A Blockchain-based Security Architecture for the Internet of Things

KELECHI G. EZE, CAJETAN M. AKUJUOBI, SHERMAR HUNTER,
SHUMON ALAM, SARHAN MUSA, JUSTIN FOREMAN
The Center of Excellence for Communication Systems Technology Research (CECSTR)
Roy G. Perry College of Engineering
Prairie View A&M University, Prairie View Texas 77446, USA

Abstract: - The Internet of Things (IoT) is growing at a very fast pace and being increasingly adopted in many scenarios of industrial applications such as energy (smart grid), automobile (smart cars), healthcare (smart healthcare), manufacturing (smart manufacturing and supply chain) and other application such as homes (smart home) and cities (smart city). Nonetheless, these IoT technologies (devices, systems, protocols, and applications) are faced with many security-related issues. IoT Systems have different layers that are vulnerable to various kinds of attacks. To defend against these attacks, one must consider appropriate security approaches and mechanisms to ensure privacy, security, and trust within the various components and layers that make up the IoT system. Appropriate security mechanism is needed at every layer of an IoT system to keep them secure. Hence, finding suitable mechanism for each IoT layer is a necessity to keep IoT systems secure in the 21st-century applications and implementations. The paper first investigates the IoT layers and protocols, their vulnerability issues, and methods to resolve the issues from existing literatures. We then present a blockchain-based security architecture for the internet of things and practically investigated its security feature through implementation of various security mechanism. Analysis and discussion of the blockchain implementation results are carried for the purpose of meeting the security, privacy, and trust requirements of IoT.

Key-Words: - Internet of Things, Blockchain, Threat model, Attacks, Security mechanisms

Received: March 5, 2021. Revised: January 10, 2022. Accepted: February 15, 2022. Published: March 23, 2022.

1 Introduction

Internet of Things (IoT) is a world wide web (WWW) infrastructure for the efficient creation, manipulation and accessing information by interconnecting uniquely addressable physical and virtual objects based on existing and evolving interoperable information and communication technology [1,2]. The advancement in sensor technology, the explosion of IoT devices and the increased adoption of IoT in many applications e.g., manufacturing, healthcare, oil & gas, government, smart grid, home automation are some of the key indicators of a tremendous growth future for IoT. It has the potential for enabling increased efficiency in industrial processes and services and convenience in most of our daily lives both at home and work. Examples of everyday usage of IoT devices and functions are wearables like a heart rate monitor, fitness bands, virtual glasses to name a few. The heart rate monitor uses a sensor to sense the heart rate of the patient and that information goes through a router or gateway and sent over the internet to an end user (e.g., a doctor), who consumes it using a nice visualization front-end. Figure 1 shows the key components of an IoT with the IoT devices/sensors, routers, clouds, and user applications.

Internet of Things technology is a blend of many different technologies having some unique security requirements and challenges. It is therefore comprised of multiple unique layers such as device or perception layer, the network layer, the support or transport layer and the application layer that needs to be secured [3, 4, 5]. Within these layers are sensors embedded in different objects or things, gateways devices, software application, the internet, the cloud technology, and the supporting communication protocols. Most IoT application areas are mission critical for example, healthcare and automobiles making security and efficiency of Internet of Things in these applications a number one priority.

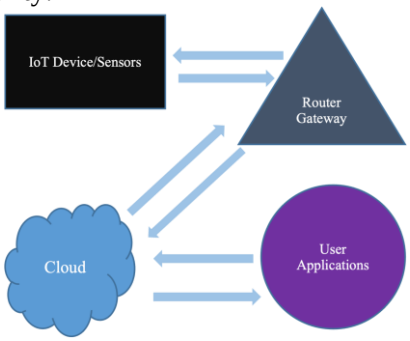


Fig. 1. Components of IoT

In the context of Internet of things security, the goal is to protect IoT systems assets and functions against damage from threat actors as well as adversarial attacks. IoT Assets includes all the hardware (e.g., sensors, servers, and gateways), application software (embedded code, real time operating systems (RTOS) and data that need to be secured from unauthorized access, use, destruction, or theft. A major challenge in IoT system is the provision of security across the IoT stack from sensor to the cloud. This is because of many reasons. (i) The device at the perception layer is computationally and memory constrained making it challenging to implement security solutions at this layer. (ii) Most of the IoT hardware and protocols at the perception layer have vulnerability by design because the focus at the design stage is functionality and not security. (iii) There are several enabling technologies involved in IoT systems with different security requirements and integration of these technologies becomes a challenge (iv) The use of client server model in IoT system design increases the risk of system-wide failure. (v) Lack of algorithms and mechanisms for efficient key management becomes another issue within a heterogeneous and decentralized IoT network. (vi) The increasing number of IoT devices connected to the Internet has expanded the entry points of adversaries and threat actors. (vii) There are many sophisticated tools and threats to compromise vulnerable IoT system components. Faced with these challenges, it is paramount to explore and find ways of ensuring availability, confidentiality, and integrity in IoT systems by efficient security mechanisms, system design and configuration.

