ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse24952020.pdf
https://doi.org/10.30534/ijatcse/2020/24952020

# Adoption of Blockchain for Security in IoT Considering QoS

**Ravi C Bhaddurgatte[1], Vijaya Kumar B P[2], Kusuma S M[3]**
[1]Research Scholar, Jain University, India, bcravi@yahoo.com
[2]M S Ramaiah Institute of Engineering and Technology, ISE Department, India, vijaykbp@yahoo.co.in
[3]M S Ramaiah Institute of Engineering and Technology, Telecommunication Engineering Department, India, kusumasm@msrit.edu

## ABSTRACT

Increased adoption of the Internet of Things (IoT) in multiple domain areas continuously increases the volume of data and transactions from the IoT devices. The IoT systems are vulnerable to more attacks because of increased adoptions and technology adoptions. Protecting the data and providing security to the data and transactions is one of the critical issues for the effective quality of service (QoS) in the IoT environments. An adaptable IoT framework is proposed based on the research approach of '*ADOPT*' that leverages the blockchain technology and features considering security as one of the QoS parameters. In the proposed model of a three-layer IoT architecture with an application layer, network layer, and perception layer, the blockchain features are adopted for the resource-constrained IoT environment. In the perception layer, the model uses a local and temporary memory to maintain the local chain, which is managed based on the memory size and time constraints. The application layer nodes manage the synchronization of the data from the corresponding local chain at the edge node. The implementation of the proposed model uses Ethereum, an open-source public blockchain, and using mobile devices as an edge node. The results are verified for security factors like access, authorizations, confidentiality, and computing resources.

**Key words:** Internet of Things, Machine Learning, Quality of Service, Blockchain.

## 1. INTRODUCTION

Internet of Things (IoT) echo system is heterogeneous and dynamic with the integration of multiple devices and protocols. The adoption of IoT is widespread, and has an array of challenges in terms of resources, deployment, architecture, security, and protocols for achieving QoS (Quality of Service). The Quality of Service (QoS) as a non-functional component is the *'capability of providing satisfactory service'* by different service providers and systems. Due to the heterogeneous nature of IoT, the overall QoS in IoT is the capability of providing service by various service providers like – sensing service, network service, cloud service, and services by various enabling technologies and components of IoT. A *QoS Parameter is defined as a*n attribute or a factor that will have an influence on the performance or efficiency of QoS of the system under consideration [4] and energy consumption controlling in IoT [33]. For this work, authors consider security as one of the QoS parameters which influence the stability and integrity of IoT systems. Providing QoS in terms of 'privacy and security' is one of the key research challenges due to the dynamic, distributed, and complex nature of IoT systems. It is very clear that the data volume and transactions in the IoT environments are increasing double, triple folded and exponentially due to increased adoption of IoT devices [6]. Due to the increased adoption of IoT technologies in multiple domain areas, more data is being generated in the systems. Managing and securing the large volume of data becomes a critical and important task in the IoT systems. As the architectures, systems and protocols of IoT becomes more stable, the adoption of IoT increases, due to which the data volume increases and thereby the use and misuse of data. Privacy and security threats to the data of the IoT systems need more attention to develop and establish a stabilized IoT echo system for providing required QoS.

The reported data on incidents of attacks on IoT devices and attacks from IoT devices indicate that there is definitely more security threats anticipated [11] because of increased data and transactions in IoT systems. The security in IoT is implemented using Machine Learning (ML) techniques, blockchain technologies, cryptographic methods, varied protocols, algorithms and hardware solutions etc. [2, 6, 9, 15 & 24]. This paper focused on the research solutions using blockchain technology for IoT security as one of the important QoS parameters. Blockchain is a combination of technologies for solving some of the problems like double-spending, disintermediation, and trust-building for data and transactions in the public domain [23]. Basically one can adopt all components **or** some selected components **or** a combination of selected and modified components for developing the target system(s) under consideration. The suitability and applicability of technology and technology components of the blockchain platform for security [15 & 24] are motivational factors to consider the technology for IoT security. The blockchain technology which is a combination of technologies for securing the systems can be considered as a whole **or** partial based on the constraints. Due to the

dynamic and heterogeneous nature of IoT systems, one can propose the models and frameworks which can act as a guideline for achieving security. The IoT architecture (IoT-A) is an architecture reference model by IoT European Research Cluster (IERC) which can be used as a reference for building IoT architectures [3]. Like IoT-A, larger and intensive research work is required to develop a reference model with guidelines for security in IoT using blockchain.

From the reviews carried out, it is observed that there are multiple approaches of using blockchain for security in IoT systems like: (i) by adding additional layers (ii) by proposing a new type of blockchain (iii) by defining a new model, or framework.

The research approach in this work considers the blockchain platform for security in the IoT environment by selective adoptability. Blockchain has core components with features supporting security in the IoT systems. As a research gap, it is observed that there are missing approaches of selective adaptability for security in IoT. Hence, there is a scope to optimize existing blockchain technology by selective adoption to suit the resource-constrained IoT environments for security. Key contributions of this paper include the following:

- Define a security model for IoT using blockchain by selective adoptability. The defined model considers blockchain for the resource-constrained IoT environment by unique design constraints like: '*ADOPT*', '*RETAIN*' and '*IGNORE*'.
- The verification of the proposed approach is done for the selected security aspects like access, authentication, integrity and confidentiality.

## 2. BACKGROUND

For implementing security in IoT there is a need for generic solutions. The review of security in IoT and research solutions is structured into four parts as follows:

(i) Security, Privacy and attacks and solutions in IoT

(ii) Standardization efforts

(iii) Machine learning adoptions

(iv) Blockchain technology for IoT security and challenges.

**Security, privacy, and attacks and solutions in IoT:** In [13], various security issues related to IoT layers are reviewed. These include IoT attacks such as physical attacks (relating to perception layer), network attacks (relating to the network layer), and software and encryption attacks (attribute more to application layer). The review summarizes how these attacks can be avoided using some of the existing solutions. There is a need for efficient security solutions for IoT environments. Similarly, authors in [22] shown the solutions for various security issues and attacks which are classified related to three IoT layers and current/recent solutions. The limitations and the need for new security systems and protocols for the IoT are also explained.

The detailed review of attacks and security issues in IoT is carried out in [31]. The limitations of IoT devices for privacy and security, and possible solutions to address the limitations is depicted in [31], and the authors next classify the IoT attacks and explain adopted solutions, the third part discusses the authentication and access control mechanisms in IoT systems. The review of security issues in different layers of IoT and the recent implementation of the security models, architectures, and open challenges are described. All the IoT devices are vulnerable for a specific type of attack at different IoT layers event after measures are taken care of by manufacturers by specific designs, protocols, and security models. So, the review summarizes the need for improvising the standards, protocols, and solutions for IoT security.

