Blockchain Based Secure Data Management for IoT Devices

(A Survey of Current Research and Future Directions)

Madhuri Sharma[1]; Dr. Arvind Mahindru[2]; Dr. Pardeep Arora[3]

[1]PhD Research Scholar, Department of Computer Science and Applications,
DAV University Jalandhar, India.
[2]Associate Professor, Department of Computer Science and Applications,
DAV University Jalandhar, India.
[3]Associate Professor, Department of Computer Science and Applications,
K.M.V College Jalandhar, India

Publication Date: 2025/03/08

Abstract: Two of the most ground breaking technologies, blockchain and the Internet of Things (IoT), are already beginning to drastically alter The network configuration as it appears now and reshape details digital world during the future. IoT integration has given the things around us life and made them "smart" and able to communicate with one another. This has allowed them to continuously record the physical world and gather massive amounts of data, which can then have analyzed and used to inform intelligent actions. It has changed the fundamental way we perceive the physical world and enabled our ideal of a smooth transition between the digital and physical realms. Still, the problem with existing Connectivity of The circumstances solutions is that they require a centralized entity, such as a cloud server, for interacting with one another over the Internet, whose conveys an important concern to the private nature and safety of the large amount of private facts being produced, Despite the original architectural plan called for for an autonomous one, such as a distributed or peer-to-peer (P2P) system, blockchain enters the picture, offering a reliable and secure method of information sharing through a distributed/P2P model, to achieve transparency, security, privacy, auditability, resilience, access authentication, data immutability, etc. In this paper, we will examine how to combine both technologies to get around their drawbacks and maximize their advantages. We have provided a thorough overview of the fundamentals of both technologies, as well as the blockchain-based Internet of Things (BIoT) architecture, protocols, and operation, as well as a few instances of BIoT applications that can be while the original architecture design requires constructed on top of it, for connecting and interacting via the Internet, which presents a serious risk to the security and privacy of the huge quantity of sensitive data being generated, and comparing.

Keywords: *IoT; Blockchain; Blockchain Protocol; Bitcoin.*

How to Cite: Madhuri Sharma; Dr. Arvind Mahindru; Dr. Pardeep Arora (2025). Blockchain Based Secure Data Management for IoT Devices. *International Journal of Innovative Science and Research Technology*, 10(2), 1728-1733. https://doi.org/10.5281/zenodo.14979317

I. INTRODUCTION

The Internet of Things (IoT) is a widespread network of people and intelligent physical things known as "Things." IoT turns the physical world into a vast information system through allowing any "Thing" to connect and interact. Cloud computing, machine learning, data analysis, and information modeling are just a few of the technologies that are rapidly becoming essential components of the Internet of Things. The business of information and communication technology (ICT) is expanding as a result of the amazing progress made in the IoT space. New business approaches are being made possible by IoT, and one of its most important features is data augmentation, which will have an impact on the expansion of the ICT sector. It comes readily from the fact that IoT will play a significant role in our daily lives. The Internet of Things will be at the heart of 95% of newly released devices by 2020 [1]. Bitcoin is a revolutionary system for decentralized digital currencies that uses cryptographic components to ensure its operation. Since its inception in 2009 by its obscure creator Satoshi Nakamoto, widespread interest in the currency has gradually grown, as have its applications. Despite regulatory uncertainty and underdeveloped infrastructure, the main computer science challenges for Bitcoin are its ability to scale to higher transaction rates and process individual transactions quickly. This study seeks to address both of those concerns and how they intersect with Bitcoin's security against double-spend attacks.

The Bitcoin protocol aims to replace centralized control over money transmission by a peer-to-peer network, rather than major corporations like banks and credit card firms. The network's nodes check each other's work, preventing single entities from misbehaving. Bitcoin does this by keeping a complete and public record of all transactions at every node in the network. This record, called as the block chain, is made up of a rising number of blocks, each holding a set of approved transactions. The primary obstacle that Bitcoin faces is synchronizing the ledger among many different nodes. Unsavory actors might try to disrupt synchronization and interrupt previously processed payments, causing them to utilize the same money again.[2] Bitcoin has tremendous promise as a platform for enabling small-scale payments, which are significantly smaller than what the traditional banking system can process. Indeed, you can swap an extremely tiny amount of value in a Bitcoin transaction without doing anything unusual and it will function, even if it is only a fraction of a cent. However, there are multiple significant shortcomings. At times such limitations don't matter since you only want to make a single, very modest payment and the recipient won't receive many of them regardless. Yet, such constraints can be too restrictive at times, necessitating the search for an alternate approach. This article discusses how to use payment channels, which are a method of setting up a pending transfer of value from one wallet to another so that the amount transmitted is increment able at a high rate and in very small increments. While this does not allow you to transmit micropayments at high speeds to different receivers at the same time, it can be used for a variety of applications, including micro-billing for capped applications. Beginning with bitcoinj 0.10, you may utilize payment channels to construct many types of metered billing software. We provide a sub-library that implements a client/server protocol for this, as well as an example client/server program that demonstrates its ease of use. Because payment channel technology is still new and experimental, if you want to utilize it, please contact us first and let us know what you're doing so we can guarantee you retain up on the latest as the code matures. [3]