Other challenges facing Internet of Things are related to the problem of standardization, addressing, connectivity and battery life. The proliferation of Internet of things devices that form a part of the global internet must be uniquely identifiable with an IP address. This necessitate widening of the address space and a shift to IPv6 where compatibility issues with low power devices is further faced. Standardization issues emerges because of the many enabling technologies (involved in IoT, which cuts across many standards with new once emerging every day. The standardization problems propagate to interoperability and compatibility issues within IoT components. Implementing security mechanisms or features in IoT devices like device level encryption leads to increased power consumption [5]. This issue with battery life limits the application of IoT significantly in scenarios like remote offshore monitoring.

The paper properly analyzed these issues and carefully considered an appropriate solution considering the security requirements of IoT. The solution proposed in this paper is based on the blockchain technology that is popular for its security and application in IoT and related application. Therefore, IoT technology and the blockchain could be integrated to solve complex problems within IoT in the areas of security and operational efficiency [6]. A system architecture is presented and analyzed based on the requirements of IoT. Security analysis of the model is further taken care of.

The rest of the paper will be organized as follows. An overview of the Internet of Things and their applications is presented in Section 2. Section 3 discusses categories and types of IoT threats and attacks. Security mechanisms for the Internet of Things is the subject of discussion for section 4. In section 5 we discuss a novel low risk model for the Internet of things. Section 6 presents the security evaluation of the proposed model. Then section 7 concludes the paper.

2 Internet of Things and its applications

The Internet of things (IoT) is known to have been increasing in popularity and application in many use-cases, spanning across many technologies ranging from sensors, actuators, smart objects, Internet network, cloud technology and analytics technologies [1, 2]. An IoT system or solution consist of four main layers, the perception layer, the network layer, support layer and the application layer [3]. The security configuration of IoT is closely related to the architectural design for a particular use case environment. For example, a healthcare environment must commit substantial amount of investing into security design robustness to ensure a high level of security and maximum availability of services as downtime due to breach or system failure could cost human life. Conversely, a smart home will not have a catastrophic effect like a smart healthcare if anything goes wrong, however proper security control must be ensured for vital assets especially sensitive information in every IoT application. We proceed to investigate today's top IoT application.

2.1 Smart Healthcare (SH)

IoT have gained application in various important aspects of healthcare service delivery. These are remote patient monitoring and diagnosis where vital signs of certain patients can be monitored using wearable and implantable IoT devices at the convenience of their homes which involves real-time sensing, storage and analytics for doctors and nurses to make prompt decisions regarding patient health [7, 8]. Smart remote surgery where doctors are equipped with IoT enabled devices to perform surgical operations on patients remotely, thereby removing the distance barrier between surgeons and patients. There are many others such as equipment monitoring and hygiene condition monitoring. Advantages of smart healthcare are – opportunities to detect illness early and in real-time, accessibility of healthcare to remote locations, improved efficiency in healthcare and flexibility in healthcare services. On the other hand, challenges facing smart healthcare are technological challenges (such as that seen in blockchain technology), integration of various technologies (sensing, communication, processing, storage, and visualization), security and risk of smart healthcare system.

2.2 Smart Manufacturing (SM)

The Internet of Things enables smart manufacturing. It involves the use of intelligent algorithm derived by learning on sensor data and built into manufacturing systems and units to enhance the overall manufacturing tasks. SM therefore applies emerging Internet-based technologies such as IoT, Artificial Intelligence (AI) and big data to make manufacturing process internet based, adaptable, efficient, and flexible [9]. Other enabling technologies are Cyber physical systems, simulation and modelling, autonomous robots, and cloud computing. Smart manufacturing then uses these enabling technologies to solve complex problems in manufacturing such as fault diagnosis, predictive maintenance, optimized supply chain leading to cost saving and maximum equipment uptime and available. The large volume of manufacturing data derived from IoT devices and sensors are analyzed and turned into value to improve operational efficiency. Data from customer feedback are used for advanced customization and satisfaction. Conversely, SM faces challenges that comes with integration of different (new and existing) technologies in terms of cost of implementation that are required to work together efficiently. In addition, the density of connectivity in SM environment raises the cybersecurity risk of adopting SM. Implementing solutions to ensure security in smart manufacturing environment requires extra capital cost as well.

2.3 Smart Automobiles (SA)

Today, the automotive product like automobiles involves high scale integration of software, hardware, and sensors to make them aware and interactive with their environment using the internet networks. These interactions are usually in form of vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications. Therefore, the various components of an automotive system must be designed to meet extra requirement of cybersecurity safety in addition to performance, quality, and efficiency. The impact of an attack on smart automobile could be a very catastrophic accident that can results to lose of lives and destruction of assets. Since most advanced safety, quality, usability, and adaptability features in automotive systems are enabled through software and these account for the over 100 million lines of code in modern automotive, there must be advanced tools for testing and always measuring the cybersecurity risks in them. These tools must be a core part of the system to give necessary warnings or complete shutdown if proper security measure is not taken.

