Science Arena Publications
Specialty Journal of Electronic and Computer Sciences
ISSN: 2412-7485
Available online at www.sciarena.com
2019, Vol, 5 (1): 30-40

Challenges and Weaknesses on Security in Internet of Things and Resolving these Challenges Using Blockchain Technology

Mohammad Mahdi Abdiyan[1]*, Mohammad Reza Hasani Ahangar[2], Majid Ghayouri Sales[3]

[1]MSc Student of Secure Computing - Imam Hossein Comprehensive University, Iran.
[2]Associate Professor, Department of Computer Engineering- Imam Hossein Comprehensive University, Iran.
[3]Assistant Professor, Department of Computer Engineering, Imam Hossein Comprehensive University, Iran.

***Corresponding Author**

Abstract: *Internet of Things is now regarded with heightened interest among the scientific community, as well as the market and trade, and is being rapidly developed; it is expected to evolve rapidly and more inclusive in the future. The issue of maintaining security between the components of network and confidentiality of information exchanged between different nodes is one of the most important challenges and concerns raised in IoT, which caused a lot of concerns for developers and users of this technology. This review article examines the layered structure of the Internet of Things and security issues of every layer, the traditional methods, as well as new approaches such as the blockchain, which is the main focus of this study, in order to overcome these challenges and weaknesses.*

Keywords: *Internet of Things, Layered Architecture, Layer Security weaknesses, Weaknesses and Security Challenges, Security Strategies.*

INTRODUCTION

The term Internet of Things was firstly introduced by Kevin Ashton in 1999. The IoT is generally the extension of non-uniform and heterogeneous devices and systems. It is also defined as a network of connected different entities and things that are available anywhere and anytime. For example, IoT entities include smart homes, smart cars, and wearable items such as smart watches, smart phones, and the like (Mahmoud *et al.*, 2015). Some research institutes, including Gartner Inc and Cisco Corporation, forecast that the number of connected IoT nodes will reach tens billions (26-50 billion) by 2020 (Mahmoud *et al.*, 2015). The components of IoT can be divided into two physical and virtual categories (Das, Zeadally and He, 2018): the physical objects include smart phones, security cameras, cars and .., and virtual objects, such as e-purses, e-books, e-cards, e- ticket, etc. The IoT architecture consists of several layers and the majority of sources split it into three layers namely physical (perceptual) layer, network layer (transport), and application layer. The following sections present a detailed description of the above layers. Some definitions and terms used in IoT domain include:

Edge (Fog) Computing and its application in IoT: Fog computing, a term developed and analyzed by Cisco company, refers to extending computing to the edge of sensors (data creation or collection devices), which are available in the bottom layer (availability level). It accelerates some detections and initial processing at the

edge, as well as prevents the traffic and wastage of the communications' bandwidth needed between the lines rather than performs all processes and storage in the core network including cloud or other resources.

Lightweight Protocols: In IoT, lightweight protocol is characterized by limited resources consumption like processing load, energy, memory and cost, which provide the necessary conditions for a level of stability in IoT with inadequate equipment.

Security issues in IoT include the following: the maintenance of confidentiality, cryptography, integrity, access control level, authentication and prevention of non-repudiation, and other challenges due to some problems in the application of traditional security mechanisms requiring a lot of memory and power (energy) and bandwidth, which contradicts the essence of most IoT components including battery-powered devices, with limited memory and bandwidth. The other problem can be related to the heterogeneity of components in IoT, which made it difficult to authenticate and create harmony between the components. In what follows, we try to comprehensively analyze these security issues and offer some approaches and mechanisms to overcome these challenges. For instance, the use of sensors, interfaces and low-power protocols can resolve the energy consumption challenge. In addition, cryptographic techniques and general-purpose authentication of IoT could be used to solve these security challenges (Conti *et al.*, 2018). Software-defined networking (SDN) technology and block-chains are two of the most promising new ways to maintain secure in IoT:

Software-defined networking (SDN) technology is an approach to network management and monitoring the separated data which is programmable for the automatic implementation of the tasks leading to the greater flexibility for network administrators (Kalkan and Zeadally, 2018).