**Standardizations:** The review of different standards for securing the IoT environment is carried out in [14]. The standardization efforts by IETF (Internet Engineering Task Force) for different layer protocols and key management etc. as different solutions shown in [14]. The major standardization effort to stabilize Datagram Transport Layer Security (DTLS) similar to Hyper Test Transfer Protocol Secured (HTTPS) for the protocol of constrained environments like IoT, and the Constrained Application Protocol (CoAP) is carried out. However, there is a need for standardization of solutions that are related to IoT security. From the review, it is identified that the other areas of immediate standardization of IoT are key management, bootstrapping for facilitating IoT authorization, commissioning, configurations, and deployment of IoT systems in a secure manner.

From the standardization and protocol perspective, there is a new scheme for implementing security in IoT [21] by integrating the Constrained Application Protocol (CoAP) standards. The CoAP is used for communication security at an application layer in a resource-constrained environment. The authors propose an approach of DTLS header compression by leveraging 6LoWPAN () standard for reducing the overhead. A communication protocol that encrypts the data transmitted across different systems/devices using a cryptographic system for authentication codes is defined for implementing security for smart home IoT applications in [26]. The implementation preserves privacy. The review indicates the scope for research and solutions for improvising the existing protocols and new protocols for IoT environments.

In [20], authors define a three-layer architecture and categorizes the IoT attacks including countermeasures by defining cyber entity units of the IoT system architecture. The security attack detection algorithms are assessed in [13], and evaluated using OMNeT++ event simulator. The results indicate that most of the attack detection systems fail if there

is a collaborative attack by multiple attackers in the IoT system. Such attacks need a security solution.

**Machine Learning for IoT security:** The ML techniques are considered as one of the major technology solutions for securing the IoT environments for specific areas of security in different researches [19]. The book chapter [19] details the volume of devices and data in IoT environment. Also, different security issues of IoT, adoption of different ML algorithms for different IoT applications are described. The categorization of ML solutions for IoT security and specific examples of different ML algorithms for securing IoT by malware detection, intrusion detection and anomaly detection, etc. are also detailed in [19]. Authors in [6] implemented the Artificial Neural Network (ANN) technique at the edge nodes for detecting data anomalies to secure the IoT system. The adoption of unsupervised clustering and classification ML technique for building a trustworthy and secure IoT environment for Mobile Crowd Sensing (MCS) applications are shown in [2].

**Blockchain for IoT and security in IoT:** The summary of the review of the applicability of blockchain along with use cases for IoT are shown in [7]. This work reveals the relevance of blockchain for IoT due to its decentralized, distributed consensus for maintaining tamperproof data and transactions in terms of adaptability, integrity, and anonymity. Also the issues identified with blockchain for direct applicability for IoT are shown in [7]. It is explored that blockchain can be adapted for IoT by handling scalability by adaptability.

Blockchain as a technology and suitability to strengthen IoT is reviewed in [15] and the review summarizes how the blockchain can be helpful to address the challenges of IoT. The applicability of blockchain/features is explained taking the scenario of supply chain and blockchain for handling complex workflows, smart contracts, identification of source of devices at the destination and many other IoT adaptations in the flow. Blockchain for cryptographic message transfer [34].

The blockchain technology is tweaked as a new lightweight blockchain architecture to eliminate overhead to suit the low computing IoT environment in [10] by retaining privacy and security features. The proposed system eliminates mining to avoid the delays. This approach uses a combination of decentralized public blockchain on high-end devices for stronger trust and centralized private immutable ledger at local networks to eliminate overhead and distributable trust. This eliminates block processing overhead to achieve security in IoT systems.

The authors in [18] defines a new nonce calculation algorithm (Proof-of-Work) to implement dynamic key management in a heterogeneous transportation system using blockchain-based system for security and privacy in the IoT system.

The functional blocks and features of blockchain technology which can be adoptable for the IoT domain for securing the echo system is explained in detail in [24]. Also some of the limitations for the resource-constrained system are highlighted. Authors in [24] discuss different ways to strengthen security in IoT and discuss a theoretical model for security in IoT using blockchain technology. However, research in blockchain for IoT can be explored for many more functions like configuring IoT devices, discovering and registering devices by defining and implementing frameworks and models.

Authors in [12] reviews the blockchain and IoT platforms (Ethereum, Smart Contract and Mobius) for applicability for IoT security solution. The system implemented using Blockchain as a database (MySQL) for data storage for security in IoT instead of a traditional server system.

The authors in [11] propose a model for securing the IoT system by introducing additional layers for blockchain at application and protocol layers. The proposed model uses token tracking and distribution of voting power across nodes for implementing Denial-of-Service (DoS) attacks in IoT systems by providing authentication and authorization service. The main focus of this work is to provide authorization and authentication using blockchain technology. The model can be also explored for other aspects of security like integrity and availability.

Blockchain as a technology is reviewed for IoT security and compared with cybersecurity in [1]. The blockchain as a technology by its design has capabilities to recover from threats and attacks, which support security and can be adopted for IoT security.

Authors in [16] design an IoT system with modules: controller, middleware, device registration, routing system, and Kerberos for taking data from sensors/devices, routing data, and key distribution. There is a security framework defined using blockchain to secure data in the IoT environment with defined modules. The system uses hashing algorithm, controller and administrator to manage overall transactions. The security model defined in [28] for IoT environment where the security issues are addressed by the model using a security framework using blockchain and traditional IoT architecture. The work uses InterPlanetary File System (IPFS) for large distributed storage and a consensus algorithm which is a combination of POS, POW for public chain, and PBFT for coalition chain for achieving security in IoT.

In [32] blockchain is looked at as possible solutions for the issues of data integrity, access and authorization, data sharing, and privacy by defining a security framework for a layered IoT architecture. The framework based blockchain has specific modules for data integrity and data sharing. It uses Ethereum for managing authorization and access and uses private and consortium blockchain features for privacy in IoT security.

The adoption of ML and blockchain (Ethereum) for securing IoT environment in customizing IoT devices based on the

user's preferences in a shared household environment is shown in [25]. Inherent features of blockchain provides partial security solutions, Blockchain technology itself has vulnerabilities for attacks as described in [30].