II. OVERVIEW OF BLOCKCHAIN IN IOT

The potential of blockchain technology to improve security, transparency, and scalability in IoT ecosystems has drawn a lot of interest to its integration with the Internet of Things (IoT) in recent years. The Internet of Things (IoT) is a network of linked devices, including manufacturing equipment, smart appliances, and sensors, that gather and share data. IoT has enormous potential in a number of industries, including healthcare, manufacturing, and smart cities, but it also has serious drawbacks, especially in the areas of data security, privacy, and system dependability. A decentralized distributed ledger system called blockchain has shown promise in overcoming these issues. Blockchain can guarantee the integrity of data transferred across Internet of Things networks by utilizing its fundamental characteristics, including indestructibility, openness and an cryptographic security. The Internet of Things (IoT) and blockchain technology have the ability to completely transform how we handle and evaluate data from IoT devices, resulting in a safe, open, and effective environment. A decentralized, distributed ledger that documents transactions across a network of devices is made possible by the combination of blockchain technology and the Internet of Things, offering a safe and impenetrable record of every contact. The application of blockchain-based IoT solutions can increase productivity, save costs, and improve decision-making in a variety of businesses, spanning supply chain management, smart cities, automated manufacturing, healthcare, and transit.[4]

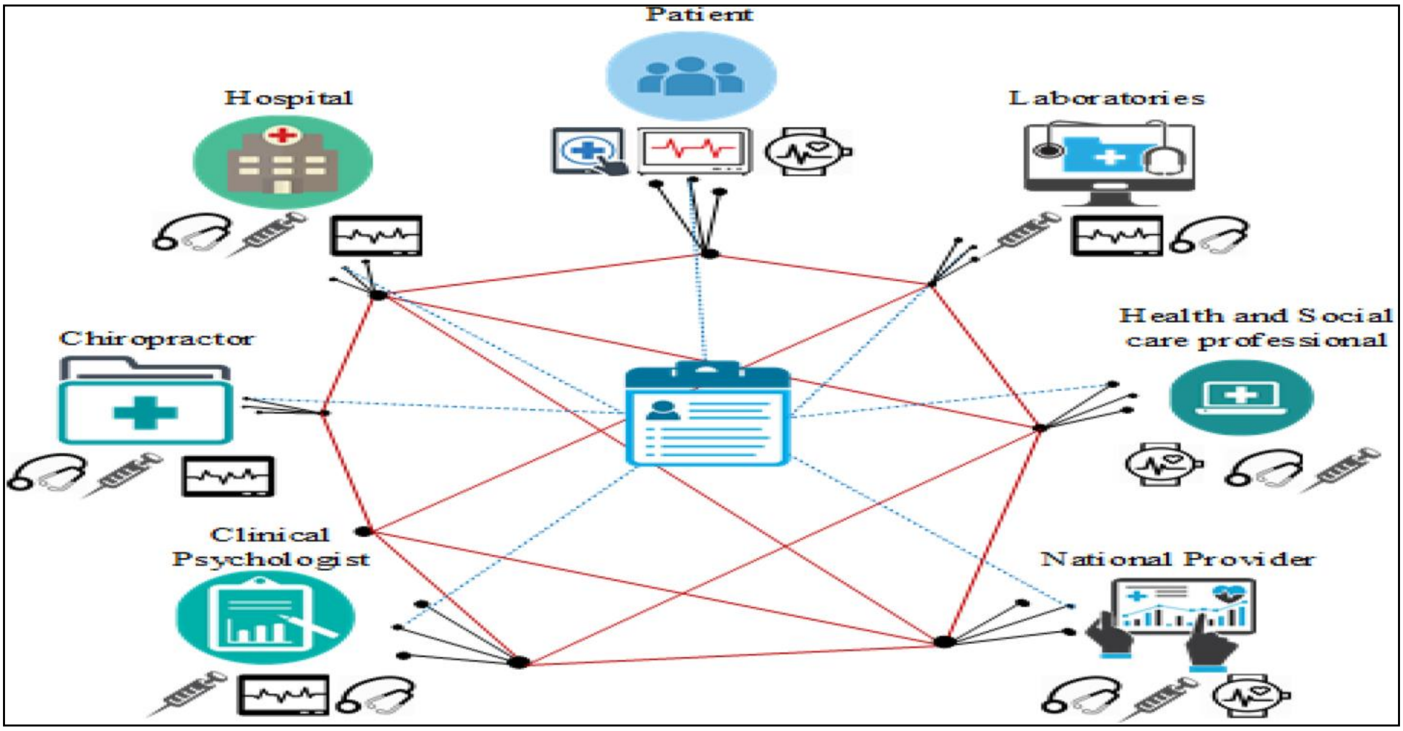

Fig 1 Architecture of Blockchain

III. BLOCKCHAIN ARCHITECTURE IN IOT

The blockchain architecture in IoT allows for secure, autonomous, and efficient interaction among devices and the network. The architecture is made up of multiple layers, such as the IoT device layer, data processing layer, blockchain network layer, and the application layer.

➢ *Hierarchical Layering*

- IoT Device Layer**:** This layer is made up of IoT devices such as sensors, actuators, and smart devices, which generate enormous amounts of data.
- Data Processing Layer: This layer analyses and analyses data generated by IoT devices using a variety of algorithms and approaches.

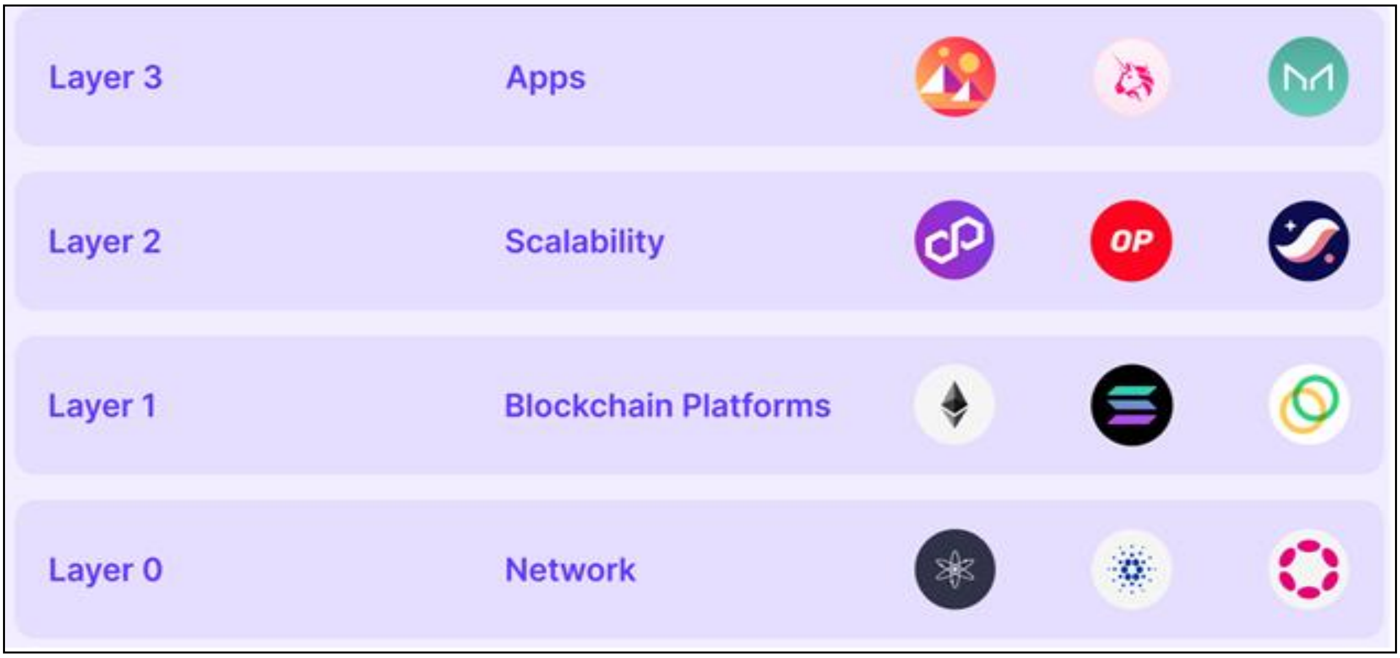

Fig 2 (Blockchain Layers)

