ACE Journal of Computer Science and Engineering

Research Article
doi: 10.36478/makacejcse.2024.1.1.8

OPEN ACCESS

Key Words
Index terms-block chain, IoT, internet of things, challenges, threats, security

Corresponding Author
Charlotte Jennifer Philips,
Department of Computer and Information Science Gannon University 109 University Square Erie, PA 16541

Received: 25 December 2023
Accepted: 22 April 2024
Published: 15 May 2024

Citation: Charlotte Jennifer Philips and Tejas Veeraganti Manjunath, 2024. Securing the Internet of Things: Harnessing Block Chain Technology for Enhanced Privacy and Protection. ACE J. Comput. Sci. Eng., 3: 1-8, doi: 10.36478/ makacejcse.2024.1.1.8

Securing the Internet of Things: Harnessing Block Chain Technology for Enhanced Privacy and Protection

[1]Charlotte Jennifer Philips and [2]Tejas Veeraganti Manjunath
[1-2]Department of Computer and Information Science Gannon University 109 University Square Erie, PA 16541

Abstract
The rapid growth of the Internet of Things (IoT) has resulted in significant progress in home automation and remote sensing. However, this expansion has brought with it new privacy and security concerns, such as the risk of cyberattacks, a lack of centralized design and insufficient resources to monitor and implement security measures. Furthermore, the traceability of sensor-generated data compromises user privacy. Block chain technology, which is a decentralized, distributed and public digital ledger, provides a promising solution to these issues. This paper investigates the advantages of integrating blockchain tech- nology with IoT, emphasizing privacy preservation via pseudony-mous addresses, access control, encryption and other techniques. Furthermore, we discuss how blockchain promotes accountability and resilience in IoT networks by enabling transparency, trace- ability and distributed architecture.

INTRODUCTION

The Internet of Things abbreviated as IoT is a network that allows ”things” or embedded devices that contain sensors to communicate with one another through either a private or public network. A result of the fact that the devices that are a part of the Internet of Things (IoT) generate, analyze and communicate copious amounts of data that is not only highly personal in nature but also essential to the protection and safety of individuals, these devices have become prime targets for a wide variety of cyberattacks[1]. Some of the most recent networked devices that make up the Internet of Things are very lightweight and have low power consumption. These devices face a significant obstacle in the shape of a daunting challenge in terms of providing acceptable security and privacy at an affordable cost. This is because they must prioritize the execution of important application functionality. Traditional security approaches are often impractical for use with the Internet of Things due to the significant amounts of energy and processing overhead they require. Because of the many-to-one structure of the traffic, the complexity of scale and the single point of failure that excessively centralized security frameworks bring, many of the most cutting-edge security

frameworks are not well suited to the Internet of Things (IoT)[2]. Existing methods sometimes reveal noisy data or partial data in order to preserve the privacy of users, which may result in certain Internet of Things apps being unable to provide personalized services to users. Because of this, the Internet of Things requires a privacy and security mechanism that is straightforward, expandable and distributed. The pervasive-ness of IoT’s use in conventional activities sheds light on the field’s potential future importance. It continues to expand at a high rate as a result of the continuous development of new hardware solutions, such as expanding bandwidth through the incorporation of cognitive radio-based networks in order to combat the underutilization of the frequency spectrum[3]. As more and more gadgets connect to the internet, there will be more chances for people to exchange and keep track of their personal data. In spite of the fact that this paves the way for a myriad of new service alternatives, concerns over the data’s privacy and security have been raised as a result[4]. Unfortunately, the present ways to protect the privacy and security of IoT devices have a limited capacity for scaling, and this requires placing faith in a centralized organization[5]. This demonstrates how essential it is for the Internet of Things to have decentralized trust mechanisms.

A trustworthy Internet of Things network might potentially be built using blockchain technology, which is quite exciting. Blocks are collections of data that are used in blockchain technology to register transactions. Blockchain is a decentral- ized, append-only database that is distributed across multiple computers[6]. Blockchain, the technology that underpins Bit- coin and was initially proposed by Satoshi Nakamoto, makes use of peer-to-peer networking, public key cryptography, and distributed databases to enable secure, distributed consensus among a network’s nodes without the need for a trusted third party to mediate the process[7,8]. Peer-to-peer networking allows users to communicate directly with one another, while public key cryptography and distributed databases store information. When using a blockchain network, miners adhere to a technique known as distributed consensus in order to construct blocks. These blocks are then put to use to hold a sequence of