Blockchain technology is an emerging technology, a database or a distributed ledger secured with unauthorized modified stored information, which offers a wide variety of services in different sectors for us according to its distributed trust management system and its reliable structure. One of the most widely used areas of this technology is related to financial issues and exchange coding, as well as security issues, documentary protection, insurance, Internet applications and the Internet of Things (Nofer *et al.*, 2017).

This distributed and decentralized blockchain approach helps us to move away from the centralized structures that require sophisticated high-power computing devices to secure, which ensures the provision of desired security through decentralized system and the lack of need for very complicated hardware; in what follows, we will look deeply into this new approach (Kouicem, Bouabdallah and Lakhlef, 2018).

Terms used in the blockchain:

The blockchain consists of two main components including distributed file and software that performs the validation and verification operations. There is no central system or single centralized file to update the block chain. The blockchain is viewed as a book containing pages (blocks); but a special ledger that its pages cannot be split up or information that modified the written text!

There is no certainty in security; therefore, this system can be modified and hacked. Like many systems, this modified or hacked file cannot be removed through leaking process or changes. In doing so, at least 51% of the transaction cycle systems should to be attacked simultaneously and undergo a change, which is practically impossible.

File: In blockchain, file is a component or subcomponent of the technology, which is equally shared across a large number of computers.

Block: block refers to each smaller part of the file (pages of a book).

Chain: chain refers to an interconnection and hierarchy between the blocks, which similar to a hyperlink in the data structure.

Hash: hash refers to a tag and symbol used as a validity sign on each block

Peer: peer refers to anyone or device that holds a copy of the file.

Bitcoin: Bitcoin is a well-known secret alphanumeric number across thousands of technologies based on the blockchain technology.

Trust: Trust can be analyzed from two perspectives: one relies to the origin and base of the blockchain system due to open access to the source and its history to the public. Another is trust to its reliable performance due to the decentralized nature and appropriate distribution of this technology, the accuracy of transactions by using mathematical calculations, and the strong connections between blocks and the impossibility of deleting or destroying information.

Miner: Miner refers to the effort and activity of the device or person to calculate and verify the hash number

Nonce: Nonce refers to an arbitrary number that is used once, or the number that is added to the hashed blocks. It is mainly used for applying difficulty level restrictions to return hash. It also refers to the number that blockchain miners are solving for.

Proof of work: Miners verify that transactions within each block are legitimate. To do so, miners should solve a mathematical puzzle known as proof-of-work problem. A reward is given to the first miner who solves each blocks problem. Verified transactions are stored in the public blockchain. A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated.

Smart contract: A smart contract, also known as a cryptocontract, is a computer program that directly controls the transfer of digital currencies or assets between parties under certain conditions. These contracts are stored on blockchain technology, a decentralized ledger that also underpins bitcoin and other cryptocurrencies. They also help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

Anonymity: In this technology, which is literally a form of pseudo-anonymity, we use a particular and unique number for each peer of system. The number is recorded. This definition is slightly different from the anonymity, in which is there is no way to trace its source.

After the analyzing this article review, we are familiar with the layered architecture of the Internet of Things, analyze the weaknesses of each layer and identify the security and macro challenges of each layer in IoT. Then, we learn the modern security solutions used in this area, as well as new ways of using the block chain for the security of the Internet of objects, and finally, try to identify the most comprehensive and optimal methods and functions for resolving the security challenges.

2- Architecture and layered structure of IoT

2-1. Three-tier architecture (3Tier) of IoT:

The Internet of things does not support a single standard, but according to most of the resources, including the ITU Association, the most basic architecture is a three-layer architecture as shown in Figure 1 (Jing *et al.*, 2014; Mahmoud *et al.*, 2015):

1) The physical or perception layer, which is the bottom layer of the IoT architecture
2) The network layer or transport, which is the middle layer.
3) The application layer, which is the upper level of architecture (Mahmoud *et al.*, 2015).