- Blockchain Network Layer**:** This layer is the architecture's central component, where data is stored, verified, and approved via a consensus mechanism like proof-of-work or proof-of-stake.
- Application Layer: This layer is where many applications like smart contracts, data analytics, and machine learning are built on top of the blockchain network to deliver different services and capacities.

➢ *Types of Blockchain Architecture*

- Universal Blockchain: A decentralized, open-source blockchain network that anybody may join and participate in.
- Corporate Blockchain*:*A centralised and closed blockchain network managed by a single entity.
- Collaboration Blockchain: A hybrid blockchain network managed by a collection of companies.

➢ *IoT-based Blockchain Motivation*

The demand for a secure, productive, and transparent approach for handling and controlling IoT devices encourages the invention of blockchain-based IoT. As more IoT devices connect to the internet, the potential of cyber-attacks and data breaches grows. Blockchain technology offers a safe method of managing and controlling these devices by keeping a decentralised and tamper-proof record of all transactions. Furthermore, blockchain technology may automate and optimise IoT activities, decreasing the need for intermediaries while enhancing efficiency. The usage of blockchain in IoT can also allow for the construction of smart expands, which can automate a variety of IoT applications, including management of supply chains and smart cities. Blockchain has many perks in the Internet of Things, such as better security, more efficiency, and more transparency. Blockchain technology can lower the risk of cyber-attacks and data breaches by offering a secure method of managing and controlling Internet of Things devices. Furthermore, blockchain technology can streamline and automate Internet of Things procedures, eliminating the need for middlemen and boosting productivity. IoT applications like logistics administration and smart cities can be automated through the use of blockchain technology, which also makes it possible to create smart contracts. Additionally, blockchain technology can offer an unchangeable and visible record of every IoT transaction, boosting transparency and confidence in IoT networks.[5]

➢ *Blockchain Adoption in IoT*

The momentous situation regarding blockchain adoption in IoT is one of growing curiosity and early deployment. Many organisations and companies are looking at the potential benefits of employing blockchain technology in IoT applications including managing their supply chains and smart cities. Some businesses are now starting to incorporate blockchain technology into their IoT applicati ons, and many studies are being introduced to explore the viability of blockchain technology in IoT. For instance, the use of blockchain-based smart contracts to automate IoT management of devices is being investigated, and some businesses are already exploiting blockchain technology to track and control the flow of goods and products along the price chain.[6]

The potential benefits associated with using blockchain in IoT are numerous. Blockchain technology can provide a secure method of handling and controlling IoT devices, lowering the risk of cyber-attacks and data breaches. It can also automate and optimise IoT processes, decreasing the need for intermediaries while strengthening efficiency. In addition, blockchain technology can generate a transparent and tamper-proof record of all IoT transactions, promoting trust and accountability in IoT networks. Furthermore, blockchain technology can offer a safe and decentralized approach to managing and storing IoT data, lowering the danger of data breaches and cyber assaults. Overall, the application of blockchain technology in IoT has the potential to increase the security, efficiency, and transparency of IoT systems.

Table 1 Blockchain Protocols for IoT

Year	**Blockchain Adoption**
2015	10%
2016	20%
2017	30%
2018	40%
2019	50%
2020	60%
2025	80%

Numerous blockchain protocols have been proposed for IoT, including Bitcoin, Ethereum, Hyperledger Fabric, and Corda. These protocols feature varying designs, consensus techniques, and smart contract gadgets, therefore being suitable for a variety of IoT applications. For example, Bitcoin is a public blockchain protocol that is appropriate for IoT applications that require high levels of security and transparency, however Hyper ledger Fabric, on the flip side, is a private blockchain protocol that is appropriate for IoT operations that demand high levels of scalability and efficiency. The consumption of blockchain technologies in IoT offers various benefits that are including increased security, efficiency, and transparency. Blockchain protocols can provide a secure way of managing and controlling IoT devices, lowering the risk of cyber-attacks and data exposures. They can also give a visible and tamper-proof record of all transactions, which promotes trust and accountability in IoT systems. Furthermore, blockchain protocols can automate and streamline IoT activities, decreasing the need for intermediaries while strengthening efficiency.[7]