From the reviews of blockchain, security and IoT it is found that there are multiple models, frameworks and research solutions for security in IoT using blockchain. However, some of the solutions define a new [9] blockchain and others propose a solution by additional layers [11] and others adopt some of the features for specific solutions [9, 12 & 24]. Each and every feature of blockchain is directly or indirectly support the security solution(s). Adopting the overall features of the blockchain in a selective manner to the IoT environment is still missing. This is considered as a research gap that can be addressed.

A new lightweight scalable blockchain (LSB) model with overlay nodes with cluster heads (also called as block manager) is defined for IoT for security by [9]. This is a new approach by completely defining the blockchain for IoT and defining the responsibilities for block manager in the overlay network. This approach also defines a new consensus approach for resource-constrained IoT and a new algorithm for transaction verification and distributed trust management. This model is simulated and verified for a smart home environment.

A detailed survey of IoT applications using blockchain, and comparison of consensus methods, architectures, and traffic modeling is done by the authors in [17]. Multiple research and practical implementation of blockchain for IoT are reviewed. The review summarizes there are still open challenges for IoT specific solutions using blockchain in terms of consensus approaches, scalability, storage and computing power optimizations, and traffic modeling. As blockchain is a p2p (peer-to-peer) network, efficient management of communication and traffic in the p2p network are critical components to be handled. This becomes even more critical for IoT environments. The review also highlights the critical need for policies, procedures, and regulations for integrated usage of blockchain in IoT.

In summary, it is inevitable to use a massive set of IoT devices (hardware) for data acquisition which are vulnerable to attacks. These devices need standards, protocols, software (algorithms), and hardware solutions to achieve security and privacy of their data transmitted. It is found that there is research scope for security solutions in the IoT but the scope of our work takes the path of blockchain for security in IoT. The IoT security solutions can be summarized into the following groups:

- ✓ Research works and solutions by defining and adopting standards for applicable protocols.
- ✓ Research works and solutions by new protocols/algorithms for preserving security and privacy.
- ✓ Research works and solutions using Machine learning techniques for securing IoT systems.
- Research works and solutions by modifying existing blockchain system and defining new blockchain models and frameworks to suit resource-constrained IoT system.

## 3. BLOCKCHAIN AND APPLICABILITY FOR IoT SECURITY

This section briefly highlights blockchain technology, relevance, applicability in IoT and security in IoT. The blockchain is defined as: 'A technology built for handling the data and transactions in a **secure and integrated** manner, which is built using technologies like: (i) **Distributed ledger** for storing data in a **decentralized** manner making the data available all the time (no single-point-of-failure) (ii) **Cryptography** (encryption and cryptographic algorithms) for securing the data and transactions to make it tamperproof (iii) **Consensus** approach for validating the transactions and building the **trust**. Blockchain uses **smart contracts** to bind the participants in the network for application, financial and contractual obligations'.

The blockchain technology (like Ethereum) works on the basis of the following functional equations for maintaining the transition, transactions and blocks formation [29]. A continuous state transition is defined using transaction (T) and previous transition by the equation (1).

$$\boldsymbol{\sigma}_{t+1} \equiv \gamma(\sigma_t, T) \quad (1)$$

$$\boldsymbol{\sigma}_{t+1} \equiv \Pi(\sigma_t, B) \quad (2)$$

$$\boldsymbol{B} \equiv (\ldots,(T_0, T_1, \ldots)) \quad (3)$$

$$\boldsymbol{\Pi}(\sigma, B) \equiv \Omega(B, \gamma\,(\gamma\,(\sigma, T_0), T_1)\ldots) \quad (4)$$

Below are the explanations of the functions and parameters in the construction of blockchain.

*(1)$\boldsymbol{\gamma}$ is the state transition function, $\gamma$ allows components to carry out arbitrary computation, while $\sigma$ allows components to store arbitrary state between transactions.*

*(2)$\boldsymbol{\Pi}$ represents the block level transition function.*

*(3)$\boldsymbol{B}$ is the block that is formed based on the transactions of previous blocks.*

*(4)$\boldsymbol{\Omega}$ is the block transition finalization function which considers the values of previous block and previous blocks states and values.*

The blockchain can be either private or public based on the application domain, type of data, and transactions of applicable domain/application. Blockchain is a p2p (peer-to-peer) network of decentralized, and distributed nodes. The data is stored in the decentralized ledgers on the nodes (all or some / full or partial) of the p2p network. The generic transaction cycle of blockchain consists of three steps.

At a high level, it includes broadcast transactions, validate transactions using consensus methods, and add transaction to block (blockchain) as shown in [*Figure 1*]. Additional financial contracts can be included in a blockchain by using smart contracts that define the agreements on the services under consideration.

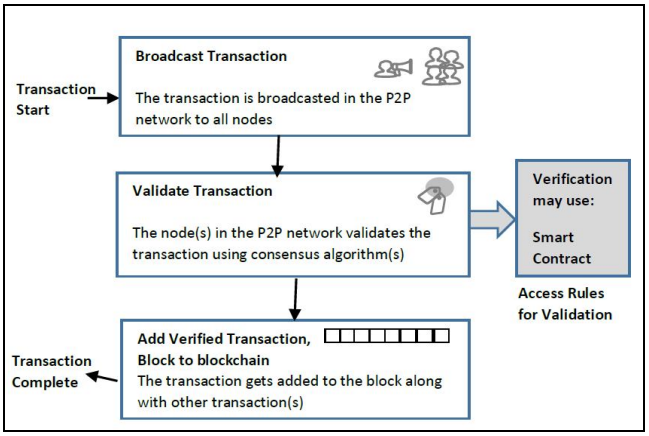


**Figure 1:** Blockchain Transaction Cycle

In Our research, analysis, and adoptability of blockchain for IoT, the constituents of blockchain are grouped as (i) Features (ii) Components and (iii) Process and Functions. This is listed in the table [*Table 1*]. The architecture, design, and features of blockchain have few requirements which are challenges in using blockchain in the resource-constrained IoT. But blockchain has features which are strengths for the security of a system. So, the main requirements of blockchain are '*high computing and high storage*' which by nature defeats the technology as IoT. This is constrained by the resources at the perception layer (edge nodes). By the detailed analysis of the blockchain ***'features vs requirements'*** and IoT ***'challenges vs security requirements'*** an adaptable framework is proposed to suit the resource-constrained IoT environment '**for achieving security in IoT'** environment.