Each layer in the Internet of things can be defined and analyzed based on their own unique function and the devices used in the layer. In the following sections, we present a detailed discussion on each layer.

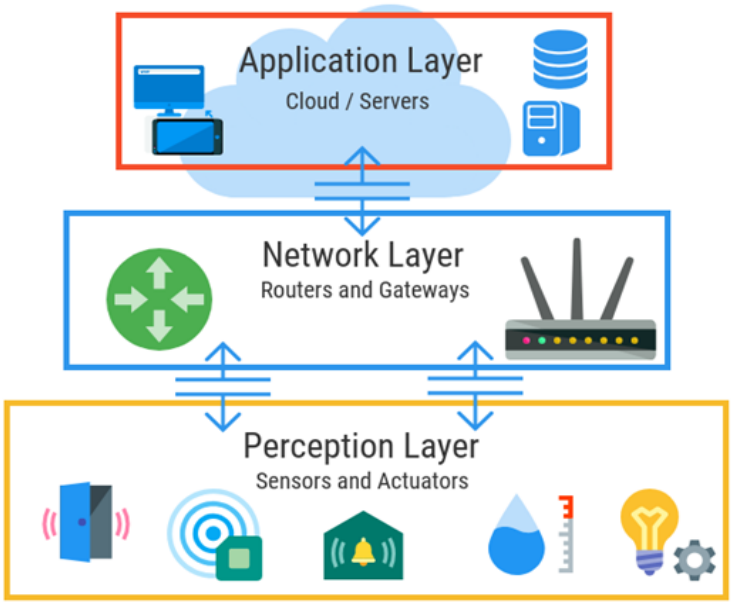

Figure 1. Three-tier architecture (3Tier) of IoT

1. Physical or Perception Layer: This layer, which is also known as sensing layer, is responsible for detecting, receiving, processing and collecting data and information from surrounding environments through smart devices and components such as sensors and operators, and RFIDs and then sends this information into its top layers, i.e. transport (network).

Technologies or protocols related to this layer are:

1) RFID: This tag is used to identify nodes. It does not need to make a specific connection for its operation and is able to exchange information using radio waves in short intervals. These tags also have good advantages, including high speed, durability, reusability, high memory and small size (Lin *et al.*, 2017).
2) WSN: These sensors can track and monitor device status and send information obtained from device status to the control unit. They can also provide an interface between real world and cyber world. The usage of WSN have several benefits such as reliability, extensibility, low cost, small size, low power consumption and the like (Lin *et al.*, 2017).
3) Network layer or transport: This layer is the middle layer that receives the information obtained from the perception layer and determines the possible route to send and transmit this information to the nodes, devices and other applications of IoT. Based on some sources, this layer is considered to be the main layer of the Internet of things due to the existence of various devices as well as the activities of various communication technologies.

Technologies or protocols related to this layer include:

1) IEEE 802.15.4: This protocol is designed for defining the physical layer and the WPAN link layer (Al-Fuqaha *et al.*, 2015; Gan, Lu and Jiang, 2011). The aim of this protocol is to focus on a low-rate wireless personal area networks (LRWPANs) to establish the communication between all devices at low rates and low power consumption as well as minimum cost (Lin *et al.*, 2017).
2) 6LoWPAN: Low-power wireless personal area network is developed based on the Internet Protocol version 6 for connecting devices with low power and high power constraints. The network has capabilities such as small packet size, low bandwidth and low power consumption (Tan and Koo, 2014).