Table 2 Blockchain Protocol Categories

Category	**Description**	**Examples**
Public	Open-source	Bitcoin, Ethereum
Private	Closed-source	Hyperledger Fabric, Corda
Consortium	Combination of public and private, group of organizations control	R3, Quorum
Hybrid	Combination of public and private, flexible access control	Chaincode, Sawtooth

Innovative concepts that disrupt always provoke a lot of debate. Although there are many critics of virtual currencies, it is clear that the technology that underpins them represents a tremendous technical shift. Blockchain is here to stay. However, influencing technology without sufficiently ensuring its operation or applying it to settings where the expense does not justify for the benefit are risks that can easily be taken. As a result, the advantages of using blockchain in the IoT should be carefully considered and adopted with prudence. This article examines the key hurdles that blockchain and IoT must overcome in order to collaborate successfully. We have highlighted the primary areas where blockchain technology can enhance IoT applications.

In our viewpoint, there are numerous potential for future study directions. We believe that, in an era marked by the widespread use of smart devices and the generation of massive amounts of data (Big data), the primary two requirements are: (i) the development of a solution to ensure data privacy and integrity; and (ii) the design of a system capable of managing the unique identity of devices in a tamper-proof manner. According to the study scope distribution, research on IoT and BC is still in its early stages. Specific fields such as Smart Energy and Smart Manufacturing require extensive investigation. Being in the beginning stages, relatively little research has been done to address the challenge of scalability. The next natural step is to break down the most extensively used platforms into self-contained subsystems, which can then be assembled into full-featured stacks using standardized/pluggable components. Furthermore, defending against novel assaults such as side channel analysis might be an intriguing endeavour. Another promising study area is the use of BC to solve the problem of data interchange and trading. With the proliferation of IoT devices and the increased generation of data, attempts to monetise the data have begun, giving rise to the Machine Economy. BC can simplify the negotiation process, diminishing the need for a competent a facilitator.

IV. IOT CYBER SECURITY EXPLOTING BLOCKCHAIN TECHNOLOGY

Blockchain, IoT, and cyber security are subfields of information technology (IT), which is a branch of electrical and computer engineering. Nowadays, everything is linked to the Internet for convenience, to keep an eye on, and to manage devices worldwide. This offers the chance to automate various tasks and switch all of the gadgets that communicate to the Internet. The most significant technological advancement of the twenty-first century is the Internet of Things (IoT), which links devices from industry to homes, or from one individual to another. Manufacturing, automotive, transportation and logistics, retail, public sector, health care, and agriculture are some of the industries that use the Internet of Things.

Securing these devices and their network is required for overall safety in all industries. Data created by device-to-device communication, as well as personal information, must be secured. Cyber security courses aim to provide students with the knowledge and skills needed to protect their data, devices, and personal information from attackers. This degree opens up an abundance of opportunities in the IT sector, as well as other production and manufacturing firms. Blockchain is a distributed ledger that records information in such a way that it cannot be changed, hacked, or cheated. Because all devices are linked to the Internet, massive amounts of data are generated, which must be securely accessed from storage and made available to authorized users. Blockchain is utilized in a variety of industries, including financial transactions, lending, residential real estate, and security.

V. FUTURE OF BLOCKCHAIN IS BASED ON CYBER SECURITY FOR IOT

➢ *The Immediate Future (2023–2025)*

- **Research and development of blockchain-based threat detection and response systems**: Blockchain-based systems for detecting and responding to cyber security threats in IoT devices and systems.
- **The creation and deployment of blockchain-based identity management platforms**: For securely managing identities and authenticating devices in IoT systems.
- **Investigation and creation of the blockchain relies data encryption protocols**: For securely encrypting and protecting data in IoT devices and systems.
- **Research and development of ways** : For integrating blockchain-based cyber security solutions with existing IoT security measures like firewalls and intrusion detection systems.