2.4 Smart City (SC)

At the core of smart city technology is the IoT. IoT sensors in smart city are used to collect data from which insights are built for efficient management and delivery of resources and services in an urban area or city (New Your city or Dubai). Smart city often involves the interconnectivity and interoperability of various IoT solution working together to deliver city-wide services such as smart transportation, smart grid, water management, environmental monitoring (e.g. weather etc.) Although the purpose of smart city applications is to improve the overall quality of life of the citizens, it also comes with many threats to the privacy of these citizens. For example, services like the smart payment using the Smart card tend to require sensitive personal information of users and collect information purchase behavior of the citizens that undermines security and privacy of the users. In addition, Smart mobile applications often time exposed the location information of the users. These are essential applications used for example by parents to track the location of their child in many

ways, therefore a compromise of such application but the safety of that child at a risk

2.5 Smart Grid

The smart grid is built on top of the Internet-of-Things (IoT) which involves many smart physical objects interconnected by networks [10]. Smart Grid presents complexity in terms of diverse communication protocols, range, and number of physical components. The severity of attack on smart grid could be very high if vulnerable risk components such as smart meters and automotive charging station are not properly secured.

3 Threats and attacks in Internet of Things

Internet of Things (IoT) has a huge security concern because of its infinite scope of vulnerabilities and attacks and growing threats on its assets [11, 12]. The vulnerabilities and threats have left many ways through which the IoT assets can be compromised. This problem if left unsolved, important assets such as sensitive information and other resources could be stolen or destroyed. The growth of IoT technologies could also pose a severe threat because the many IoT devices around us, that can sense, store, compute, and communicate information significantly elevates the attack surface. Accordingly, because of the growth of IoT, new security challenges arise in the existing security framework that need to be addressed [12, 13]. A better understanding of adversary attacks in IoT are crucial as they are the major hindrance to the development of IoT in the various domains of its applications [12, 13].

3.1 Vulnerabilities in the IoT systems

IoT security is the protection of IoT assets against cyber-attacks in the presence of adversaries. In a layered IoT model, each layer has its own vulnerabilities that could lead to cyberattacks. Vulnerability are security weaknesses, flaws, or holes in the IoT assets like devices, protocols and data that. The vulnerabilities scope in IoT systems is usually infinite [12]. However, vulnerabilities are broadly grouped into four major types: missing security controls, system bug (flaw), user actions and organizational actions. The common vulnerabilities are discussed below.

3.1.1 Deficient physical security

Most IoT devices are made and left alone with little to no security mainly because they are low-cost and can function without the help of a person [14]. Unless a security issue arises, which may not be obvious in most cases, the IoT is left vulnerable to a physical attack. An example would be someone having physical access to a sensor and disturbing it that way.

3.1.2 Insufficient energy harvesting

IoT devices unfortunately have limited power or energy [14]. If a sensor were to be battery powered like a smart parking application, it would be susceptible to a sleep deprivation attack where the IoT device would hopelessly have all its energy drained causing it to power down. Sleep deprivation attacks are explained in Section 4.

3.1.3 Inadequate authentication

Authentication keys are used to access the IoT when complicated authentication methods are being implemented [10]. If these keys were to be lost, stolen, damaged or destroyed the complex authentication would be used against the users. An example would be losing the authentication key to an IoT database containing private information on clients or applications, like a bank which would include personal information, passwords, etc.

3.1.4 Improper encryption

Despite encryption technology coming a long way, the possibility of an attacker successfully decrypting data within an IoT is not impossible if the encryption is weak [14]. An example would be an attacker cracking the encryption with a random decryption key.

3.1.5 Unnecessary open ports

Some IoT devices that have open ports while running services and applications, can be compromised by an adversary who wants to take advantage of such a vulnerability in the system [14]. An example of an open ports in IoT is a conversation between to people through e-mails, a port would need to be open for the e-mail to go through. Any open port is vulnerability that an attacker can exploit.

3.1.6 Insufficient access control

Most IoT devices do not enforce adequate access control mechanisms in which in which strong and complex passwords are required. Others do not even request a change from the default password authentication [10]. For example, some IoT devices, such as smart phones or smart cars, and applications only require the default access credentials to grant access to users.

3.1.7 Lack of software updates

Tiny or Real Time Operating Systems (RTOS) in IoT and related applications should be updated appropriately, but sometimes these updates lack proper security making it possible for an attacker to modify the update for personal gains [14]. For an example, an update for an application could add a new feature, but this new feature could overlook a security issue.

3.1.8 Improper patch management capabilities

While code is improving and becoming more secure, there are cases where a program is released with vulnerabilities obvious to the hackers [14]. An example would be a programmer using a very common algorithm in the code of an IoT and the hacker exploiting the weakness of the algorithm because they know how that code works.

3.1.9 Insufficient audit mechanisms

Many IoT devices lack detailed and full logging procedures, this issue makes it possible for attackers to act unnoticed within the IoT [14]. An example would be an attacker being able to delete the history of their actions after an attack.