**Table 1:**.Overview of blockchain constituents and requirements gaps

| **Components / Features supporting components** | **Features Across Blockchain** | **Process / Functions** | **Blockchain Requirements** |
|---|---|---|---|
| **Distributed ledger (**Decentralization **)**<br><br>✓ **Availability**<br>✓ Fail-proof<br>✓ Scalability<br>✓ Data Sharing | | 1. Distributed and non-cloud centric storage of data blocks (**blockchain**)<br>2. p2p Nodes / Users in the domain **OR** network<br>3. Adaptability | • High and Replicated Storage<br><br>• High and Distributed Computing<br><br>• Long time for completing transactions<br><br>• Scalability<br><br>• Trust among the community<br><br>• Legal and compliance issues |
| **Cryptography (**Immutability**)**<br><br>✓ Security<br>✓ **Integrity**<br>✓ Immutability<br>✓ Tamperproof<br>✓ Access and authorization<br>✓ **Confidentiality**<br>✓ Anonymity | | 1. Cryptographic / Hashing / Encryption algorithms<br>2. Public and Private keys | |
| **Consensus (**Transparency**)**<br><br>✓ Verification of transactions<br>✓ Trust building<br>✓ **Confidentiality**<br>✓ **Integrity**<br>✓ Data Sharing | | **1. Consensus methods of verification of transactions by Miners:**<br>✓ Proof of Work (PoW)<br>✓ Proof of Stake (PoS)<br>✓ Distributed consensus<br>**2. Broadcasting / Gossiping** | |
| **Smart Contracts**<br><br>✓ Financial and contractual bindings | | 1. Business logic and processes for financial and contractual bindings.<br>2. Digital Contracts | |

As we will be discussing further in detail, there is no single solution for all security problems. This work is to address a major chunk of security issues with minimum technology adoption. Authors here consider to adopt a globally proven and accepted '*Pareto Principle' (80:20 rule)* to decide on the adoption of a blockchain feature for securing the IoT systems and for '*achieving multiple solutions using minimum adoption*'. The blockchain features and security issues [*Table 1*] are analyzed and, it is understood that adopting one major technology construct of blockchain '*cryptography*' which can address a lot of security concerns of IoT. So, using blockchain '*cryptography*' can bring-in 80% of the software security solutions mainly '*integrity*' and '*confidentiality*'. These two cover many of the security solutions (may not be exactly 80% per se).

*Integrity*, *Confidentiality and Availability (ICA)* are considered as fundamental requirements for securing any system. All the requirements of security fall under these three security pillars. Maintaining complete and end-to-end *ICA* may require a combination of solutions. The combinations of solutions can include hardware solutions, configurations and deployment solutions, solutions using algorithms, cryptographic, encryption, and other software technology solutions.

## 4. PROPOSED SECURITY MODEL FOR IOT BY LEVERAGING BLOCKCHAIN

In this paper, different security solutions are explored and choose to deep dive and build a security solution and

framework using blockchain technology for the IoT environment. *With a clear understanding and review of features and limitation of blockchain, an adaptable IoT based security model is proposed using the functional modules of IoT and blockchain.*

### 4.1 Approach towards the blockchain adaptability

The approach is based on the defined design considerations as described in the column *'B': 'Research Design Considerations for decision'* in the table [*Table 2]*. The details of the columns 'A', 'B', and 'C' are as described below.

A. IoT challenges / Resource constraints of general IoT environment

B. Design considerations for decision

C. Research Design decision, the description of the design decisions are described as below.

i. ***RETAIN*** the feature of for achieving security
ii. ***ADOPT*** to minimize / eliminate / overcome the limitations
iii. ***IGNORE*** if not critical for the domain

**Table 2:** IoT Resource Constraints and Design Considerations based on gap analysis

| **Components / Features supporting components** | **A. IoT Challenges / Resource Constraints** | **B. Research Design Considerations for decision:** ✓ ***RETAIN*** ✓ ***ADOPT*** ✓ ***RETAIN*** | **C. Design Decision** |
|---|---|---|---|
| **Distributed ledger (**Decentralization**)** | • *Scalability* • *Resource Constraints* • *Access and identity* • *Integrity* • *Vulnerability for attacks* • *Deployment* • *Configuration* • *Non standardized architecture, protocols etc* | Considering '**Distributed ledger'** of storing the blockchain data on all nodes to achieve '**availability'** is **considered as less-critical** in terms of data but considered **critical** for IoT system to be up for capturing the data. | *ADOPT* |
| **Cryptography (**Immutability**)** | | Considering blockchain feature '**Cryptographic'** for IoT we can achieve many security solutions in IoT such as:<br>- Security<br>- Integrity<br>- Confidentiality<br>- Anonymity<br>- Immutability<br>- Tamperproof<br>- Access and authorization<br>- And more….<br>This is considered as effective as it will not need high resources in the resource constrained IoT environment.<br>- Computing<br>- Storage<br>- Time for completion of transaction | *RETAIN* |
| **Consensus (**Transparency**)** | | Considering '**Consensus**' for getting the transactions validated in the system to achieve '**trust'** is **considered as less-critical** in terms of transaction data, done by validating the public key associated with trusted edge nodes.<br>- **Verification of transactions**<br>- **Trust building**<br>- Confidentiality<br>- Integrity | *ADOPT* |
| **Smart Contracts** | | Smart contract (programs) for placing the transaction, verify the source (designated edge nodes) and retrieval of data in secured manner. | *ADOPT* |

The blockchain has resource-intensive storage, transactional and computational needs. Applicability and adoptability of blockchain for resource-constrained IoT echo system is a challenge. On the other side the basic features of blockchain-like distributed ledger, cryptographic (for high security), and consensus (immutability) make it considerable for the IoT domain. There are twenty-four types of attacks classified [8] into these three IoT layers in which '*software and encryption'* attacks attributing mainly to the application layer. *The vulnerabilities and attacks in IoT systems keep increasing as the systems, integrations increase and there is no single security solution for all types of attacks.*

The security model design is based on the below guidelines and research considerations.