➢ *Intermediate (2025–2030)*

- **Blockchain-based secure communication protocol development:** Blockchain-based secure communication protocols for securely transmitting data between IoT devices and systems are being researched and developed.
- **Development and implementation of blockchain-based cyber security exchange of data systems:** Create and deploy blockchain-based cyber security information sharing systems that make it possible IoT stakeholders to share cyber security information and best practices.
- **Investigation and creation of blockchain-based incident response systems**: Capable of responding to cyber security incidents in IoT systems in an efficient and timely fashion.
- **Study and creation of blockchain based:** Cyber security training and awareness initiatives to educate IoT stakeholders on cyber security procedures and potential hazards.

➢ *Ongoing (2030–2035)*

- Research and development of blockchain-based autonomous cyber security systems: capable of detecting and responding to cyber security threats in IoT devices.
- The creation and setting up of blockchain based cyber security systems: For industrial control systems, including those utilized in power grids and water treatment plants.
- The development of blockchain-based cyber security systems: For smart cities, such as those for safeguarding smart transportation collaborations and smart energy grids.
- Development and research of blockchain-based cyber security systems for healthcare: This includes systems for safeguarding medical devices and electronic health records.

VI. CONCLUSION

The combined use of blockchain technology and IoT has the potential to transform the way we address cyber security in the world of Internet of Things (IoT). By taking advantage of block chain's decentralized, immutable, and transparent nature, we can create a more secure and trustworthy environment for IoT devices and systems. The usage of blockchain-based cyber security solutions in IoT can give several advantages, including increased security, efficiency, and transparency. Furthermore, blockchain-based cyber security solutions can aid in mitigating the risks associated with IoT devices and systems, including data theft, cyber-attacks, and equipment manipulation.

The investigate brief discusses the present state of blockchain cyber security in IoT, including the benefits, problems, and future prospects of this new topic. The article also discusses the many blockchain-based cyber security solutions that are being developed and used in IoT, including blockchain-based threat detection, identity management, and data encryption. Furthermore, the study investigates the significance of blockchain in IoT cyber security, particularly its ability to create a safe and trustworthy environment for IoT devices and systems to work in. The report also discusses the constraints and limitations of blockchain-based cyber security solutions for IoT, such as scalability, interoperability, and regulatory issues.

In conclusion, the combined use of blockchain technology and IoT may offer a more reliable and safe operational setting for IoT systems and devices. The usage of blockchain-based cyber security solutions in IoT can give several advantages, including increased security, efficiency, and transparency. However, there are several obstacles and constraints to using blockchain-based security solutions in IoT, such as scalability, interoperability, and regulatory problems. More research is needed to fully understand the potential for blockchain-based cyber security solutions in IoT, as well as the challenges and limitations connected with their application.

REFEREENCES

[1]. Newsroom, G. Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018. Available online: **https://www.gartner.com/newsroom/id/3869181** (accessed on 30 March 2018).

[2]. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: Financial Cryptography and Data Security, pp. 34–51. Springer (2013)

[3]. Lewenberg, Y., Sompolinsky, Y., Zohar, A.: Inclusive block chain protocols. In: Financial Cryptography and Data Security. Springer (2015)

[4]. Andrew Miller, Elaine Shi, Ahmed Kosba, and Jonathan Katz. Preprint: Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions.

[5]. Alphand, Olivier, et al. "IoTChain: A blockchain security architecture for the Internet of Things." Wireless Communications and Networking Conference (WCNC), 2018 IEEE. IEEE, 2018.

[6]. Jon Wood, 'Blockchain of Things—cool things happen when IoT & Distributed Ledger Tech collide', April 2018,

[7]. Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," IEEE Access, vol. 6, pp. 45655–45664, 2018.

[8]. T. Le and M. W. Mutka, "CapChain: A privacy preserving access control framework based on blockchain for pervasive environments," in Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP), Jun. 2018.

[9]. K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun. IEEE 14th Int. Conf. Smart City IEEE 2nd Int. Conf. Data Sci. Syst., Sydney, NSW, Australia, 2016.

[10]. A. Kiayias and G. Panagiotakos, "Speed-security tradeoffs in blockchain protocols," in Proc. IACR Cryptol. ePrint Archive, vol. 2015, 2015.

[11]. Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong, "A blockchainbased storage system for data analytics in the Internet of Things," in New Advances in the Internet of Things. Cham, Switzerland: Springer, 2018.

[12]. S. Sicari, A. Rizzardi, C. Cappiello, D. Miorandi, and A. Coen-Porisini, "Toward data governance in the Internet of Things," in New Advances in the Internet of Things. Cham, Switzerland: Springer, 2018.