3.2 Threat and Attacks in IoT Systems

The IoT is a complex ecosystem that entails a variety of applications, technologies, protocols, devices, and users. Accordingly, an IoT solution has four layers: the sensing layer, the gateway layer, the network layer and the application and service layers. Figure 2 shows the various layer in IoT protocol stack. The complexity of IoT makes the attacks more complex and widespread in most cases as it could span geographic boundaries. Figure 3 shows common attacks in IoT systems. These attacks on IoT can be prevented by studying the threats associated with IoT solution and implementing security controls and mechanisms usually early in the design stage as countermeasures to mitigate against threats and attacks. Threats in IoT systems are studied by performing threat modeling. Threat modeling is carried out on the IoT system by taking its various components into account to enumerate possible threats and the countermeasures necessary to prevent such threats.

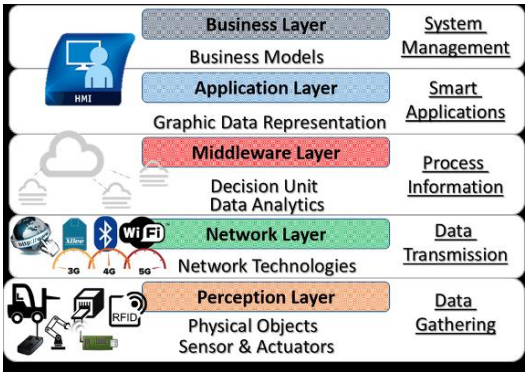


Fig 2. IoT protocol stack

3.2.1 Device Capturing

IoT devices on the perception layer constitutes of several heterogeneous constrained nodes such as sensors and actuators. Devices on this layer are vulnerable to a variety of threats. The attackers may malicious node could be accessed or captured in the IoT system, which will now act as rogue node that is controlled. This could lead to other serious and complex attacks on the IoT system.

3.2.2 False Data Injection Attack

This type of attack is a second level of device capturing attack on IoT device where the captured node is taken advantage of and used to produce erroneous data that is transmitted onto the IoT system. This usually leads to false results on the consumer and the malfunctioning of the applications that run on the IoT network. The false data injection attack is the basis on which DDoS attacks are perpetrated. Variants of replay false data injection attack are the replay attacks.

3.2.3 Code Injection

Processes on embedded devices often runs with the highest level of privilege that makes code injection on these devices highly expansive causing device malfunction and data compromise. This type of

attacks occurs when an adversary injects malicious code into the embedded code of the constrained node on the perception layer. The vulnerabilities in todays over the air method of firmware upgrade in IoT presents a hole or vector through which attackers inject malicious code that could cause wide ranging adverse effects on the IoT system.

3.2.4 Timing Attack

This is also known as Side Channel Attacks. Side channel attacks are categories of indirect attacks on IoT devices that result to sensitive information leakage in IoT networks. The statistically analyses of the timing or power consumption of the execution of cryptographic algorithms as well as the microarchitectures of processors and electromagnetic consequences leaks sensitive device information. Side channel attacks is be based on power consumption, laser-based attacks, timing attacks or electromagnetic attacks. Positive countermeasures are being implemented on modern IoT device component to prevent channel attacks.

3.2.5 Eavesdropping Attacks

This could also be referred to as sniffing or snooping attack, which is launched against sensor data as it is being transmitted over an unsecure protocol. In other words, the adversaries successfully intercept the IoT communication channel to perform Eavesdropping attack [15].

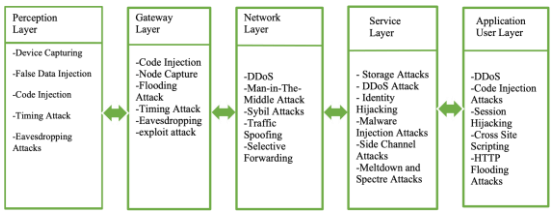


Fig 3. Common attacks in IoT

3.3 Security Control consideration for the Internet of Things

Security controls (mechanisms) are set of techniques or technical tools that are used to implement countermeasures to vulnerabilities, threats, and attacks in computer systems, including IoT. They range from firmware update mechanisms (OTA), various access control techniques, and data in motion encryption to encrypted storage optimized to provide Confidentially Integrity and Availability in IoT and other specialized security requirements of IoT. Other security mechanisms involve the use of security appliances like the firewalls, proxies, and technology platform like the blockchain technology and the actor model of computation. Most security mechanisms today largely depend on cryptographic techniques, antimalware and firewalls, Intrusion Detection (IDS) however emerging technologies like the machine learning and blockchain technology have proven very effective in protecting IoT from various attacks that target them [16].