- The IoT environment is resource-constrained for both: computation and storage.
- The design is focused on bringing '*security'* in the IoT environment for the IoT data based on the classified and listed '*functional modules'* [*Table 3*]. The design does not focus on the aspects of the performance of the blocks and blockchain creation.
- The functional modules like: *'data sharing'*, *'data storing'*, '*data access'* and '*data transfer'* need securing the data by maintaining integrity, confidentiality, and availability.
- The model focus on '*securing*' the IoT data from the edge nodes.
- There are no single solutions for all security issues. The model is focused on securing the IoT system for the defined set of parameters as listed in [*Table 2*] by applying '*cryptography'*.
- The '*distributed ledger'* storing the complete blockchain at all (or many) nodes need high storage.
- The proposed approach stores the partial blockchain in the edge nodes as edge nodes are storage constrained. ***This does not make the system completely 'fail-proof' or completely 'available' but the modified or lightweight ledger (or memory pool) is implemented for maintaining the integrity and confidentiality.***
- The blockchain feature '***consensus'*** needs high computing. The sensor data in the IoT environment from edge nodes do not get validated from other nodes as this

is the origin of the data. So, the design considers a simple consensus of validation of data/transactions using the applicable public key values of the edge nodes. The edge nodes do the two basic functions which are less resource-intensive:

- To maintain the local and temporary chain (memory pool) and transfer the data to the main blockchain.
- Clear the local memory pool based on the configured limits of memory pool size and time limit.

- The design consideration [*Table 2*] of '*RETAIN'*, '*ADOPT'*, and '*IGNORE'* are based on the IoT challenges and resource constraints.
- The implementation of the model is by defining separate methods for managing the temporary chain at the edge nodes of the IoT system and p2p nodes at the application layer.
  - Application node blockchain management: The method of replicating the complete blockchain when creating new p2p nodes or when a new block is added.
  - Perception node temporary chain management: The method of replicating the complete blockchain when creating new p2p nodes or when a new block is added.
- Smart contracts are part of the blockchain for business rules, contractual agreements, and bindings. Simple smart contracts can be considered for data hashing, storage, and keys generation.

### 4.2 Proposed Model for IoT Security

In this paper, a methodology is devised for making design decisions and decided to '*ADOPT*' blockchain technology for '*cryptographic'* implementation in an IoT environment. The functional modules of IoT systems are classified [5] for each layer as '*core modules specific to layer'* and some are '*adaptable and context-specific'* modules as listed in the table [*Table 3*]. The **'***Data Processing*' is considered as a domain-specific module and not considered under the scope of this framework security. The modules are considered to adopt the blockchain technology for '*packaging'*, '*storing'* and '*access'* of the IoT data at different layers in a secure and, confidential manner by maintaining the integrity of data across the system by using the '*cryptographic'* feature of blockchain [*Figure 2*]. The system uses public key (asymmetric key) cryptography so the data access and authorization is maintained by private and public keys.

The proposed model and framework are to place all the IoT data into the blockchain. Maintain a local and partial blockchain in edge nodes of the perception layer and a global full data blockchain in the application layer nodes. The proposed adoption model for IoT security considers below guidelines to implement the blockchain feature '*cryptography'* for data sharing / transfer / routing.

**Table 3:** Core Functional modules of IoT layers**.**

| IoT Layer | Core Functional Modules of IoT Layers | Pillars of Security | Blockchain Features Adopted for 'Data Sharing' |
|---|---|---|---|
| Application Layer | -Processing<br>-Data Transfer | Availability<br>**Integrity**<br>**Confidentiality** | **Cryptography**<br>✓ Security<br>✓ **Integrity**<br>✓ Immutability<br>✓ Tamperproof<br>✓ Access and authorization<br>✓ **Confidentiality**<br>✓ Anonymity |
| Network Layer | -Data Communication<br>-Data Routing<br>-Data Transfer | | |
| Perception Layer | -Data Sensing<br>-Data Transfer<br>-Data Storing<br>-Data Sharing<br>-Data Access | | |

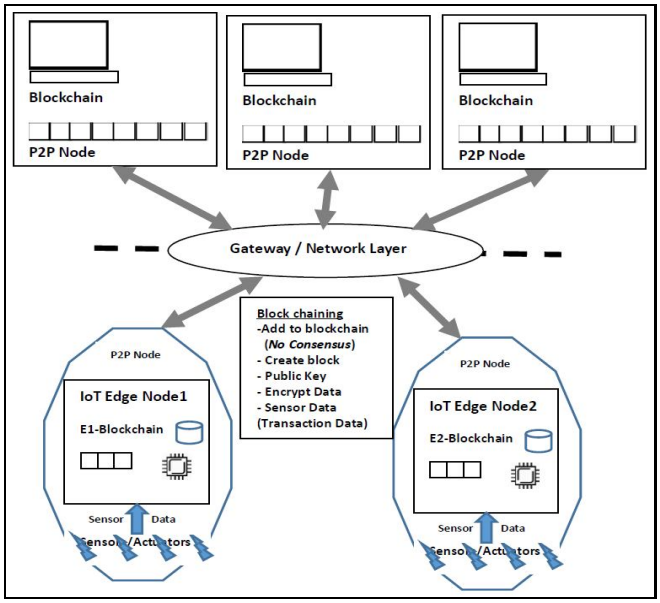


**Figure 2:** IoT Security Framework across three layers using blockchain

*Customized blockchain for IoT Security*

Applying the cryptographic principles by adding public key, transaction, and time stamp information, the transactions are created and broadcasted. The transactions get added to the local blockchain (temporary memory pool) and then added to the global blockchain (complete) [*Figure 3*]. The features of the blockchain adopted across layers: *cryptography* and *distributed ledger*. By adopting the technology components, the IoT system inherits the security features under the technology of blockchain. The *consensus* is adopted only at the application layer nodes where the nodes validate the source of data using the public key values associated with the received transaction data.

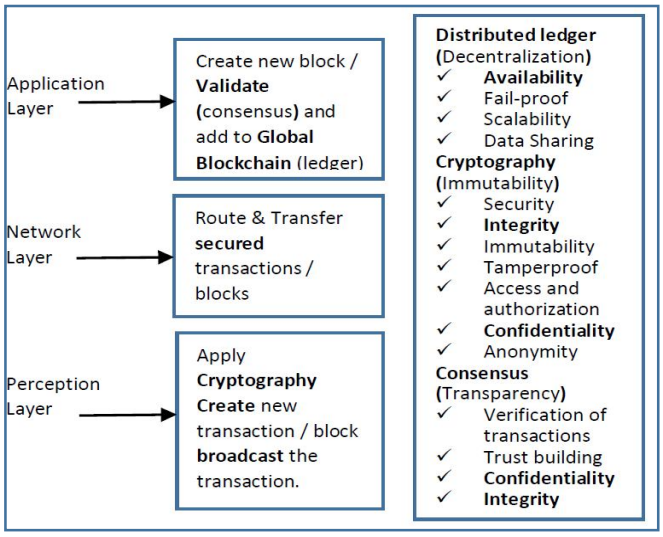


**Figure :**. Customized blockchain and security across layers

### *Perception Layer Adoption*

The data sensed from the IoT devices in this layer is considered for the creation of the transaction. The transaction formed at the perception layer node stored in a local block/memory pool and gets broadcasted into the application layer nodes. The local chain is maintained at the edge nodes till the chain is within the defined size limit or within the time limit. The data / block migration is achieved by the migration module using the thresholds of memory size and time duration limits. Once the local blockchain reaches the memory size limit and all blocks of the blockchain are transferred to the application layer then the local chain gets deleted [*Figure 4*].