Transactions that are tied to one another. The very first block that is added to a blockchain is referred to as the genesis block. A reference to a cryptographic hash connects each successive block in the chain to the block that came before it. This connection cannot be severed. Any attempt to change the contents of a block would be promptly discovered due to the fact that the hash value of the altered block would cause an inconsistency in the hash values of future blocks. Therefore, if you wish to make a modification in a block that no one else sees, you will need to renew all of the blocks that come after it using the consensus procedure, which might take a significant amount of time and effort. This time-consuming and expensive technique protects against an attack in which malicious users attempt to change the data contained within blocks. Due to the fact that it is a distributed ledger, each node in the network possesses its own copy of the blockchain. As a consequence of this, it is safe in the event that a node fails or an attack is launched against a node.

Literature Review: The authors of the paper titled “Blockchain Technologies for IoT” state that due to the rise in the number of Internet- connected devices that are equipped with sensing, processing and communication capabilities, developers have created a plethora of IoT applications that foster smart environments, facilitate device-to-device communication and pave the way for novel business models[9]. The authors of the paper also state that this rise in the number of Internet-connected devices has resulted in an increase in the number of cyberattacks. They explain that Internet of Things (IoT) devices are

able to collect data, do analysis on it and distribute it thanks to the interactions those devices have with one another and the settings in which they operate. In addition, the development of applications for the Internet of Things (IoT) is hampered by a lack of attention paid to the reliability of data, as well as security and privacy concerns. Blockchain technology has recently garnered a lot of attention from academic institutions as well as corporations due to the fact that it has the potential to improve data security, privacy, and dependability. The authors also state that smart contracts can be used to auto-matically execute programs based on predefined criteria and that distributed ledgers provide tamper-proof records for IoT connections. Both of these benefits can be derived from using blockchain technology. Incorporating blockchain technology into the Internet of Things (IoT) could be beneficial, but doing so would offer substantial challenges in the design of blockchains that is best suited for IoT characteristics, such as scalability. Their paper aligns with our argument that blockchain could be one of the potential solutions to the problems faced in IoT. In addition to this, they discuss the challenges involved in implementing blockchain technology within an Internet of Things (IoT) system.
The authors of the paper titled ”Blockchain for IoT Security and Privacy: The Case Study of a Smart Home” state that security and privacy in the Internet of Things (IoT) are significant issues due to the sheer size and dispersed nature

Of IoT networks[10]. The authors of the paper also stated that blockchain technology could be used to address these issues. Blockchain-based systems may provide decentralized security and anonymity, but it is unlikely that most Internet of Things devices will be able to make use of them because of the high energy, latency and processing costs associated with them. In recent work, they proposed an implementation of a blockchain that is streamlined and efficient, making it an excellent choice for Internet of Things applications. They demonstrated that a smart house is comprised of three key elements, which are cloud storage, an overlay and the smart home itself. They investigated the smart home layer in further depth and detailed its fundamental functions and components in their article. A single, high-capacity device that is permanently linked to the internet manages all of the internal and external communication in a smart home. In addition to this, the miner on the device maintains a private blockchain that can be used to monitor and control all messages going out and coming in. They demonstrated that their blockchain-based smart home system satisfies the core security goals of confidentiality, integrity and availability by conducting an in-depth analysis of the system and demonstrating that it satisfies the minimum security standards established by those goals. Finally, the authors present simulation findings to demonstrate that the approach’s advantages in terms of security and privacy outweigh the approach’s drawbacks in terms of overhead (in terms of traffic, processing time, and energy usage). This demonstrates that blockchain technology has the potential to be an efficient and low-overhead solution for the Internet of Things area.

The Internet of Things (IoT) has emerged as a field of enor-mous significance, potential and growth with the introduction of smart homes, smart cities and smart everything, with Cisco Inc. estimating 50 billion connected devices by the year 2020. The authors of the paper IoT security review blockchain solutions and open challenges say this has occurred as a result of the proliferation of smart homes, smart cities and smart everything[11]. They also mentioned that to make problems much worse, the majority of these Internet of Things gadgets are simple to hack and utilize in malicious ways. Because the computing power, storage capacity and network connectivity of these Internet of Things devices are often inferior to those of other endpoint devices such as smart phones, tablets, or personal computers, they are more vulnerable to attacks. In this report, they describe and survey some of the most significant security problems regarding the Internet of Things. They take a look at the widespread security problems that surround the layered architecture of the Internet of Things as well as the accompanying networking, communication and management protocols and then categorize those concerns according to the type of issues that they provide. They also discuss the importance of Internet of Things (IoT) security, in addition to describing the most recent attacks, dangers and innovative solutions. In addition, they produce a table as well as a map to illustrate the relationship between IoT security problems and previously published solutions. They discuss

how blockchain technology has the potential to become an important enabler in the process of resolving a number of Internet of Things security problems. This study is consistent with our philosophies, which hold that blockchain technology is one of the most effective solutions to problems relating to the security of the internet of things (IoT).