3) ZigBee is a wireless network technology designed for short-range communications with low power consumption and has several benefits such as reliability, low cost, security, low complexity, and support for multiple topologies (Tan and Koo, 2014).
4) Z-Wave: Like the ZigBee protocol, this protocol is efficient for short-range communications. It has several benefits including low-power and high reliability; however, it cannot support up to 232 nodes and can be easily implemented compared to Zigbee.
5) MQTT is a messaging protocol used to collect data measured by remote sensors and send them to servers. It has a simple and lightweight structure (Lin *et al.*, 2017; Al-Fuqaha *et al.*, 2015).
6) CoAP is a messaging protocol based on the REST architecture. Because most IoT devices have very limited resources, the HTTP protocol is not applicable because of its complexity and heavy nature (Al-Fuqaha *et al.*, 2015). To solve HTTP problems, some functions of the protocol are modified by CoAP (Lin *et al.*, 2017).
7) XMPP is an instant messaging protocol based on the XML architecture. The protocol has some capabilities including good security, extensibility, providing desirable platforms for video and audio streaming, and can be effectively used for addressing and object-to-object communications (Lin *et al.*, 2017).
8) DDS is a publish and subscription protocol used to support device communication with high-performance devices (Lin *et al.*, 2017; Al-Fuqaha *et al.*, 2015).
9) AMQP is an open standard messaging protocol that can be used in the application layer and act as a firmware protocol (Lin *et al.*, 2017; Al-Fuqaha *et al.*, 2015).

2. **Application layer:** This layer, also known as Business Layer, is considered as a top layer of conventional IoT architecture. It receives the information sent through the network layer and uses it to deliver the desired or predetermined tasks. There are many applications for the layer including: smart city, intelligent transportation, intelligent network ... (Mahmoud *et al.*, 2015; Lin *et al.*, 2017).

2-2- Service Oriented Architecture for IoT

This architecture, is known as the IoT reference architecture in some sources, is the fourth layer and considered as the service, interface, or middleware layer for **IoT** in addition to the physical, network and application layers. The arrangement of architecture is built on the bottom to the top layers composing of physical layer, the network layer, the service layer, and the application layer. The tasks of these three layers are similar to those in the four-layer model; however, the service layer, which is located between the network layer and the application layer, acts as the interface between the two layers and is responsible for delivering services to support the application layer (Lin *et al.*, 2017).

3. Weaknesses, Challenges and Security Threats on Internet of Things

3.1 Security issues in IoT can be categorized into two general categories of technology (technical) challenges and security challenges (Mahmoud *et al.*, 2015).
1) Technology problems and challenges arise from the multiplicity, heterogeneity and variety of devices in IoT, which mainly relate to wireless technologies, energy constraints, IoT scalability and its distributed system.
2) Security challenges result from applying principles and rules for securing access to a secure network through the authentication, confidentiality, end-to-end security, integrity and the like. These principles should be considered while developing devices.

We analyze the security problems and challenges in a detailed way:

Confidentiality: Confidentiality ensures that authenticated nodes will only be able to analyze and receive information processed by other nodes. This issue is of great significance in IoT, because the sensitive information such as human health information can be received and processed by sensors and operators and as a result, disclosing this information may pose serious risks. There are several ways to benefit from the IoT confidentiality including the key management distribution (Lin *et al.*, 2017).

Integrity: Integrity ensures that the data stored and / or being transferred will be underwent changes and interventions, whether wanted or unwanted. This feature is of great importance because the storage or transmission of malicious, false or fake data on devices or undergoing changes of pre-existing data may lead to inaccurate actions or predictions or interrupt the feedback of IoT devices objects for subsequent actions of the total system performance.

Availability: Availability implies that devices or their data are accessible to authorized users. The important thing about the availability or usability of components of IoT is that the most of the requests and responses to the Internet of Things should be generated immediately and promptly; therefore, the implementation and maintenance of such a system is difficult in terms of security (Lin *et al.*, 2017).