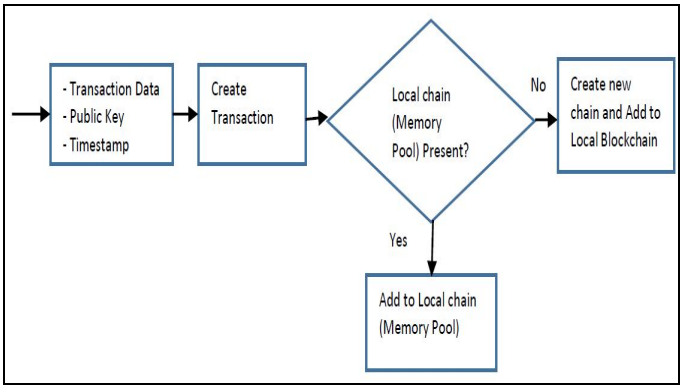


**Figure 4:**Transaction, block, local chain (partial) formation

### *Application Layer Adoption*

Each transaction received from the perception layer thru network layer gets added into the blockchain by following a simple consensus of validating the device identification (public key). The node at an application layer uses the public key and private key for authorized access of the block (*Figure 5*). The implementation to make sure the transactions stored in the blockchain adheres to access, authorizations, confidentiality and anonymity as defined in the blockchain contract rules by maintaining integrity of the data as a need to secure the transactions.

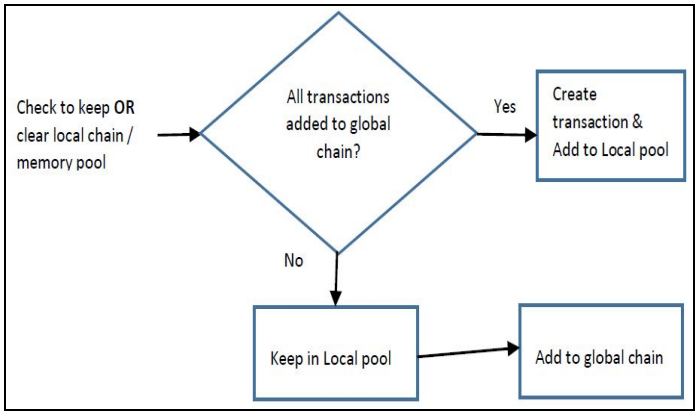


**Figure 5:** Forming global blockchain (complete)

**No adoption at the network layer**, but the secured transaction gets routed through the communication and network layer. The data / blocks are validated using the applicable key values and an algorithm.

## 5. IMPLEMENTATION AND RESULTS

The implementation uses the open-source blockchain '*Ethereum*' by connecting to '*testnet'* which is a public blockchain for testing. Ethereum is a global, decentralized platform for currency and other applications in the public domain in a secure manner. Ethereum can be used for applications that control currency or transactions using the distributed application (*dApp*) accessible anywhere on the Internet.

### *Implementation:*

The block diagram showing implementation in IoT with Mobile as edge/Wallet & p2p node as the Application layer Node is shown in [*Figure 6*]. The high-level steps of implementation are listed in [*Steps 1*] and the security factors verification listed in [*List 1*].

- Mobile device used as an edge node(s) to take data from the perception layer. Mobile devices to get the IoT data (image captured using a mobile APP).
- One of the computers in the application layer used as p2p node in our network to receive the transaction data (blocks) and maintain the blockchain.
- Create public and private keys for both:
  - Edge node(s), mobile device(s) used as wallets to send the transaction.
  - p2p nodes to maintain the blockchain for our transactions.
- Smart contract program at Ethereum network executed by Wallet client at edge node(s)
  - Package the captured image as transaction
  - Keep the transaction local memory pool, full blockchain not maintained in the edge nodes.

- Send the transaction to the global blockchain at an application layer p2p node(s).

- Smart contract program on the Ethereum network to do the following tasks:
  - Consensus to verify the public key to ensure transactions from designated edge nodes.
  - The block gets added at global blockchain on the distributed p2p network of nodes.

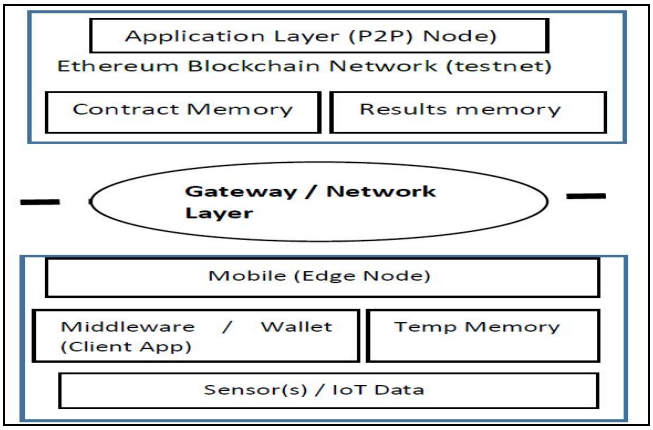


**Figure 6:** Edge/Wallet (Mobile) & p2p node (Application layer)

**Results and Analysis:**

The sample transactions and block results while doing blockchain transactions are shown [Figure 7 and Figure 8.]. The transactions at an edge node are put into public blockchain and accessed. The testing is done to verify and ensure the security of the data in terms of integrity and, confidentiality as listed in [List 1]. For verification, a single node is created to access the data on the network. Blocks (transactions) added to the blockchain (blocks) with a simple consensus of checking the designated edge node addresses (keys) at the application layer.

***List 1: Testing and Verification of security factors.***

**START:**

Verified the following ***security*** aspects

1. **Integrity –** data is same at all points: At edge node before sending to blockchain and application layer after retrieved from blockchain.
2. **Immutability/Tamperproof** – Not able to modify.
3. **Access and authorization** – Able to access data on the blockchain only by an authorized person (private and public key pair).
4. **Confidentiality**– Access possible only by an authorized person (private and public key)
5. **Pseudonymous** – Users identity only known by the public key and can access data on blockchain only using these key values.