Security Issues and Their Categories: In the context of the Internet of Things (IoT), security issues can be categorized based on the threat level or potential impact of the attack. This can help organizations prioritize their efforts to address different security risks and allocate appropriate resources to mitigate the most serious threats. For example, security issues in IoT can be categorized as follows:

1. **Low-level Threats:** These are security issues that have a minimal impact on the confidentiality, integrity, or availability of IoT devices and systems. They may involve minor breaches of security, such as unauthorized access to a device's interface or unauthorized data access. A good example of low-level security issues in IoT include gain-ing unauthorized access to a device's interface: This type of security issue involves someone gaining unauthorized access to the user interface of an IoT device, such as a smart thermostat or security camera. This may allow the attacker to view the device's settings or manipulate its functions, but it would not allow them to access sensitive data or control the device's core functions
2. **Medium-level Threats:** These are security issues that have a moderate impact on the confidentiality, integrity, or availability of IoT devices and systems. They may involve more serious breaches of security, such as unauthorized access to a device's firmware or unauthorized access to sensitive data. A good example of medium-level security issues in IoT include gaining unauthorized access to sen-sitive data: This type of security issue involves someone gaining unauthorized access to sensitive data generated by an IoT device, such as financial information or personal health data. This may allow the attacker to view, modify, or steal the data, potentially causing serious harm to the device's owner or the organization that operates the device.

- **High-level Threats:** These are security issues that have a significant impact on the confidentiality, integrity, or availability of IoT devices and systems. They may in-volve major breaches of security, such as unauthorized access to a device's control functions or unauthorized access to critical data. These threats may pose a serious risk to the organization's operations and may require urgent attention to mitigate the potential damage. A good example of high-level security issue in IoT in-clude gaining unauthorized access to a device's control network: This type of security issue involves someone gaining unauthorized access to the control network that connects multiple IoT devices, such as a smart home network or industrial control system. This may allow the attacker to manipulate multiple devices simultaneously potentially causing widespread damage or disruptions to the organization's operations.

By categorizing security issues in IoT based on the threat level, organizations can prioritize their efforts to address different security risks and allocate appropriate resources to mitigate the most serious threats. This can help ensure that the organization's IoT devices and systems are adequately protected against a wide range of security threats.

Blockchain Solutions for Security in IOT: The Internet of Things (IoT) has transformed many indus-tries by enabling seamless connectivity between devices such as sensors, actuators and appliances. This interconnectivity allows for the exchange of data and the development of new levels of automation and control[11]. However, the prolif-eration of IoT devices raises serious security concerns. IoT devices, which frequently have limited computing power and storage, are vulnerable to hacking and other security threats. The vast number of interconnected devices complicates the overall security of the IoT ecosystem. As a result, individuals and organizations must address the security implications of IoT technology and put strong safeguards in place to protect their devices and data.

Blockchain technology has the potential to provide en-hanced security for the Internet of Things (IoT). A blockchain is a distributed database that maintains a continuously growing list of ordered records, called blocks. Each block contains a timestamp and a link to the previous block, making it resistant to tampering and revision. Because of its decentralized, transparent and tamper-proof nature, blockchain technology offers promising solutions for improving security in IoT networks. In this section, we discuss the key attributes of blockchain that make it an ideal solution for IoT applications

- **Decentralized Architecture:** Blockchain technology elim-inates the need for a central authority by utilizing a distributed database, which can prevent single points of failure and reduce vulnerability to attacks. By using blockchain, IoT devices can securely share and store data without the need for a central authority. By ensuring that there is no single point of failure, the decentralized approach can deter hackers from compromising the system[12]
- **Data Immutability:** Blockchain is resistant to tampering and revision because of its inherent structure of ordered, timestamped blocks linked to their predecessors. IoT devices can use blockchain to securely store and share data, ensuring data integrity and adding an extra layer of security