4 Proposed Distributed Architecture for The Internet of Things Security Implementation

4.1 Distributed Architecture

The proposed model adopts the blockchain technology for the purpose of decentralizing the IoT system and enforcing system-wide security in the system. Hence, a distributed architecture appropriate for peer-to-peer communication pattern, scalability and fault-tolerance needed in IoT is presented for a system-wide security in IoT using the blockchain platform. Figure 4 shows the proposed blockchain-based distributed model for IoT. In as much as the proposed model contains all the components that make up the IoT ecosystem, the network architecture is decentralized with blockchain and thus eliminates the various network layer attacks and single points of failure of the client server model. Thus, the following are the components of the model

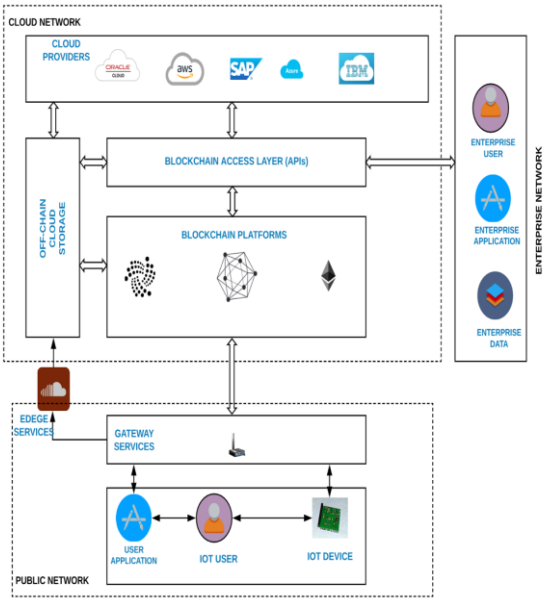


Fig 4. Distributed architecture for IoT

4.1.1 Perception or Sensing Layer

The sensing part in the proposed model corresponds to the physical layer in a traditional TC/IP network architecture concerning functions. It is made up of sensors and the physical medium separating them from an IoT gateway and carries out sensing. Depending on a particular design, these sensors can be embedded inside the gateway or communicate with the gateway using a low power protocol (Bluetooth, NB-IoT, 6LowPAN, Lora WAN etc.) while the gateway is Internet Protocol enabled to be part of the blockchain network and communicate with the rest of IoT network.

4.1.2 The Network Layer

The network layer represents the distributed blockchain network that delivers the functions of the network layer in a typical TCP/IP model. Hence, the network layer handles functions such as secure peer-to-peer transmission and routing of information and logical address of distributed network components. The network topology for a blockchain network is different variation of graphs with the particular graph depending largely on the design and use case. In the case of IoT directed acyclic graphs (DAG) is the recommended topology for enhanced network efficiency in terms of transaction throughput.

4.1.3 The cloud and Service Layer

his is where the heavy lifting occurs, such as bulk storage and computations. This can also be referred to as the computational back end of the IoT network that handles data storage, protection, and processing. Algorithms such as encryption to protect data in storage (i.e., data at rest) and AI to turn the data into meaningful insights to be provided as a service to user applications run on this layer. Smart contract is at the heart of the whole network, enforcing rules of communication, visibility and access and determines what ends up in the cloud storage.

4.1.4 The applications or User layer

This constitutes the enterprise network or user network that communicates with the cloud to access the results or service of the IoT systems and to manage their enterprise data. The application or user layer is a part of the blockchain network and very secure as every node is modeled to run on the blockchain that is cryptographically protected and configured with no single point of failure.

4.2 Threat Modeling of The Proposed Model

We use threat modeling for analyzing the security of the proposed model with the goal of eliciting threats and vulnerabilities to know what countermeasures to focus on. There are many approaches to threat modelling however the most popular threat modeling approaches are the STRIDE model and Attack graph approach. Threat modeling also helps avoid introducing vulnerability during the design of IoT systems as well as identifying vulnerability in existing IoT systems. Hence its approach used to analyze and understand the business systems from a security point of view [17]. Threat modeling is therefore an incremental process that changes every time the IoT system changes. We adopted the stride approach due to its ease of use and reproducibility. We adopted the Microsoft threat modelling tool. The inputs to the threat modeling tools are the system model with explicit specifications on the components and data flows. The output is the system with enumerations of threats and possible counter measures. This output is shown in Figure 6. This helps to know the countermeasure to focus on while integrating the initial model with the blockchain. The process is repeated on the final proposed model. We have shown the discussed threat modeling process in Figure 5.