**END.**

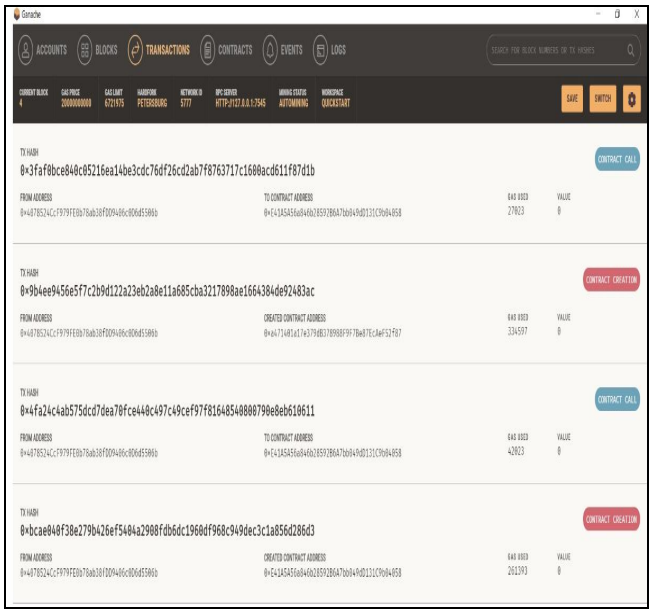


**Figure 7:** Transactions on test blockchain

***Steps 1. Implementation of blockchain in IoT for Security***

**START**

**1.** Setup development *truffle framework* with editor for development, deploy smart contracts.

**On local blockchain**

**2.** Setup local blockchain for testing, *Ganache*

**3.** Develop, compile, deploy and test smart contracts using *Solidity* programing language
   a. Creating transactions
   b. Adding transactions to test blockchain
   c. Retrieval of blocks from block chain

**On public blockchain**

**4.** Get free ETHER for using on public blockchain, Test Ether Faucets - *Rinkeby faucet*

**5.** Get public & private keys for blockchain Wallet on Mobile (mobile device).

**6.** Get public & private keys for blockchain p2p node(s).

**7.** The public *testnet* blockchain is used to connect and test.

**8.** Connect to public blockchain
   - Get wallet, *metamask* to manage the account on the network
   - Connect to an Ethereum node
   - Setup project settings to access the Ethereum node

**9.** To migrate, deploy and test on public blockchain

**10.** Package and send the data (image) as a transaction to p2p node from the edge node using Wallet application (*WallETH).*

*11.* Communicating With Ethereum, *Web3.js* JavaScript API.

**12.** Smart contract on public blockchain to consensus to validate the data from designated edge nodes.

**13.** Add block to the blockchain on Ethereum network

**14.** Access block and verify data for integrity and confidentialitv.

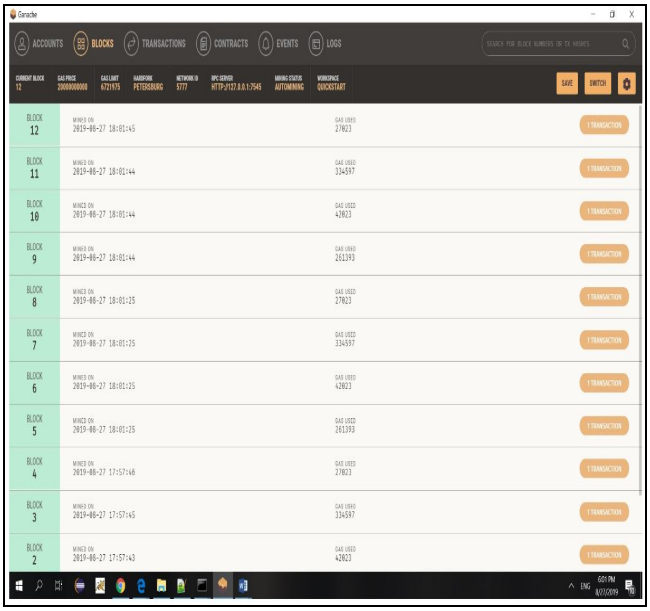


**Figure 8:** Blocks created on test blockchain

## 6. CONCLUSION

Security with the Internet or without the Internet in the IoT environment is one of the critical challenges which needs solutions to handle the threats and vulnerabilities in the IoT environment. The literature review done on various types of attacks and security solutions indicate that the security is an ongoing activity. The technological evolution leading to new vulnerabilities and attacks needs new solutions. The reviews of research works and solutions in IoT environments indicate the usage and adoptions of different research approaches for security including machine learning and blockchain technologies.

All of the technology components of blockchain are highly resource-demanding. The proposed model adopts the features by the specific design consideration '*ADOPT*'. The model adopts blockchain features cryptography, distributed ledger and, the consensus at the application layer nodes. At the perception layer, a local temporary chain (memory pool) suitable for resource-constrained IoT is maintained. The proposed model is implemented using smart contracts in the test environment for (i) maintaining the local memory pool as a temporary local chain (ii) moving the data/transactions to the global chain (iii) consensus approach of using the device identifications for validating the transactions. The research approach and model can be adopted in the IoT systems in real-time scenarios using the existing blockchain systems that have the capability to support the development of new modules and functions (programming abilities) for managing the overall transactions and consensus. For the simulation of the model, an open-source blockchain platform Ethereum is used. Ethereum supports smart contracts which is a strong technology tool for tailoring the adoptability by specific rules of an implementation of the technology features. The approach is verified by checking the access and authentication, integrity, and confidentiality as security factors

## 7. FUTURE RESEARCH DIRECTIONS

The Blockchain technology have functional features to adopt the technology for IoT scenarios. The consensus methods is a heavy resource-demanding technology that needs to be scaled for the IoT environment as the IoT environment has very specific and unique requirements. So, the immediate future work will be on research and solutions on consensus approaches for device configuration, management, identification, and registration of IoT devices for optimal technology and business solutions for security in IoT environments using blockchain.

## ACKNOWLEDGEMENT

Thanks to Jain University for providing access to resources and providing an opportunity to work on research activities and providing access to research literature and facilitating the execution of research. Thanks to colleagues of ISE department at MSRIT for support and ePrayag Software Private limited for facilitating the test environment and data for verifying the results.