- **Cryptographic Security:** Blockchain uses cryptographic techniques such as public-private key pairs to ensure secure communication and data exchange between IoT devices. This improves data confidentiality and integrity, making it more difficult for malicious actors to intercept or manipulate the information
- **Scalability and Efficiency:** Blockchain technology can handle a large number of IoT devices and their data, allowing for secure and efficient data storage and manage-ment, which is essential for large-scale IoT deployments
- **Interoperability:** Blockchain technology can enable seam-less communication and data exchange among hetero- geneous IoT devices and systems, allowing for greater collaboration and streamlined processes across a wide range of applications and industries

Additionally, the use of cryptographic techniques in blockchain can provide an additional layer of security for IoT devices. Overall, the use of blockchain in IoT can help to improve the security and reliability of connected devices. Here, in this section, we explore and highlight some of blockchain’s core qualities that make it well-suited for Internet of Things (IoT) applications, especially in the realm of IoT security.

Security for Identity of Things: Identity of Things (IDoT) is a concept that refers to the ability of IoT devices to have a unique and verifiable identity, just like individuals and organizations do. This can be useful for a variety of purposes, such as ensuring the authenticity and integrity of IoT devices, enabling secure communication between them and enabling access control and permissions management. When it comes to the Internet of Things, one of the biggest problems is figuring out who owns what. Throughout its existence, a product may pass from the hands of the producer to those of the supplier to the merchant to the consumer[13]. If an Internet of Things device is resold, deactivated, or compromised, the consumer can lose ownership of the device. An additional difficulty is managing the attributes and connections of an IoT device. Manufacturer, model, kind, serial number, deployment GPS coordinates, location, etc. are all examples of device attributes. IoT devices have connections, in addition to traits, capabilities and functions. Relationships within the IoT can be human-device, human-device, or human-service. Relationships with Internet of Things devices might include deployment, use, shipment, sale, upgrade, repair and resale.

Blockchain technology has the potential to play a role in enabling and managing IDoT, by providing a decentralized and secure platform for storing and managing the identity of IoT devices. Through the use of digital signatures and smart contracts, blockchain can provide a tamper-resistant and verifiable means of assigning and managing the identity of IoT devices. This can help to prevent counterfeiting and tampering and ensure that only authorized devices are able to access networks and resources. In terms of governance, the decentralized nature of blockchain can provide a transparent and auditable means of managing the processes and policies governing the identity of IoT devices. This can help to ensure that the IDoT system is fair, accountable and transparent and can give stakeholders visibility into and control over the identity management process. Additionally, the use of smart contracts can automate the enforcement of IDoT policies and regulations, helping to ensure compliance and reducing the potential for human error. Overall, the combination of IdoT and blockchain has the potential to provide enhanced security, trust and transparency for the Internet of Things.

Security for Communications: Communication protocols used by IoT applications, such as HTTP, MQTT, CoAP, or XMPP and routing protocols, such as RPL and 6LoWPAN, are not built with security in mind. For messaging and application protocols to allow secure communication, they must be encapsulated within additional security protocols like DTLS or TLS. Routing protocols like RPL and 6LoWPAN commonly employ IPSec for safety reasons. The popular PKI protocol is used for key management and distribution, although it is computationally and memory-intensive compared to other popular protocols like DTLS, TLS, IPSec and even the lightweight TinyTLS. by using blockchain, as soon as an Internet of Things (IoT) device is installed and connected to the blockchain network, it will have its own unique GUID and asymmetric key pair, eliminating the need for any kind of key management or distribution. There will be no need to deal with and exchange PKI certificates during the handshake phase of DTLS, TLS, or IPSec in order to negotiate the cipher suite settings for encryption and hashing and to establish the master and session keys, which will significantly simplify the security protocol. As a result, it’s easier to imagine lightweight security mechanisms that could accommodate and stratify the needs of the limited processing power and storage space of IoT devices.