Authentication and authorization: Authentication ensures that unauthorized devices and programs fail to connect the other components of IoT. In addition, the authorization ensures that the devices and their requests, applications, as well as information to be legally transmitted and accessed in the Internet of things. In IoT, the authentication is a critical issue for securing the system; however, implementation is a difficult and complex task due to the large number of protocols and functional devices used in IoT (Lin *et al.*, 2017).

Privacy: Privacy implies the monitoring and protecting the user's personal information. It is difficult to maintain privacy in the large IoT network, because a lot of devices shared their information and data there (Lin *et al.*, 2017).

Trust: Trust helps ensure security and privacy. In IoT, trust objectives encompass several aspects: establishing trust relationships between devices and nodes, layers, as well as applications (Lin *et al.*, 2017).

2-3. Security issues related to each layer of IoT:

1. **Physical or perception Layer:** This layer can be divided into two sections: nodes of the perception layer, which includes sensors and information receivers, as well as controller and the perception network layer, which is interacting and communicating with the transmission network (Jing *et al.*, 2014; Lin *et al.*, 2017). RFID technology is one of the security challenges associated with this layer. Since there is no standard encoding for this technology, it is not possible for other devices with different standards to read the specifications of these tags (label (S), or faced with problems and deficiencies while reading these specifications (Jing *et al.*, 2014).

Privacy Issues in RFID tags:

Due to their limited computing power and battery power, it is difficult to maintain the privacy of IoT devices and therefore, low-cost and so-called lightweight approaches should be utilized to overcome this problem. The privacy can be classified into privacy of information and data, as well as the location and position of devices or entities (Jing *et al.*, 2014).

Privacy Issues in WSNs: Eavesdropping, malicious routing, and unintended alternators to data are among the problems that occur while collecting information through these sensors. There are some approaches to prevent such hazards including: encryption methods and algorithms, key management, secure routing, and trust management in nodes.

2- Network layer or transmission: Since this layer is responsible for the transmission and transfer of information received from the physical layer. The major security challenges that pose threat to the layer are concerned to the impacts that may negatively affect the availability of resources and information; most of these issues should be addressed in the field of wireless equipment, since the wireless devices and equipment constitute the majority of the communication channels used in the layer (Lin *et al.*, 2017).

Security issues related to access network:

WIFI Security Issues: This technology is used to connect devices to the Internet. Security issues include access attacks, trapping users, and eavesdropping their connections (conversations) through announcing a fake and malicious access point instead of a legitimate and authorized access point and possible DOS / DDOS attacks (Jing *et al.*, 2014).

Security issues related to cellular telecommunication systems: leaked user information, incomplete data, unauthorized access to nodes and others are among the security issues associated with this layer. Encryption and authentication approaches can help resolve many of these problems; however, studies are in progress to ensure the security in these systems (Jing *et al.*, 2014).

Security issues related to AD-HOC networks: Wireless Ad hoc network is a group of autonomous wireless nodes or terminals cooperated and formed, independent of the fixed infrastructure which use of distributed network management, is a self-creating, self-organization and self-management network. Forging a node as an authorized node and connecting it to other nodes, creating interference and transmitting noise on radio waves are among the security problems of the network. Authentication and validation of nodes and encryption of data can be used to overcome these network security problems (Jing *et al.*, 2014).

Security issues related to the core network:

The major conventional security issues and problems are correlated to the protocols used to resolve severe processing problems and the limited number of Internet protocol addresses in the layer, including the 6LoWPAN protocol (Jing *et al.*, 2014).

Security issues related to the local network:

In IoT, local area network should take data leakage very serously; the goal of access control is to ensure the network resources being used legally, (Jing *et al.*, 2014; Zhang, Zou and Liu, 2011).

3- Application layer:

Security issues related to the support section: this section supports all sorts of business services and realizes intelligent computation and resources allocation. During the whole process, the application support layer can recognize valid data, spam data and even malicious data. The prioritization risk is one of the security problems that threaten this layer; more precisely, the prioritized processing are threatened to recover data and the like (Jing *et al.*, 2014).