## REFERENCES

1. Alkurdi, F., Elgendi, I., Munasinghe, K. S., Sharma, D., & Jamalipour, A. (2019). Blockchain in IoT Security: A Survey. 2018 28th International Telecommunication Networks and Applications Conference, ITNAC 2018, 1–4. https://doi.org/10.1109/ATNAC.2018.8615409
2. Banerjee, N., Giannetsos, T., Panaousis, E., & Took, C. C. (2018). Unsupervised learning for trustworthy IoT. IEEE International Conference on Fuzzy Systems, 2018-July, 1–8. https://doi.org/10.1109/FUZZ-IEEE.2018.8491672
3. Bassi, A. (2013). Internet of Things Architecture: Mission. IOT-A: Internet of Things Architecture, 257521, 1–256. http://www.iot-a.eu/public/introduction/missioncollage
4. Ravi, C. Bhaddurgatte., & Vijaya Kumar, B. P. (2015). A Review: QoS Architecture and Implementations in IoT Environment. Research & Reviews: Journal of Engineering and Technology, 2016, 6–12. http://www.rroij.com/open-access/a-review-qos-architecture-and-implementations-in-iot-environmnt.php?aid=63427
5. Ravi, C. Bhaddurgatte., Vijaya Kumar, B. P., & Kusuma, S. M. (2019). Machine learning and prediction-based resource management in IoT considering Qos. International Journal of Recent Technology and Engineering, 8(2), 687–694. https://doi.org/10.35940/ijrte.B1705.078219
6. Canedo, J., & Skjellum, A. (2016). Using machine learning to secure IoT systems. 2016 14th Annual

Conference on Privacy, Security and Trust, PST 2016, 219–222. https://doi.org/10.1109/PST.2016.7906930

7. Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, 0. https://doi.org/10.1109/AICCSA.2016.7945805
8. Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 32–37. https://doi.org/10.1109/I-SMAC.2017.8058363
9. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. Proceedings - 2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (Part of CPS Week), 173–178. https://doi.org/10.1145/3054977.3055003
10. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (n.d.). (2017). LSB : A Lightweight Scalable BlockChain for IoT Security and Privacy. 1–17.
11. Gupta, Y., Shorey, R., Kulkarni, D., & Tew, J. (2018). The applicability of blockchain in the Internet of Things. 2018 10th International Conference on Communication Systems and Networks, COMSNETS 2018, 2018-Janua, 561–564. https://doi.org/10.1109/COMSNETS.2018.8328273
12. Jeon, J. H., Kim, K. H., & Kim, J. H. (2018). Block chain based data security enhanced IoT server platform. International Conference on Information Networking, 2018-Janua, 941–944. https://doi.org/10.1109/ICOIN.2018.8343262
13. Karande, J. B., & Joshi, S. A. (2018). Comprehensive Assessment of Security Attack Detection Algorithms in Internet of Things. Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018, 1–6. https://doi.org/10.1109/ICCUBEA.2018.8697406
14. Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. IEEE Internet of Things Journal, 1(3), 265–275. https://doi.org/10.1109/JIOT.2014.2323395
15. Kuhn, R., & Weil, T. (2017). Can Blockchain Strenghtne the IoT? Securing IT, August, 68–72. https://doi.org/10.1093/cercor/bhh040
16. Krishnan, K. N., Jenu, R., Joseph, T., & Silpa, M. L. (2018). Blockchain Based Security Framework for IoT Implementations. 2018 International CET Conference on Control, Communication, and Computing, IC4 2018, 425–429. https://doi.org/10.1109/CETIC4.2018.8531042
17. Lao, L., Li, Z., Hou, S., Xiao, B. I. N., Hong, T., & Polytechnic, K. (2020). A Survey of IoT Applications in Blockchain Systems : Architecture, Consensus, and Traffic Modeling. 53(1).
18. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. IEEE Internet of Things Journal, 4(6), 1832–1843. https://doi.org/10.1109/JIOT.2017.2740569
19. Moh, M., & Raju, R. (2019). Using Machine Learning for Protecting the Security and Privacy of Internet of Things (IoT) Systems. Fog and Edge Computing, 223–257. https://doi.org/10.1002/9781119525080.ch10
20. Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the Internet of things. Computer, 46(4), 46–53. https://doi.org/10.1109/MC.2013.74
21. Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the Internet of things. IEEE Sensors Journal, 13(10), 3711–3720. https://doi.org/10.1109/JSEN.2013.2277656
22. Santhosh Krishna, B. V., & Gnanasekaran, T. (2017). A systematic study of security issues in Internet-of-Things (IoT). Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 107–111. https://doi.org/10.1109/I-SMAC.2017.8058318
23. Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. Technical Report.
24. Singh, M., Singh, A., & Kim, S. (2018). Blockchain: A game changer for securing IoT data. IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings, 2018-Janua, 51–55. https://doi.org/10.1109/WF-IoT.2018.8355182
25. Singla, K., Bose, J., & Katariya, S. (2018). Machine Learning for Secure Device Personalization Using Blockchain. 2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018, 67–73. https://doi.org/10.1109/ICACCI.2018.8554476
26. Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2018). A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. Proceedings - 2016 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI 2016, 2018-Janua(6), 519–524. https://doi.org/10.1109/IIKI.2016.3
27. Symantec. (2019). Internet Security Threat Report VOLUME 21, February 2019. Network Security, 21(February), 61. https://doi.org/10.1016/S1353-4858(05)00194-7
28. Wang, Z., Dong, X., Li, Y., Fang, L., & Chen, P. (2018). IoT Security Model and Performance Evaluation: A Blockchain Approach. Proceedings of 2018 6th IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC 2018, 260–264. https://doi.org/10.1109/ICNIDC.2018.8525716
29. Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 1–32.

https://doi.org/10.1017/CBO9781107415324.004(Wood , 2014)

30. Xu, J. J. (2016). Are blockchains immune to all malicious attacks? Financial Innovation, 2(1). https://doi.org/10.1186/s40854-016-0046-5
31. Yang, Y., Wu, L., Yin, G., Li, l.,& Zhao, H. (2017). A survey on security and privacy Issues. IEEE Internet of Things Journal, 4(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844
32. Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. IEEE Wireless Communications, 25(6), 12–18. https://doi.org/10.1109/MWC.2017.1800116
33. Majeed, A., Bhana, R., & Parvez, S. (2019). Controlling energy consumption by internet of things (Iot) applications. International Journal of Advanced Trends in Computer Science and Engineering, 8(1), 8–11. https://doi.org/10.30534/ijatcse/2019/0281.12019
34. Krishna Chaitanya, A., Prasanthi, M. L., & Sambasivarao, N. (2019). Cryptographic based message transfer using block chain technology. International Journal of Advanced Trends in Computer Science and Engineering, 8(1.3 S1), 45–50. https://doi.org/10.30534/ijatcse/2019/1081.32019