Security in Supply-Chain: Blockchain technology has the potential to enhance the use of the Internet of Things (IoT) in supply chain management. Blockchain is a distributed database that allows for the secure and transparent tracking of transactions. This can provide an immutable record of the movement of goods

Other IoT challenges and potential blockchain solutions

IoT Challenge	Potential Block chain Solution
Having a flawed design in which any one component of the Internet of Things architecture has the potential to bring down the entire system; being susceptible to DdoS attacks, hacking, data theft, and remote hijacking; and so on.	To ensure that only the intended recipient received a message, its authenticity must be validated, and all transactions must be crypto graphically signed and authenticated.
Servers in the cloud can go down for a variety of reasons, including cyberattacks, software issues, power outages, overheating, and lack of cooling.	There is no single point of failure because data is spread across multiple computers and storage devices.
Information can be easily manipulated and misused.	Due to its immutability and decentralized nature, malevolent actions can be thwarted. When the security of a device's blockchain updates is device's blockchain a whole will not accept the updates is compromised, the system as update.
Increased IoT expansionis accompanied by rising costs and capacity restrictions.	Using blockchain thereis no longer a requirement for a central authority, as smart contracts enable decentralized autonomous device-to-device communication, value exchange, and action execution.

through the supply chain, allowing for better tracking and visibility. By combining blockchain with IoT technology, it is possible to create a ”smart” supply chain that can automatically track and record the movement of goods in real time. For example, IoT sensors attached to shipping containers could automatically record data such as location, temperature and other relevant information, which could then be added to the blockchain. When an IoT security vulnerability is discovered, it allows for targeted containment. Product recalls due to security flaws are only one example of a crisis situation that blockchain tech-nology may help mitigate and manage. Due to blockchain's transparency, it is feasible to track down the origin of any given goods, down to the raw components and to correlate transactions in order to single out the owners of potentially vulnerable Internet of Things gadgets. This would provide a secure and transparent record of the movement of goods through the supply chain, allowing for better tracking and accountability. Considering a real-life example, if supply chains had implemented blockchain, problems like the cyberattacks on Dyn, which were tied to the Internet of Things, could have been handled more effectively. Internet-connected camera and accessory manufacturer Hangzhou Xiongmai Technologies of

China recalled affected goods in the United States due to the threat posed by the Mirai malware[14]. However, tracing their rightful owners was a challenging task. Overall, the combination of blockchain and IoT in the supply chain can help improve the efficiency and transparency of supply chain operations.

Smart Contracts for Automation and Access Control: Smart contracts based on blockchain technology can be used to automate numerous jobs in IoT networks, such as triggering certain actions when certain circumstances are ful-filled. These programmable contracts can also enforce access control restrictions and manage permissions, ensuring that only authorized people or devices are allowed to do particular tasks, hence increasing security[15]. Smart contracts are self-executing contracts in which the conditions of the parties' agreement are directly encoded into lines of code. They are kept on a blockchain platform and are intended to auto-matically facilitate, verify and enforce contract negotiation or performance. They are essential in IoT networks because they automate procedures and enable access management, improving security and efficiency. In this section, we will go over smart contracts in further detail for automation and access control. Smart contracts may be employed to manage IoT devices, data and service access. They can impose fine-grained access control policies that specify who has access to specific devices or resources, as well as the circumstances under which access is provided. You may strengthen the security and privacy of the IoT ecosystem by specifying access control rules in smart contracts. This ensures that only authorized parties can access or operate IoT devices and their data. For example, before allowing access to sensitive data created by an IoT device, a smart contract may demand multi-factor authentication or confirmation from various parties. A smart contract can also be used to design and manage roles and permissions, ensuring that each member in the IoT network has access to only the information and functions relevant to their role.

When certain circumstances are met, It can also be pro-grammed to perform predetermined actions. In the context of IoT, it can automate a variety of procedures and functions, including device registration, data exchange and billing. A smart contract, for example, may automatically activate an IoT device after it has been confirmed and registered on the network. This automation eliminates the need for manual in- tervention, streamlines procedures and reduces the likelihood of human error or fraud. They can enable smooth interaction between multiple IoT devices, systems and platforms because they are platform-agnostic and can connect with other smart contracts. This enables secure data interchange and collabora-tion between different applications and sectors, resulting in a more efficient and secure IoT environment.

Smart contracts in IoT networks provide transparency and auditability. All smart contract operations are recorded on the blockchain, making it simple to track and verify any modifications or transactions. This can aid in the detection of illegal access or fraudulent activity, as well as in regulatory compliance. There is also an increase in cost savings and efficiency as it can assist to minimize the time and effort required for manual management and administration in IoT networks. It does this by automating operations and enabling access control. Finally, by automating procedures and enabling access management, smart contracts play a critical role in improving security and efficiency in IoT networks. Their self-executing, transparent nature ensures that only authorized parties may access and control IoT devices and data, resulting in a more interconnected ecosystem. They are able to enable secure data interchange and collaboration between different applications and sectors, resulting in a more efficient and secure IoT environment.