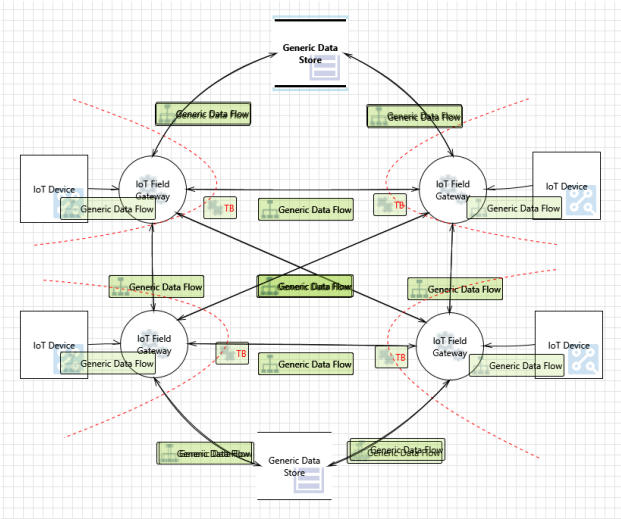


Fig 5. Threat model of the proposed model

Threat Modeling - Version 1

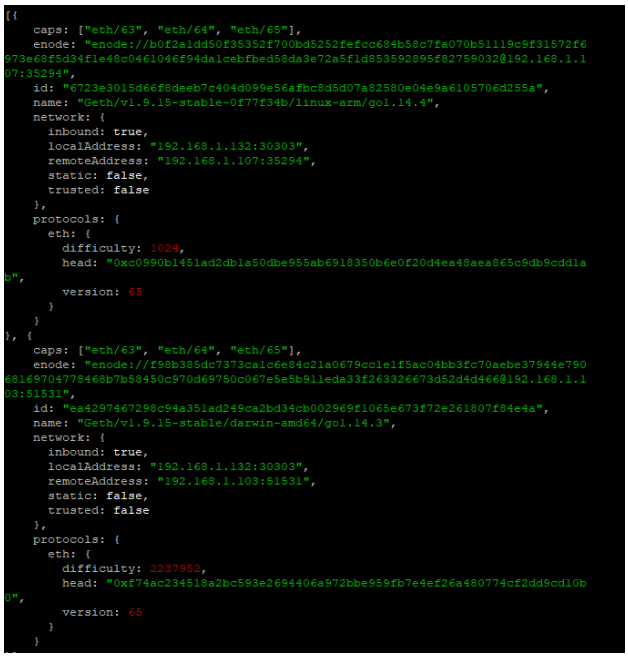
Category	Interaction	Priority	Description	Possible Mitigation	Phase	Frequency
Spoofing	Generic Data Flow	High	An attacker may extract cryptographic key material from the IoT gateway either at the software level of hardware level An Adversary may replace the IoT field gateway or its part with other IoT device An adversary may gain access to the field gateway by leveraging faulty credentials	-Ensure device authentication -Ensure default credentials are changes	Design Implementation	56
Tampering	Generic Data Flow	High	An adversary gain unauthorized access to IoT Field Gateway, Tamper its OS and get access to confidential information -may launch malicious code into IoT field gateway and execute it -may perform man in the middle attack on encrypted traffic sent to the IoT field gateway -may leverage vulnerability and exploit the device if the firmware of the device is not updated	-Encrypt OS -Verify X.509 certificate -Store cryptographic keys securely -Ensure cloud gateway implement secure processes -Use per-device authentication	Design Implementation	82
Repudiation	Generic Data Flow	High	Actions such as spoofing attempst, unauthorized access; It is important to monitor these attempts	-Ensure appropriate logging and auditing is ensure on the gateway	Design	20
Information Disclosure	Generic Data Flow	High	An adversary may eavesdrop and interlene with the communication between the device and the field gate	-Secure device to field gateway communication	Design	4
Denial of Service	Generic Data Flow	High	N/A		Design	0
Elevation of privilege	Generic Data Flow	High	Adversary leverage insufficient authorization check on the gateway and execute malicious commands remotely -may gain access to admin interface or privileged services like WiFi, SSH, File shares, FTP on a device -may use unused features or services such as UI, USP ports, etc.; Unused features expands the attack surface	-Ensure minimun services/ features are enabled on devices -Ensure admin interface are secured	Design Implementation	44

Figure 6: Threat modeling

4.3 Implementation of security mechanisms

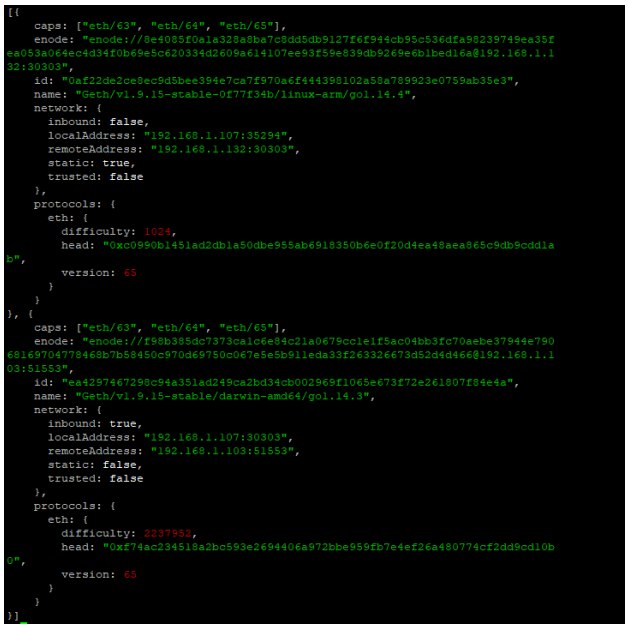
Using the proposed model as a reference, a permissioned blockchain network is set up as a testbed using heterogeneous IoT devices namely, embedded temperature sensors and light sensors, raspberry pie and traditional computing device MacBook computer and a user device smart phone. The embedded sensors represent the sensing layer, the network layer is a private Ethereum network that was set up in the lab environment. The cloud is represented by the MacBook computer while the user can consume service (readings of the sensor) to monitor the temperature of the surrounding from the smartphone. Figure 7 shows the network set up of the sample implementation and Figures 8 and 9 shows the peering of the IoT nodes in the network.

