International Journal of Engineering Sciences & Emerging Technologies, Oct. 2023.
ISSN: 22316604 Volume 11, Issue 2, pp: 71-78 ©IJESET

AN APPROACH TO SECURE IOT APPLICATIONS OF SMART CITY USING BLOCKCHAIN TECHNOLOGY

Saurabh Srivastava[1], Tasneem Ahmed[1], Amit Saxena[2]

[1]Advanced Computing Research Laboratory, Department of Computer Application, Integral University, Lucknow, India
srsaurabh@iul.ac.in, tasneemrke@gmail.com
[2]Department of Computer Science & Engineering, MIT, Moradabad, India
er.amitsaxena79@gmail.com

ABSTRACT

The objective of a smart city is to solve the problem that is occurring due to population growth in urban areas such as physical security, residual management, transportation systems, etc. The backbone of a smart city is technology, and citizens of a smart city are connected with the government and other organizations through interconnected systems. Internet of Things (IoT) technology refers to the effective solution for the development of a smart city at a low cost with its high applicability in an uncountable number of scenarios. Intelligent devices (IoT devices) are continuously collaborating in various areas of the smart city to exchange a continuous flow of information and provide high-quality services to citizens as the ultimate goal. Urbanization continues growing and due to urbanization, integrated policies are required to improve the lifestyle of the urban citizen through the implementation of integrated, interoperable, and secure electronic services. A secure IoT application should ensure that the flow of data shouldn't tampered, and private information shouldn't be leaked. Blockchain is a distributed tamper-resistant and privacy protection ledge that provides a promising solution for decentralized secure IoT applications. However, due to the large number of IoT systems and the contradiction between traceability and data privacy, blockchain faces big data and privacy challenges. Blockchain can solve problems in local communities, according to government officials. Blockchain is initially considered through collaboration with cryptocurrency i.e. Bitcoin, and it provides an innovative perspective on how smart cities can be organized and a more transparent economic model for resource management. The current era is technology-oriented, and everyone is seeing the innovation of the smart city. Modern technologies are playing an important role in the development of the smart city and creating new opportunities in terms of social and economic. In a smart city, The IoT is increasingly connecting homes, cars, public places, and other social systems. IoT devices are increasing day by day while IoT services are expanding. As IoT devices are increasing, the number of attacks and threats on IoT devices are also increasing which fades the success of IoT. In the current era, cyber-attacks are not new, but IoT will be deeply woven into human life and societies hence it becoming a big issue so cyber defense takes it seriously. The IoT-based applications can be accessed through smartphones that take input from the user, The input of the user can include some personal, professional, and sensor data, and the application provides different kinds of information. The major issues of IoT application development are the security and privacy of user data, which is a challenging task from a different perspective. In this study, some privacy and security issues have been discussed related to IoT-based smart city applications and a blockchain-based framework has been proposed for IoT-based applications to a smart city that can overcome the challenges of user data security and privacy.

KEYWORDS: *Smart City, Blockchain, IoT, Internet of Things, Smart Applications*

DOI: 10.5281/zenodo.10434277

1. INTRODUCTION

Today, applications of the smart city provide user recommendations such as reduced energy consumption, warnings about broken devices, reliable device and software selection, diagnostics, and more. Internet connectivity has a dynamic and heterogeneous nature for smart city environments and creates new challenges in the areas of privacy, security, and authentication [1]. Smart cities aim to solve the challenges posed by urban population growth, such as the transparent management of various public resources [2]. IoT technology provides an inexpensive and effective solution for the development of smart cities with its high applicability in countless scenarios [2]. A large number of devices and other components are connected in the IoT environment which creates the surface for attacks [2]. The significant risk of exposing a weak IoT ecosystem is the ability to infect a large number of potential IoT devices that can become members of the botnet capable of conducting distributed attacks [2].

The blockchain is a network of decentralized peers-to-peers where all created transactions are verified by signed nodes and stored in a decentralized, immutable ledger. Consensus algorithms are used in blockchain technology to ensure network reliability. The produced events cannot be certified by a central authority; each transaction on the blockchain must be independently verified by each blockchain node [2]. A Smart City includes essential elements that enable data centralization. These elements can take many different forms, from straightforward web pages to intricate programs run by specialized hardware [3]. It is important to guarantee the data's availability so that users can freely use the system and interactively suggest updates and adjustments [3]. Smart city-based IoT applications can help to improve the quality of life, and a "smart" cityscape with numerous connected devices create large communication networks that cannot be secured easily with traditional cyber security mechanism [3]. Blockchain is a cutting-edge digital technology that might upend a variety of businesses and organizations, forcing them to reevaluate their objectives and capabilities [4]. In many different application sectors, including the financial industry, healthcare, education, and communication networks, sophisticated privacy safeguards are utilized to protect sensitive and important data [5]. The challenges in IoT-based smart city applications are information security, data privacy, and cyber-related concerns because an unauthorized user can access the information [7]. In this study, a blockchain-based framework has been proposed for IoT-based applications to a smart city that can overcome the challenges of user data security and privacy.

