JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

The Imperative Need for Block chain in Smart Cities: Ensuring Data Security

[1]Akhil S & Dr. Jose Reena K [2]

[1]Ph. D, Research Scholar**,** *School of Computing Sciences, VISTAS, Chennai, Tamil Nadu, India*

[2]Assistant Professor, (Corresponding Author), School of Computing Sciences, VISTAS, Chennai, Tamil Nadu, India

Abstract:

The connection of common physical objects, devices, and systems using the technology of internet is known as Internet of Things (IoT) and it represents a paradigm shift in technology. These items may autonomously collect and share data among themselves and with centralized systems in an IoT environment because they are outfitted with sensors, software, and communication capabilities. This is all done without the need for human intervention. The Internet of Things (IoT) widely used in smart cities to gather and share massive amounts of data in order to uplift urban living. However, ensuring the privacy and the security of this data is paramount.

Keywords: - IoT, Smart City, Block chain

INTRODUCTION

Internet of Things (IoT) is an interesting technology that refers to the network of common objects that are equipped with sensors, electronics, and software which are connected to the internet to exchange and gather data without user intervention. In the context of the IoT, "things" refers to everything and anything that are connected to or accessed over the internet to the betterment of daily life. An advanced urban setting is termed as a smart city that uses cutting-edge technology along with data-driven solutions to empower sustainability, optimize the effectiveness of various services and infrastructure, and altogether improve the quality-of-life style for its citizens. In order to attain this, it is important to gather and process data about energy use, public safety, traffic flow, environmental conditions, and other topics. This particular task is done by employing a network of interconnected sensors, devices, and data analytics. The IoT primarily allows to share and gather data over the internet with other systems and devices by maintaining an interconnected network of real-world items and devices that have been equipped with sensors, software and other technologies. The potential real-world application of IoT in a variety of sectors, such as agriculture, healthcare, transportation, and smart homes, has made it extremely popular [1].

IoT covers a wide range of spectrum and its devices can range from actuators and simple sensors to complex systems like industrial automation equipment and self-driving cars. These devices communicate with each other and central servers, enabling real-time data analysis and decision-making [2]. Smart cities rely on IoT networks to gather data from various sensors, devices, and infrastructure elements. This data serves as the foundation for efficient city management and improved quality of life [3]. However, the massive data flow in smart cities introduces security vulnerabilities.

DATA SECURITY CHALLENGES IN SMART CITIES:

1. **Data Proliferation:**
   Unprecedented volumes of data are generated by smart cities, including confidential data about people, traffic patterns, and vital infrastructure. It is crucial to keep sensitive data safe from unlawful access [5].
2. **Privacy Concerns:**
   Smart city IoT equipment may unintentionally gather personal data, which raises privacy issues. Privacy violations may result from unauthorized access to this information [6].
3. **Critical Infrastructure:**
   Smart cities use IoT to handle essential services like transportation, utilities, and public Safety. If data security is compromised, significant consequences could befall urban Infrastructure [7].
4. **Cyberattacks:**

The potential attack surface expands along with the number of linked devices. Cyberattacks aimed at halting services, stealing private information, or causing bodily harm are a threat to smart cities [8].

Block Chain Technology: A solution for Smart Cities

Block chain provides a decentralized and tamper-proof ledger for data storage. It ensures data integrity and immutability by chaining data blocks [9]. A method for transferring digital payments between parties without the requirement for a central authority, block chain was initially made public as bit coin. As a new technology, block chain has several benefits: it is transparent, anonymous, trust less, democratizing, automated, decentralized, and secure. These blockchain features promote the development of smart cities and improve services offered by them.10].In conjunction with block chain Technology and IoT has produced creative answers for smart cities, particularly when it comes to services offered by the sharing economy. The suggested system makes use of the inherent security and immutability of block chain technology to build mutual trust among users of edge-deployed IoT devices for real-time data gathering and decision-making. This integration facilitates secure and transparent transactions, enabling seamless sharing of resources, assets and services among citizens. Additionally, cognitive computing capabilities are integrated into the framework, increasing adaptability, and intelligence in resource allocation and service optimization. It covers its potential to revolutionize the landscape of the sharing economy in smart cities and promote sustainability, inclusion and efficiency while addressing challenges related to data security and trust [4]

THE FUTURE OF SMART CITIES WITH BLOCK CHAIN

(a) Block Chain Enabled 5G Mobile Edge Computing with RFID-Based Authentication for Supply Chain:

Supply chains need to be able to transmit secure real-time data on the commodities they are moving, and this requires bandwidth that is beyond the capabilities of the current infrastructure. Thus, mobile edge computing with IoT with 5G capability aims to significantly boost this capacity. The RFID-based system for authentication supported by lightweight block chain technology (LBRAPS), a novel effective lightweight RFID-based supply chain authentication protocol in the context of 5G mobile edge computing, was created to address this problem. LBRAPS exclusively uses bitwise rotation, single-path cryptography hashing, and activities that use bitwise exclusive-or (XOR). LBRAPS has proven to be secure against a number of assaults. Additionally, the popular Automated Verification of Applications and Protocols for Internet Security (AVISPA) tool's simulation-based formal security verification confirms the security of LBRAPS. [11]

The following lists a few crucial traits that all business transactions utilizing block chain technology have in common.