Security issues related to applications of IoT: this section encompasses integrated or single programs, as well as significant issues including the specific privacy issues (Wang *et al.*, 2010). Nowadays, IoT applications are widely integrated into our daily lives including smart transportation, smart home, smart wearables and the like (Jing *et al.*, 2014).

Conventional problems found in this area include the leakage of information regarding the location of devices or users as well as emerging issues such as inference and identification through data mining techniques in queries (Suo *et al.*, 2013).

Macro security issues in Internet of things: Building unique security for each layer fails to maintain strong IoT security; therefore, the security should be maintained at the macro level and for the entire layers. In addition, it should be noted that each application has its own security issues. For example, privacy is critical in smart transmission or medical care (health), whereas authentication is the most important element in smart city management. We must try to integrate security into the individual layers using optimal and efficient methods, and establish a uniform pattern for heterogeneous layers in order to guarantee the security of the system (Jing *et al.*, 2014).

1- IoT security solutions

Security subject is one of the hot research problems in IoT and has attracted a lot of researchers not only from academic and industry but also from standardization organizations. We classify approaches to address these

security challenges in two categories: classical or traditional and new or emerging approaches (Kouicem, Bouabdallah and Lakhlef, 2018).

1.4. Classical Approaches: This section tries to provide an explanation for the most important and conventional solutions that have already been tried:

1) **Confidentiality solutions:** In Internet of Things, we need to protect data exchanged between objects from attackers by means of encryption mechanisms. Hence, we should ensure that only legitimate users are able to disclose encrypted data. For this goal, cryptographic solutions exist to ensure data confidentiality, however, in most cases, these solutions are inefficient or even inapplicable in IoT devices with high resource constraints; but they are analyzed as classical methods (Kouicem, Bouabdallah and Lakhlef, 2018; Malina *et al.*, 2016).
2) **Symmetric Encryption (Private Key):** each entity in the system should share cryptographic keys with all other entities in the system. The main advantages of symmetric based cryptographic solutions are their efficiency (they are less-computational) and easy to implement in hardware platforms; but they suffer from scalability and key management issues. There are two general techniques for distributing keys in symmetric cryptography, including probabilistic key distribution and 2) deterministic key distribution (Kouicem, Bouabdallah and Lakhlef, 2018).
3) **Asymmetric encryption (public key):** As we know, this method makes uses of two separate keys. The public key, which is made available to everyone and the other is private key, which is unique to each node independently. The advantages of this approach are flexibility, scalability and optimal key distribution. High computational power required to process encryption or decryption operations as well as valid credentials to validate public key are among the disadvantages mentioned for the approach. These problems are in contradiction to the nature of low-power and limited devices needed to respond quickly to the Internet of Things. Therefore, this approach is not applicable or practical for IoT (Kouicem, Bouabdallah and Lakhlef, 2018; Nguyen, Laurent and Oualha, 2015).
4) **Identity–based cryptography:** This approach has the same functionality as the asymmetric cryptography due to the use of two different keys. In order to overcome the problems of non-scalability and computational complexity of the mentioned methods, an identity-based encryption method has been proposed that uses an unforgeable string (such as user's phone number, email address, etc.) as public key to encrypt data and thereby eliminate the need for certificates. Although their scalability and efficiency, IBE techniques are not very suitable for IoT because they are expensive and incur heavy resource consumption (Kouicem, Bouabdallah and Lakhlef, 2018).

Privacy solution:

Privacy is a critical issue and mandatory in the IoT because data issued by smart objects are very sensitives and inherently related to real life's individuals. The main goal of privacy techniques is to ensure the following requirements:

Anonymity: Property ensuring that a third entity is unable to identify person's identity among other identities in the system.

Unlinkability: Impossibility to cover the persons' identity from the information they produce (Kouicem, Bouabdallah and Lakhlef, 2018).

Untraceability: Difficulty to track actions and information issued from the behavior of an entity in the system (Kouicem, Bouabdallah and Lakhlef, 2018).