2. TECHNICAL BACKGROUND

2.1. Smart City

The smart city is equipped with a large number of electrical equipment, and the technology and equipment enable smarter more accessible, and adaptable smart cities as a result [6]. Smart cities are places where economic, social, and environmental factors are balanced and connected through delegated processes to more effectively manage significant resources, assets, and urban flows for in-the-moment activities [7]. To improve social as well as urban interconnectivity through increased public involvement and government efficiency, smart cities are based on an ICT infrastructure with IoT-enabled sensor technologies [7]. Urban populations are growing around the globe, and 68% of the world's population is anticipated to reside in cities by 2050. Sustainable development increasingly depends on effectively controlling urban growth, particularly in countries with low or middle incomes where urbanization is expected to accelerate at the highest rate. The majority of countries have difficulties providing fundamental services to their citizens, including housing, public transportation, energy systems, infrastructure, job opportunities, health services, and education. Urban and rural citizens' lives must be improved, and the social, environmental, and economic relationships that already exist between them must be strengthened, through the implementation of integrated policies [3].

2.2. Internet of Things (I0T)

Internet and things are two terms that are used to form the phrase "Internet of Things." The definition of the Internet is a network of networks that can link billions of users via traditional Internet protocols. Using contemporary technologies, the internet combines many agencies and industries. There are

DOI: 10.5281/zenodo.10434277

numerous ways to access the Internet, including through mobile devices, personal computers, and businesses. The second term, "thing," denotes devices or items that can change into intelligent objects [8].

The IoT is growing in popularity and tackling a number of real-time application difficulties thanks to 6G technology. Big data analytics rely heavily on artificial intelligence, which also provides reliable data analysis in real-time [9]. In many areas of smart city scenarios, intelligent gadgets can work together to exchange a steady stream of information and offer inhabitants high-quality services [2]. The term "intelligent" refers to IoT devices that can interact independently and with little to no human intervention [2]. IoT gadgets have been able to offer a wide range of helpful services, however, due to limited computational power and a lack of IoT device monitoring, the proliferation of IoT solutions offers serious security issues [2]. Several studies have focused on identifying vulnerabilities in the IoT ecosystem and proposing effective solutions to address them as a result [2]. Sensors, actuators, switches, and lightbulbs are examples of IoT devices found in smart homes. The majority of IoT devices have heterogeneous designs, short battery lives, and weak computing capabilities, making them challenging to adapt to new situations [1].

At the same time, there are billions of IoT mobile devices all around us that might take the place of the utility provided by specialized gear. By 2025, there will be 75.44 billion users of mobile IoT devices, including laptops, smartphones running Android, iPhones, iPads, and other gadgets. Each user will be linked to six of these devices [10].

In 2003, there were 500 million Internet-connected devices and around 6.3 billion people on Earth. In 2010, 12.5 billion devices were online, mostly as a result of the fast expansion of smartphones and tablets. Going forward, Cisco IBSG predicts that 25 billion devices will be connected to the Internet by 2015 and 50 billion devices will be connected to the Internet by 2020. However, such connections can provide critical security to IoT systems, as an attacker could break into the system and gain unauthorized access to the resources provided (data, services, storage units, computing units, etc.). It can also cause problems in IoT devices [1].

2.3. Blockchain

IoT devices will gather data from urban areas and provide real-time management information using new network paradigms like Edge Computing and Fog Computing. Making sure the data provided via Edge Computing are trustworthy is one of these difficulties. Blockchain technology has been more popular recently due to its strong security in finance and cryptocurrency [11].

Blockchain is a distributed database in which data are stored on various computers known as nodes in the blockchain network. The network has no central authority, and it is maintained by the nodes that participate [4]. For example, altering information in the database necessitates the participants' agreement. Because there is no single point of failure, this distributed method of storing and handling data is more secure. This decentralized system is also more reliable because any changes to the ledgers will be made public [4]. Today, blockchain has become extremely popular, and technological progress is the only constant in the fight to preserve data in the insecure digital world [5]. The blockchain was first described in 1991 by a group of researchers, and the goal of blockchain's design and development was to provide a timestamp for digital documents [5]. Blockchain proposes two ways to build a network such as permitted and unauthorized blockchain [2].

