchain to the target blockchain. This method is close to a safe channel linking two different cyber zones.

When the destination blockchain is reached the user interacts with a smart contract encouraging cryptographic processes to get rid of tokens making them useful in a new blockchain environment. Search processes makes use of proves which are cryptographic in nature and can keep reliability and safety across cross chain transmission. To summarize the cross chain bridge makes use of the nuanced cryptographic and blockchain technology to make controlled and safe movement of tokens across different block chain ecosystems possible.

IV. Contribution

In the context of smart cities, the paper provides a comprehensive analysis of the opportunities and challenges related to data-centric cybersecurity. It explores the possible uses of blockchain technology in a variety of smart city domains, including as transportation, security, and governance. The study also looks at the advantages and potential outcomes of using data to drive Security protocols for applications within smart cities. It also discusses the difficulties in putting these techniques into practice and offers possible answers. To conclude, this study deepens our understanding of the importance of cybersecurity in the context of smart cities, highlighting the potential enhancement through the application of blockchain technology.

V. Conclusion

The concept of a "smart city" is rapidly becoming a reality, enhancing our quality of life through the converg-

-ence of IoT, cloud computing, and ICT tools. This technological advancement has fostered a sophisticated lifestyle but also heightened vulnerability to cyber-attacks, potentially compromising entire cities' data integrity. The financial losses and data breaches associated with smart cities could be unprecedented. To mitigate these risks, innovative technologies must be explored and implemented. Blockchain technology offers a robust solution for securely storing user data, thereby enhancing cyber security resilience in smart cities. This study examines the application of blockchain across various smart city domains, including security, governance, and transportation, highlighting its potential to address current cyber security vulnerabilities and ensure a safer, smarter urban environment.

REFERENCES

[1] R.M.A. Mohammad and M.M. Abdulqader, "Exploring cyber security measures in smart cities," Proc. -2020 21st Int. Arab Conf. Inf. Technol. ACIT 2020, 2020, doi: 10.1109/ACIT50332.2020.9300050.
[2] F. Almeida, "Prospects of Cybersecurity in Smart Cities," Futur. Internet, vol. 15, no. 9, pp. 1–21, 2023, doi: 10.3390/fi15090285.
[3] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," Energy Reports, vol. 7, no. xxxx, pp. 7999–8012, 2021, doi: 10.1016/j.egyr.2021.08.124.
[4] N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "Opportunities and challenges of data-driven cyber security for smart cities," Syst. Secur. Symp. SSS 2020 - Conf. Proc., 2020, doi: 10.1109/SSS47320.2020.9174388.
[5] R.O. Andrade, S.G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garces, "A comprehensive study of the IoT cyber security in Smart Cities," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3046442.
[6] C. Formisano et al., "The advantages of IoT and cloud applied to smart cities : ClouT user scenarios and reference architecture," Proc. - 2015 Int. Conf. Futur. Internet Things Cloud, FiCloud 2015 2015 Int. Conf. Open Big Data, OBD 2015, pp. 325–332, 2015, doi: 10.1109/FiCloud.2015.85.
[7] B. Bhushan, A. Khamparia, K.M. Sagayam, S.K. Sharma, M.A. Ahad, and N.C. Debnath, "Blockchain for smart cities: A review of architectures, integration trends and future research directions," Sustain. Cities Soc., vol. 61, p. 102360, 2020, doi: 10.1016/j.scs.2020.102360.
[8] S.R. Maskey, S. Badsha, S. Sengupta, and I. Khalil, "BITS: Blockchain based Intelligent Transportation System with Outlier Detection for Smart City," 2020 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2020, pp. 12–17, 2020, doi: 10.1109/PerComWorkshops48775.2020.9156237.
[9] A. Khanna et al., "Blockchain: Future of e-governance in smart cities," Sustain., vol. 13, no. 21, pp. 1–21, 2021, doi: 10.3390/su132111840.
[10] J.V. Botello, A.P. Mesa, F.A. Rodriguez, D. Diaz-Lopez, P. Nespoli, and F.G. Marmol, "Block SIEM: Protecting smart city services through a blockchain-based and distributed SIEM," Sensors (Switzerland), vol. 20, no. 16, pp. 1–22, 2020, doi: 10.3390/s20164636.
[11] A.E. Akin-Ponnle and N.B. Carvalho, "Energy harvesting mechanisms in a smart city-a review," Smart Cities, vol. 4, no. 2, pp. 476–498, 2021, doi: 10.3390/smartcities4020025.
[12] A.A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S.E. Venegas-Andraca, and J. Peng, "Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities," Inf. Process. Manag., vol. 58, no. 4, p. 102549, 2021, doi: 10.1016/j.ipm.2021.102549.
[13] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," Energy Reports, vol. 7, pp. 7999–8012, 2021, doi: 10.1016/j.egyr.2021.08.124.

AUTHOR'S PROFILE

First Author
Abhishek Sharma, Student, Department of Computer Science and Informatics, Central University of Himachal Pradesh, India. email id: sabhibhardwaj3@gmail.com

Second Author
Onkar Srivastava, Student, Department of Computer Science and Informatics, Central University of Himachal Pradesh, India.

Third Author
Dr. Pradeep Chouksey, is an Associate Professor and Head of Department of Computer science and informatics at Central University Himachal Pradesh (H.P.). He has teaching and research experience of more than 16 years. He is actively involved in research with more than 50 presentations, publications and articles in several reputed peer-reviewed international journals, National and international conferences, edited books, etc. He had served as session chair at several National and international conferences. He serves as external examiner for doctoral candidates, external member of doctoral committees, member of board of studies, and academic auditor for various institutions and universities. He also serves as reviewer of papers for various international journals and subject expert for external committees. email id: dr.pchouksey@hpcu.ac.in

Fourth Author

Dr. Parveen Sadotra, (MCA, Ph.D, CCSP, CEH, and CCCA) is presently working as Assistant Professor in Department of Computer Science Informatics, Central University of Himachal Pradesh has definitive experience in the field of computers and Cyber Crime Investigation Training. He specializes in Cyber Security, Ethical hacking and Cyber forensics, furthermore, Dr. Sadotra presented and published various research papers on Cyber Laws, Investigation of cybercrime, Intrusion Detection System, Cyber Security, Web Security, E-Commerce and Cyber Education in the leading journals. He also published a book on Mobile Technologies and Cloud Computing. In addition to this he deliver--ed various Lectures and Presentation in Workshop, Seminar and in capsule Trainings. He has got various Appreciations & Commendations certificates from J&K Police for Working on Cyber Crime. email id: sadotramca2k6@gmail.com

Fifth Author

Mayank Chopra, has received BSc Physics (Hons.) degree from Himachal Pradesh University, India, and MSc Information Technology degree from Central University of Himachal Pradesh, India. Currently he is working as an Assistant Professor in the Department of Computer Science & informatics at Central University of Himachal Pradesh, India. His current research interest includes deep learning, UAV, web development, security and data science.
email id: mayankchopra.it@gmail.com