Fig 6. Network setup



```
[{
    caps: ["eth/63", "eth/64", "eth/65"],
    enode: "enode://b0f2a1dd50f35352f700bd5252fefcc684b58c7fa070b51119c9f31572f6
973e68f5d34f1e48c0461046f94da1cebfbed58da3e72a5f1d853592895f82759032@192.168.1.1
07:35294",
    id: "6723e3015d66f8deeb7c404d099e56afbc8d5d07a82580e04e9a6105706d255a",
    name: "Geth/v1.9.15-stable-0f77f34b/linux-arm/go1.14.4",
    network: {
      inbound: true,
      localAddress: "192.168.1.132:30303",
      remoteAddress: "192.168.1.107:35294",
      static: false,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 1024,
        head: "0xc0990b1451ad2db1a50dbe955ab6918350b6e0f20d4ea48aea865c9db9cdd1a
b",
        version: 65
      }
    }
}, {
    caps: ["eth/63", "eth/64", "eth/65"],
    enode: "enode://f98b385dc7373ca1c6e84c21a0679cc1e1f5ac04bb3fc70aebe37944e790
68169704778468b7b58450c970d69750c067e5e5b911eda33f263326673d52d4d466@192.168.1.1
03:51531",
    id: "ea4297467298c94a351ad249ca2bd34cb002969f1065e673f72e261807f84e4a",
    name: "Geth/v1.9.15-stable/darwin-amd64/go1.14.3",
    network: {
      inbound: true,
      localAddress: "192.168.1.132:30303",
      remoteAddress: "192.168.1.103:51531",
      static: false,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 2237952,
        head: "0xf74ac234518a2bc593e2694406a972bbe959fb7e4ef26a480774cf2dd9cd10b
0",
        version: 65
      }
    }
```


Figure 8: blockchain network node peering



```
[{
    caps: ["eth/63", "eth/64", "eth/65"],
    enode: "enode://8e4055f0a1a328a8ba7c0dd5db9127f6f944cb95c536dfa98239749ea35f
ea053a064ec4d34f0b69e5c620334d2609a614107ee93f59e839db9269e6b1bed16a8@192.168.1.1
32:30303",
    id: "0af22de2ce8ec9d5bee394e7ca7f970a6f444398102a58a789923e0759ab35e3",
    name: "Geth/v1.9.15-stable-0f77f34b/linux-arm/go1.14.4",
    network: {
      inbound: false,
      localAddress: "192.168.1.107:35294",
      remoteAddress: "192.168.1.132:30303",
      static: true,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 1024,
        head: "0xc0990b1451ad2db1a50dbe955ab6918350b6e0f20d4ea48aea865c9db9cdd1a
b",
        version: 65
      }
    }
}, {
    caps: ["eth/63", "eth/64", "eth/65"],
    enode: "enode://f98b385dc7373ca1c6e84c21a0679cc1e1f5ac04bb3fc70aebe37944e790
68169704778468b7b58450c970d69750c067e5e5b911eda33f263326673d52d4d466@192.168.1.1
03:51553",
    id: "ea4297467298c94a351ad249ca2bd34cb002969f1065e673f72e261807f84e4a",
    name: "Geth/v1.9.15-stable/darwin-amd64/go1.14.3",
    network: {
      inbound: true,
      localAddress: "192.168.1.107:30303",
      remoteAddress: "192.168.1.103:51553",
      static: false,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 2237952,
        head: "0xf74ac234518a2bc593e2694406a972bbe959fb7e4ef26a480774cf2dd9cd10b
0",
        version: 65
      }
    }
}]
```


Figure 9: blockchain network node peering

4.3.1 Identity Management and Access control (authentication and authorization)

The objective here is to demonstrate the usability of blockchain in implementation of various access control methods to meet the security needs of the internet of things as specified in the threat model result of figure: This is applicable for protecting the Internet of Things (IoT) devices from unauthorized or malicious access. This is important as Internet of things is characterized by memory-constrained devices, lightweight communication protocol, dynamic behavior, heterogeneity, enormous scale,

intelligence, and low latency connectivity and hence demand a different security approach than the traditional ones. Access control for the IoTs, therefore, requires a decentralized lightweight service and management architecture to overcome the limitations present in the client-server architecture and meet the growing scale of IoTs. The limitations of the client-server model are a single point of failure, scalability issues, management, and performance bottlenecks. Secure service and management model based on blockchain technology is adopted in this research study. Access control methods are modeled using an access control matrix. An access control matrix represents a two-dimensional matrix structure where subjects (users) are related to objects (resources) with their corresponding access rights. The result from the access control matrix is translated into a smart contract, which is a code, token, or business logic that run on the blockchain. Evaluation of results is based on requirements of the Internet of Things such as security and privacy, decentralization, manageability, resource efficiency and scalability. Figure 10 and Figure 11 shows the results of the access control implementation based on the proposed model.