1) **Data privacy:** This task can be completed primarily through the following three techniques:

Data tagging: is one of the most known techniques, mainly used to ensure privacy of data flows. The idea behind this concept is to associate additional labels called tags, to data flows in order to allow trusted computing entities to reason about flows of private data (Kouicem, Bouabdallah and Lakhlef, 2018).

ZKP (Zero Knowledge Proof) is a powerful mechanism largely used to ensure the privacy of users' identities. The idea behind ZKP is to allow to one party (prover) to demonstrate to another party (verifier) some property by proving its possessing of some information without disclosing it. This concept is very useful to develop security protocols while preserving the privacy of users' data and properties (Kouicem, Bouabdallah and Lakhlef, 2018).

K-anonymity model is another potential approach to protect the privacy of data in Internet of Things' applications. Considering the context of a set of homogenous data stored in a table where each column represents a record of these data which is owned by some specific user. The K-anonymity models aim to protect each record in the table and make it indistinguishable from the rest of records by hiding the sensitive information about its owner (Kouicem, Bouabdallah and Lakhlef, 2018; Sweeney, 2002).

2) **Privacy of users' behaviors**

In Internet of Things, users and objects perform actions in the systems such as access to sensor data, control remote actuators, etc. Therefore, it is mandatory that their behaviors should be protected against malicious intruders (Kouicem, Bouabdallah and Lakhlef, 2018).

3) **Availability:** In IoT, the availability of the system is one of the most important security services needs to be protected against malicious attacks (like DoS/DDoS) or unintentional failures. Very often, the damages caused by the violation of the availability are tremendous which can be economical losses (Kouicem, Bouabdallah and Lakhlef, 2018).

An approach for minimizing denial-of-service attacks:

IP Traceback methods are powerful mechanisms largely adopted in IP based networks such as Internet to detect DoS and IP flooding attacks in real-time (Kouicem, Bouabdallah and Lakhlef, 2018; Sahraoui and Bilami, 2015). The use of methods to improve the TLS protocol is just among the proposed solutions (Maleh, Abdellah and Belaissaoui, 2016).

Artificial Intelligence (AI) techniques: Using techniques such as the artificial neural network helped detection the intrusion and identification of attacks, including denial of service attacks (Kouicem, Bouabdallah and Lakhlef, 2018).

2-4 New emerging security solutions for Internet of Things include blockchain and software defined networking based solutions approaches: since conventional and generally centralized were not appropriate and efficient to secure the Internet of things due to the existence of different technologies and the importance of availability to these equipment anywhere and anytime, as well as the rapid extensibility of this equipment; therefore, this industry needs new solutions to overcome its challenges.

1. **Blockchain based solutions**

Blockchain is a new effective technology that has revolutionized the world of cryptocurrency. It consists mainly of a secure distributed database called public ledger containing all transactions have been made by all the participating entities and all transactions are done and validated in a distributed peer to peer infrastructure. For example, when an entity wants to carry out a transaction with another entity, it sends a transaction request to all the peers in the blockchain network. Then, each node collects periodically and groups them in a single block. Finally, the process of validation of each block is done in a distributed way using a consensus algorithm that is executed by some nodes in the network, called miners. Using this technology, our information will be more stable and secure and kept away from unwanted or unauthorized changes.

1. **Benefits of blockchain in IoT**

Some added values that blockchain technology can bring to IoT and security domains.

• **Decentralization**: Because of the decentralized architecture of IoT, blockchain is most suitable as a security solution in IoT. The decentralized architecture of blockchain makes security solutions most scalable and can solve the problem of single point of failure and becomes more robust to DoS attacks.

Pseudononymity: The nodes in blockchain are identified by their public keys. These pseudonyms don't link any information about the identity of the participating nodes.