CONCLUSION

The Internet of Things (IoT) has made significant advances in today's increasingly interconnected world, ushering in a new era of automation and data interchange. However, the current state of IoT devices is rife with security flaws, making them vulnerable to hackers. These vulnerabilities are exacerbated by the limited resources accessible to IoT devices, the lack of established standards and the absence of secure hardware and software design, development and deployment procedures. Furthermore, the sheer variety of IoT resources hampers the development of a comprehensive, worldwide framework for protecting the various layers of the IoT ecosystem.

We examined and classified IoT security risks in this research based on threat levels, which included high-level, intermediate-level and low-level threats. This classification enables firms to prioritize security risks and more effectively deploy resources, focusing on mitigating the most serious threats. Furthermore, we investigated how blockchain technol-ogy may be used to address and fix some of the most important IoT security challenges.

Blockchain solutions are decentralized, transparent and tamper-proof, which can improve the security, privacy and dependability of IoT networks. We can improve the secu-rity of IoT devices and the data they generate by utilizing blockchain technology and its inherent characteristics such as smart contracts, cryptographic approaches and a distributed architecture, while simultaneously retaining user privacy and optimizing procedures. As the Internet of Things expands and integrates into more industries and applications, solving its security flaws becomes increasingly important. We can build a strong, scalable, and secure foundation for the IoT ecosystem by implementing blockchain technology. By doing so, we not only preserve users' privacy and security but also ensure that IoT technology may fully achieve its potential in altering our connected world.

REFERENCES

1. Sicari, S., A. Rizzardi, L.A. Grieco and A. Coen-Porisini, 2015. Security, privacy and trust in internet of things: The road ahead. Comput. Net., 76: 146-164.
2. Roman, R., J. Zhou and J. Lopez, 2013. On the features and challenges of security and privacy in distributed internet of things. Comput. Net., 57: 2266-2279.
3. Mohanta, B.K., D. Jena, U. Sata pathy and S. Patnaik, 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things, Vol. 11 .10.1016/j.iot.2020.100227.
4. Mohanta, B.K., D. Jena, S. Ramasubbareddy, M. Daneshmand and A.H. Gandomi, 2021. Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet Things J., 8: 881-888.
5. Banerjee, M., J. Lee and K.K.R. Choo, 2018. A blockchain future for internet of things security: A position paper. Digital Commun. Networks, 4: 149-160.
6. Agrawal, R., P. Verma, R. Sonanis, U. Goel, A. De, S.A. Kondaveeti and S. Shekhar, 2018. Continuous security in iot using blockchain. EEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), April 15-20, 2018, IEEE, Canada, pp: 6423-6427.
7. Congressional Research Service, 2021. U.S.-China Trade Relations., https://crsreports.congress.gov/product/pdf/IF/IF11284/13.
8. Lin, I.C. and T.C. Liao, 2017. A survey of blockchain security issues and challenges. Int. J. Net. Secur., 19: 653-659.
9. Dedeoglu, V., R. Jurdak, A. Dorri, R.C. Lunardi, R.A. Michelin, A.F. Zorzo and S.S. Kanhere, 2019. Blockchain Technologies for IoT. In: Advanced Applications of Blockchain Technology, Kim, S. and G.C. Deka, (Eds.)., Springer Singapore, Singapore, ISBN-27: 9789811387746,9789811387753, pp: 55-89.

10. Dorri, A., S.S. Kanhere, R. Jurdak and P. Gauravaram, 2017. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), March 13-17, 2017, IEEE, USA, pp: 618-623.
11. Khan, M.A. and K. Salah, 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Comput. Syst., 82: 395-411.
12. Sengupta, J., S. Ruj and S.D. Bit, 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Network Comput. Appl., Vol. 149 .10.1016/j.jnca.2019.102481.
13. Granjal, J., E. Monteiro and J.S. Silva, 2010. Enabling Network-Layer Security on IPv6 Wireless Sensor Networks. IEEE Global Telecommunications Conference GLOBECOM 2010, December 06-10, 2010, IEEE, USA, pp: 1-6.
14. Kshetri, N., 2017. Can blockchain strengthen the internet of things? IT Professional, 19: 68-72.
15. Bindra, L., C. Lin, E. Stroulia and O. Ardakanian, 2019. Decentralized Access Control for Smart Buildings Using Metadata and Smart Contracts. IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), May 28-28, 2019, IEEE, Canada, pp: 32-38.