- In permitted, blockchains allowed (private blockchains) limit access to nodes that belong to the network and perform tasks. The capacity to select the level of network decentralization is a characteristic of this kind of blockchain [2].

- In unauthorized, blockchain (public blockchain) allows candidates to become nodes and join the network. As long as they have the physical resources, nodes on this blockchain can complete any work (such as block mining, transaction validation, etc.) [2].

DOI: 10.5281/zenodo.10434277

3. An Approach to Protect IoT Applications Using Blockchain Technology

Application for a smart city is based on modern technologies such as IoT, ICT, Cloud, etc. The objective of smart city applications is to make human life easier. Now, lots of applications are running that are providing different kinds of services such as cloud kitchen, traffic monitoring, navigation services, etc. Smart applications are mostly based on smartphones because the application can use mobile hardware that reduces the cost of application and may be in every smartphone. Smartphone has user' personal and professional information, and if they lose their phone then it can be hacked by someone means the user loses the data as well as they loosed their password for social media, email, and many more. The thief or hacker can use the user's information for their benefit. Smart application takes input from user in form of the structured, unstructured, and semi-structured format. The structured format includes the input data, the unstructured format includes images, audio, video, sensor data, etc., and the semi-structured format includes the characteristics of the structured and unstructured format.

Now, IoT-based applications are not so reliable because the IoT devices are connected through the networks and lots of tools are available that provide mechanisms to take control of a smartphone. User shares their personal and professional information on different platform such as sharing their activities on social platform on a routine basis, and the attacker/ hacker trace user activities through social media and observes the key parameter of user security. Lots of applications store the data of users on a centralized database. In the centralized database, data is stored in a single location which creates problems during a system failure or system hack. In this study, an approach to secure IoT applications of smart cities using blockchain technology has been proposed, the block diagram of the proposed framework is shown in Figure 1.

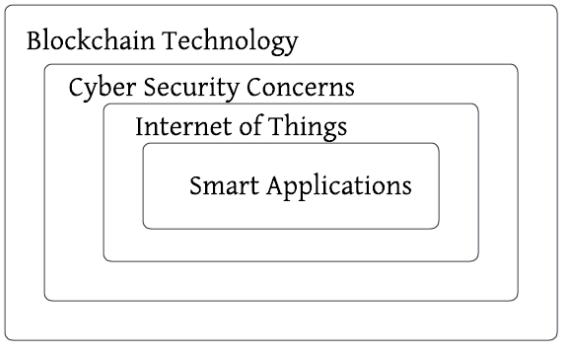

Figure 1. An Approach to Secure IoT Applications of Smart Cities using Blockchain Technology.

3.1. Smart Applications

The objective of smart applications is to improve the quality of human life. Various applications are available that provide different kinds of services, and users are using them to minimize their time and effort. Smart applications monitor the activities of the user to understand the nature and interest of the user, and applications recommend a lot of things to the user based on the user's interest. Smart applications use personal information to provide a high quality of services. The trending smart cities applications are shown in Figure 2.

DOI: 10.5281/zenodo.10434277

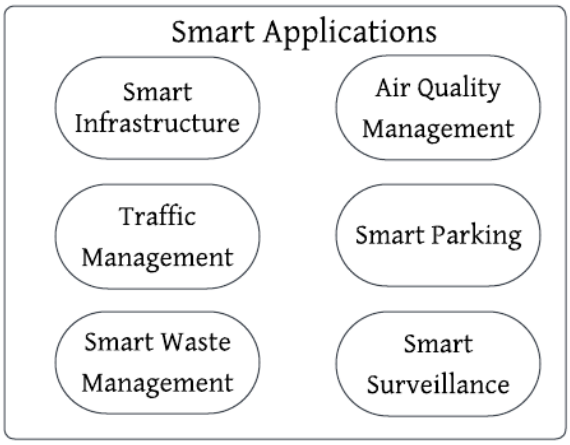

Figure 2. Trending Smart Cities Applications.

3.1.1. Smart Infrastructure

With the ability to create circumstances for continual development, modern technologies are becoming a significant source for cities. As a result, buildings and urban infrastructures should be developed effectively and sustainably. To reduce CO2 emissions, cities must additionally make investments in electric and self-propelled vehicles. Building a sustainable infrastructure and achieving efficient energy use may be made possible by intelligent technologies.