1) **Real-time records**: - With programming automating the process, distributed ledgers are continuously updated as transactions and other events may occur. Such characteristics ensure that to reduce the possibility of several types of extortion, every network entity should have its own current transaction records.
2) **Immutable records**: - With the help of block chain technology, substances can produce everlasting transaction records. This ability provides a clear commercial benefit, but it can also increase administrative risk for some parties. It becomes more difficult for parties to argue that they don't have enough transaction records when controllers can be provided permission to see whole transaction narratives during an examination, including transactions tied to a block chain.
3) **Anonymity:** - Block chain technology makes it easier for users of networks to employ pseudonyms that has implications in lieu of network coordinators who must adhere to numerous rules including “anti-money laundering (AML) and “know-your-customer (KYC) laws.
4) **Cyber Security Risk**: - Block chain systems have developed as hackers' favourite targets for a variety of reasons. The decentralized block chain structured networks are stronger against a range of network-wide assaults, including data tampering. The scope of security events has ranged from routine administrative interruptions to an uptick in genuine data breaches and crypto currency thefts.
5) **Tax-implications**: - Depending on what manner the relevant taxation body views "virtual currency," block chain transactions involving virtual currency could result in unexpected tax repercussions.[11]

In recent years, "Radio Frequency Identification (RFID)" the use of technology expanded quickly and been taken in a variety of applications, including "inventory management, supply chain, product tracking, transportation, logistics, and self-administration store." An adversary can undertake passive attacks like "eavesdropping attacks" and active attacks like "replay attacks and Denial-of Service (DoS) attacks" because RFID tags and readers communicate with each other via radio frequency signals (wireless). RFID is currently being used in many industries, including airline baggage management, automated payment systems, and supply chain management. The private RFID information was transferred through a public network and is also kept on various hardware. Considering that RFID-capable gadgets with a variety of delicate goods, such as passports as well as identification records, that is essential to establish communication security protocols that make RFID systems. Additionally, it is necessary to prevent the leakage of private RFID data regarding real-time apps or health monitoring systems [11]

(b)"5G Unchained: Pioneering Block chain Services for Local Operators"

The Smart cities, driverless cars, remote surgery, Industrial Internet of things (IIoT), virtual and augmented reality, as well as other fields have the potential to benefit from the development of 5G, a promising new technology. Since each of these verticals has a unique set of network connectivity needs, it is difficult to provide tailored services for each one utilizing a single 5G infrastructure. Therefore, operating private 5G networks or local 5G operator (L5GO) networks is a practical solution to this problem. A localized small cell network called an L5GO network can supply services in a customized way. Vertical owners can deploy and manage L5GO networks with the help of the application of network software in 5G. The implementation of L5GOs, however, brings up a number of challenges pertaining to subscriber management, roaming users, spectrum, security, as well as the infrastructure. In order to offer various services for L5GOs, the study introduces a collection of modularized functions built on block chain technology, including service rating systems, bidding strategies, and selection functions. Utilizing block chain technology ensures availability, reduces dependency on reliable third parties, secures transfer payments, and has many other benefits [12].

ADVANTAGES OF BLOCK CHAIN IN SMART CITIES

The main benefit of block chain technology is that it allows nodes with extremely decentralized decision-making authority to come to an agreement on whether or not the transactions in the block are valid in a decentralized system. The PoW mechanism, which is used in classic block chain technology, heavily depends on the dispersed nodes' processing capacity to ensure consensus amongst them.[13]

Conclusion

In conclusion, adopting block chain technology in smart cities is not just recommended but also necessary. Smart integration of technology is becoming more and more important for sustainable development as urban populations increase. The promise of greater citizen engagement, economic growth, and the realization of truly smart, resilient, and secure urban settings are all made possible by block chain, which serves as a defender of data security and fortifies the foundation of smart cities. A commitment to constructing the cities of the future on a foundation of security and trust requires more than just a decision to embrace block chain technology.

References:

1. Ashton, K. (2009). "That 'Internet of Things' Thing." RFID Journal, 22(7).
2. Atzori, L., Iera, A., & Morabito, G. (2010). "The Internet of Things: A survey." Computer Networks, 54(15), 2787-2805.
3. Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. "Journal of Urban Technology," 18(2), 65-82.
4. Md Abdur Rahman,Md Mamunur Rashid[...],Mohsen Guizani IEEE Access (2019).” Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City”
5. Zhang, X., Han, R., & Jia, W. (2015). "Security and privacy in smart city applications: Challenges and solutions." IEEE Access, 4, 2297-2311
6. Kumar, N., & Jain, A. (2016). A survey of Internet of Things architectures. "Journal of King Saud University-Computer and Information Sciences."
7. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). "Fog computing and its role in the internet of things." In Proceedings of the first edition of the MCC workshop on Mobile cloud computing (pp. 13-16).
8. Lee, I., & Lee, K. (2015). "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business Horizons, 58(4), 431-440.
9. Chamara S. Gunasekara, et al(2019)"Blockchain for Data Security and Privacy in IoT: A Survey".IEEE Internet of Things Journal.
10. Junfeng Xie,Helen Tang,[...]Yunjie Liu(2019) “A Survey of Block chain Technology Applied to Smart Cities: Research Issues and Challenges” IEEE Communications Surveys and Tutorials
11. Srinivas Jangirala, Ashok Kumar Das,Athanasios V. Vasilakos(2020) ” Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment” IEEE Transactions on Industrial Informatics
12. Nisita Weerasinghe,Tharaka Hewa, [...],Mika Ylianttila(2021)” A Novel Block chain-as-a-Service (BaaS) Platform for Local 5G Operators” IEEE Open Journal of the Communications Society.
13. Wenbo Zhang,Zonglin Wu,[...],Lei Shu(2020)“LDC: A lightweight dada consensus algorithm based on the blockchain for the industrial Internet of Things for smart city applications”. Future Generation Computer Systems.