Security of transactions: Each transaction, before being sent to blockchain network, is signed by the node and must be verified and validated by miners. After the validation, it's practically impossible to forge or modify transactions already saved in the blockchain. This provides a proof of traceable events in the system (Kouicem, Bouabdallah and Lakhlef, 2018; Conoscenti, Vetrò and De Martin, 2016).

2. Secure IoT transactions

The first IoT platform based blockchain solution was developed by IBM, which consists of proof of concept of a decentralized and secure IoT platform based on Ethereum protocol which is a seamless solution to deal with devices contracting and transactions in a most scalable way. So IoT devices can define and set autonomously their own roles, responsibilities and permissions in the whole IoT ecosystem and also can do transactions and complex negotiations between themselves (Kouicem, Bouabdallah and Lakhlef, 2018).

3.Data Sharing

In several IoT applications, a lot of data is exchanged between objects and with other entities. For that, it's very important to deal with these data and propose security solutions to share it with others. to ensure privacy in IoT systems, it is recommended to use peer-to-peer architecture, and specifically the blockchain technology. In addition, as all the operations handled on IoT data are controlled by the blockchain, it is easy to detect any abuse in data (Kouicem, Bouabdallah and Lakhlef, 2018; Conoscenti, Vetrò and De Martin, 2016).

4. Main challenges of blockchain in IoT

The block chain needs a relatively large amount of distributed memory, use a lot of computations and processing while undergoing changes and updates and validation operations, etc. Due to its comprehensiveness nature, the analysis of all the nodes is performed with time delay and needs relatively large bandwidth due to interactions with other nodes in modifying and updating processes (Kouicem, Bouabdallah and Lakhlef, 2018).

1. **Software-based software solution:** the analysis of this approach is beyond the scope of this research.

Conclusion

Conventional approaches used to secure the confidentiality, privacy and security in IoT require a lot of memory due to problems such as heavy processing load that is imposed on each node. In addition, low-speed approaches (contrary to the real-time IoT) are not very efficient, so it is necessary to utilize newer and more innovative methods to secure IoT. Due to the its decentralization and distribution nature, blockchain-based methods apply advanced techniques and hash algorithms to provide more security than traditional methods, possess reliability and high tolerance against errors leading to the effectiveness of this approach.

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.

2. Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). "Blockchain for the internet of things: a systematic literature review," *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 1-6.
3. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544-546, 2018.
4. Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems*, *89*, 110-125.
5. Gan, G., Lu, Z., & Jiang, J. (2011, August). Internet of things security analysis. In *2011 international conference on internet technology and applications* (pp. 1-4). IEEE.
6. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501.
7. Kalkan, K., & Zeadally, S. (2017). Securing internet of things with software defined networking. *IEEE Communications Magazine*, *56*(9), 186-192.
8. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221.
9. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125-1142.
10. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336-341). IEEE.
11. Maleh, Y., Ezzati, A., & Belaissaoui, M. (2016, November). Dos attacks analysis and improvement in dtls protocol for internet of things. In *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*(p. 54). ACM.
12. Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks*, *102*, 83-95.
13. Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, *32*, 17-31.
14. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187.
15. Sahraoui, S., & Bilami, A. (2015). Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things. *Computer Networks*, *91*, 26-45.
16. Suo, H., Liu, Z., Wan, J., & Zhou, K. (2013, July). Security and privacy in mobile cloud computing. In *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 655-659). IEEE.
17. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557-570.
18. Tan, J., & Koo, S. G. (2014, May). A survey of technologies in internet of things. In *2014 IEEE International Conference on Distributed Computing in Sensor Systems* (pp. 269-274). IEEE.
19. Wang, K., Bao, J., Wu, M., & Lu, W. (2010, October). Research on security management for Internet of things. In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)* (Vol. 15, pp. V15-133). IEEE.
20. Zhang, B., Zou, Z., & Liu, M. (2011, May). Evaluation on security system of internet of things based on fuzzy-AHP method. In *2011 International Conference on E-Business and E-Government (ICEE)* (pp. 1-5). IEEE.