3.1.2. Air Quality Management

To capture pollutant data in real-time and forecast emissions, smart cities are putting in place mechanisms. Poor health, early deaths, and harm to crops, buildings, and ecosystems are all consequences of poor air quality. Since the majority of people live in metropolitan areas, the impacts of poor air are more severe there. As a result, the majority of cities trust air quality monitoring systems. The air quality of a smart city is currently monitored by large, expensive sensing stations that have sensors installed in key locations. These stations measure parameters like particulate matter (PM), nitrogen dioxide (NO2), carbon dioxide (CO2), and ozone (O3), which allows accurate monitoring but is only applicable to certain areas.

3.1.3. Traffic Management

The cities are facing a major problem which is traffic and trying to find the best possible technology to optimize the traffic. An intelligent transportation system has been put into place in several smart cities throughout the world to manage traffic. The integrated pavement sensors transmit real-time traffic flow updates to the central traffic management platform, which analyzes the data and swiftly adapts the signal lights to the current traffic scenario. At the same time, the collected data is used to predict where traffic can go, and none of these processes is required human interference.

3.1.4. Smart Parking

The smart parking-management systems are complementary with the traffic monitoring system and the aim is to manage efficiently traffic flows for informing citizens, when they are looking for parking then it can suggest free parking space nearby. Many cities are taking advantage of intelligent parking solutions. Sensors are built into the ground which helps to identify the vehicle that has left the parking area. Sensors sense and forward the report of the location of free parking spaces via a mobile app to the drivers.

DOI: 10.5281/zenodo.10434277

3.1.5. Smart Waste Management

Waste (Garbage) management solutions improve the effectiveness of garbage collection and save operating expenses by more effectively managing most of the environmental problems connected to ineffective garbage collection. In these solutions, the garbage can is equipped with a level sensor, and when a particular level has been exceeded, the truck driver's control platform notifies them via their smartphone.

3.1.6. Smart Surveillance

Urban security is a crucial component of smart cities, and residents are extremely concerned about security. Nowadays, many towns adopt smart surveillance systems that rely on cameras placed practically everywhere in the metropolis. While some are private cameras placed by private organizations to reduce crime, others are police-installed cameras that allow real-time surveillance of the most important places.

3.2. IoT

The IoT is a network of actual physical objects that are equipped with software, sensors, and other tools to connect and communicate with other systems and devices through the Internet. The number of IoT applications for smart cities is continually growing. A lot of cities are using sensors and activists to monitor all of the activities that go on there. These devices usually communicate via wireless links and form a type of capillary network pervading the city. Smart cities currently use certain widespread applications, including participative sensing, intelligent parking, intelligent monitoring, and environmental and traffic surveillance.

The Internet is used by IoT applications to connect disparate heterogeneous objects, which explains why smart cities have sensor networks and connect their smart appliances to the Internet for monitoring their health. The Internet is the IoT's convergence point, and it is a high-speed network that uses common communication protocols. The fundamental principle of the IoT is that anything that exists may be measured, estimated, and changed in some manner.

The proliferation of various objects and communication tools empowers IoT. IoT includes things like smartphones and other amenities like food items, machines, and locations that can work together to achieve a common goal. The IoT requires wireless sensor communication since wired connections between millions of sensors would be expensive. Multiple devices can be connected using low-power standard communication. According to location and distance coverage, some networks offered by IoT are shown in Figure 3.

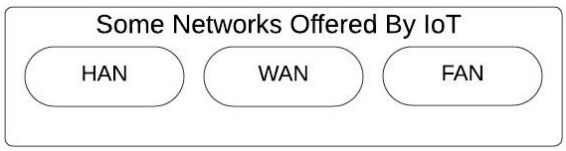

Figure 3. Some Networks are offered by IoT.

- Home Area Networks (HAN) are used as a short-range standard like Dash7, ZigBee, and Wi-Fi. The HAN connects all components and equipment used for monitoring and controlling a home.

- Wide Area Networks (WAN) facilitate interaction among customers and distribution utilities. WAN implementation requires broadband wireless technologies like 3G and LTE or fiber optic cable because it needs far broader coverage than HAN.

- Customers and substation connections are made using field area networks (FAN).

DOI: 10.5281/zenodo.10434277

3.3. Cyber Security Concerns

Various platforms are available that are providing various types of services in many areas that make human life easier. People in smart cities are sharing their personal and professional information through different platforms to take advantage of smart services. Hackers engage in a variety of actions to obtain user information, and secret information can be used to unlock the user's confidential items such as their banking system, e-mail, and social media accounts. Hackers engage in a variety of unethical activities to get control of a user's system to steal or damage personal and organizational data. The cyber concern can be categorized into two categories: individual concerns and technical concerns which are shown in Figure 4.

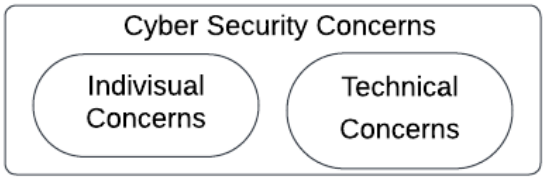

Figure 4. Cyber Security Concerns.

3.3.1. Individual Concerns

The smart city provides a platform of services for individuals seeking and raising social issues. Citizens' safety, communication, transportation, and banking are individual concerns in terms of cyber security.

3.3.2. Technical Concern

Numerous applications provide a variety of services that make human life easier. Everyone wants to get more benefits from it, but users can hurt themselves if they make a small mistake. A hacker participates in a variety of activities to get unauthorized access to a user's system. Some technical instruments can be used for security, monitoring, or preventing unauthorized access such as Biometrics, Smart Grids, etc.

3.4. Blockchain Technology

Lots of cyber concerns exist nowadays and need a mechanism that can protect the user information that exists on different servers. Blockchain is a modern technology that can help to secure the IoT environment. A blockchain is a growing collection of records known as blocks that are connected via encryption. Each block contains a time stamp, exchange information, and a cryptographic hash of the block before it. Using blockchain, we can securely store data over a distributed system so that no one can alter it and everyone can only view it. Blockchain will keep track of all information transactions in a ledger, and it will employ a distributed method to verify each transaction. The blockchain is used to securely exchange crucial data such as money, property, contracts, etc. without the need for a third-party middleman such as a bank or government. After the information has been saved on a blockchain, it is highly difficult to change it.

4. CONCLUSION

Nowadays, there are many more smart cities, and their residents have access to many high-tech services thanks to the IoT. Unfortunately, such IoT devices are typically insecure, providing an ideal playground for cybercriminals and posing an unavoidable risk to the widespread deployment and success of Smart cities. Blockchain immediately contributes to the security of IoT ecosystems by tightly regulating security events resulting from the IoT Sentinels shielding a particular group of IoT devices and ensuring integrity and non-repudiation by utilizing the advantages of blockchains. Furthermore, Blockchain provides desirable security aspects such as resilience, trust-orientation, auditability, and scalability. Extensive testing has shown that blockchain performs admirably with a range of security events and short transaction times with the highest impact consensus technology.

DOI: 10.5281/zenodo.10434277

REFERENCES

[1] Dang, T. L. N., & Nguyen, M. S. (2018, November). An approach to data privacy in smart home using blockchain technology. In 2018 International Conference on Advanced Computing and Applications (ACOMP) (pp. 58-64). IEEE.

[2] Botello, J. V., Mesa, A. P., Rodríguez, F. A., Díaz-López, D., Nespoli, P., & Mármol, F. G. (2020). BlockSIEM: Protecting smart city services through a blockchain-based and distributed SIEM. Sensors, 20(16), 4636.

[3] Rotună, C., GHEORGHIȚĂ, A., Zamfiroiu, A., & SMADA ANAGRAMA, D. (2019). Smart City Ecosystem Using Blockchain Technology. Informatica Economica, 23(4).

[4] Ying, W., Jia, S., & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group. International Journal of Information Management, 39, 1-4.

[5] Rupa, C., & Midhunchakkaravarthy, D. (2020, May). Preserve security to medical evidences using blockchain technology. In 2020 4th international conference on intelligent computing and control systems (ICICCS) (pp. 438-443). IEEE.

[6] Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. P. (2017). A review of smart cities based on the internet of things concept. Energies, 10(4), 421.

[7] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 1-22.

[8] Goyal, K. K., Garg, A., Rastogi, A., & Singhal, S. (2018). A literature survey on Internet of Things (IoT). International Journal of Advanced Networking and Applications, 9(6), 3663-3668.

[9] Sharma, A., Podoplelova, E., Shapovalov, G., Tselykh, A., & Tselykh, A. (2021). Sustainable smart cities: convergence of artificial intelligence and blockchain. Sustainability, 13(23), 13076.

[10] Wang, J., Zhu, J., Zhang, M., Alam, I., & Biswas, S. (2022). Function Virtualization Can Play a Great Role in Blockchain Consensus. IEEE Access, 10, 59862-59877.

[11] Ferreira, C. M. S., Garrocho, C. T. B., Oliveira, R. A. R., Silva, J. S., & Cavalcanti, C. F. M. D. C. (2021). IoT registration and authentication in smart city applications with blockchain. Sensors, 21(4), 1323.

DOI: 10.5281/zenodo.10434277