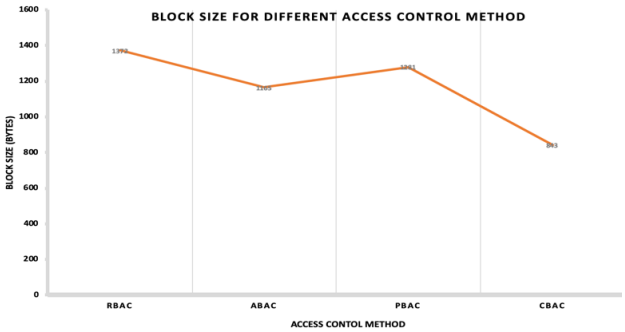


Fig 10. Access control methods

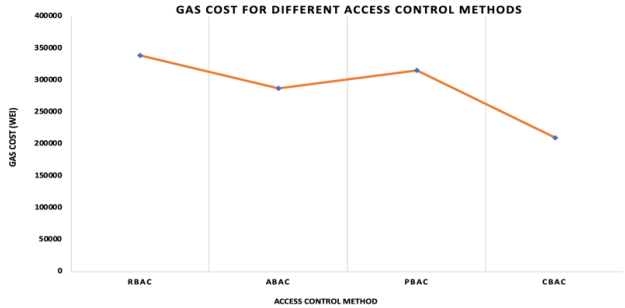


Fig 11. Access control methods

4.3.2 Intrusions and DDoS Prevention

We demonstrated the ability of the network to prevent intrusions by simulating a simple denial of service attack on the network. To simulate this attack, we made the following assumptions:

(i) The intruder has not gathered enough information about the network such as network id and authentication information.

(ii) The intruder cannot validate network transaction ie a miner.

These assumptions are just enough to make an adversary gain control of the network and overwhelm it.

The network was configured with layered security that makes a DDoS attack on the network very difficult

Layer 1:

The network is configured with a network id which makes joining of the network impossible without the knowledge of the id.

Layer 2:

The nodes of the network are not dynamic but static. Dynamic nodes configuration allows a new node to join the network once it has the network id information, but static nodes have a preconfigured nodes information, and those nodes are known to the network. Node peers are formed from the list of these nodes and hence reject any new nodes from joining the network

Layer 3:

Every transaction is authenticated with credentials which must be valid and correct for a transaction to be successful.

Layer 4:

Access to resources as well as read, write access are controlled by the access control layer implemented using smart contracts.

4.3.3 Intrusion Detection

The assumption here is that the adversary was able to bypass all the layered security of the network to gain access to the network to compromise it. By monitoring the transaction logs with the logging feature of the blockchain, minimal information like the block number of the transaction can be traced back to the node issuing the transaction which can in turn be traced back to the node information

5 Discussion of Results

Figure 7 shows the initial result of the threat model. The results have 7 main columns. The category column is in line with our thread modeling method STRIDE. The second column is interaction which is the same for across all the categories of attack. The

third column is a description of the categories in column 1.

The fourth column are possible mitigation that is countermeasures to prevent the attack. The Fifth column is the phase which is the early stage; design and implementation of the system. The frequency column shows the number of components of the system that could be impacted by such attack and hence points to the severity level of the attack

Figure 9 and Figure 10 shows the results of the evaluation of the access control methods implemented. The various access control methods is implemented with smart contracts in form of classes with its associated methods. These methods form the application binary interface in the Ethereum virtual machine while compile with its associated bytecode. The complexity of the access control method is proportional to the computational power of compiling its code into binaries and functions as well as the cost of its function invocation (transactions). We measure these two parameters in terms of block size and gas costs which was in turn observed as showing great correspondence.

6 Conclusion

The paper explores internet of things security issues. A brief study of the IoT components and its application areas was carried out with the aim of putting into perspective assets and the type of environments these assets exist as IoT systems. This was necessary because adversaries carry out attack to compromise systems and damage these assets. Then we propose an architectural model based on blockchain for designing such IoT systems with system-wide security in mind. Then we analyze our approach which entailed threat modelling and implementing a sample of our model using Ethereum blockchain. Discussion on the security of the model was carried out as well as the results

References:

[1] L. Atzori, A. Iera and G. Morabito, "The Internet of things: A survey," *Computer Networks*, vol. 54, no. 15, 2010, pp. 2787-2805,

[2] "Internet of Things Global Standards Initiative-ITU," https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[3] C. Sharma and N. K. Gondhi, "Communication Protocol Stack for Constrained IoT Systems," *Proceedings of the 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2018, pp. 1-6.

[4] I. Ali, S. Sabir and Z. Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," *International Journal of Computer Science and Information Security*, vol. 14, no. 8, August 2016, pp. 456-466.

[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019

[6] K. G. Eze, C. M. Akujuobi, M. N. Sadiku, M. Chouikha, and S. Alam, "Internet of things and blockchain integration: use cases and implementation challenges," *Proceedings of the International Conference on Business Information Systems*, Springer, Cham, June 2019, pp. 287-29

[7] Y. Yin, Y. Zeng, X. Chen, Y. Fan, "The internet of things in healthcare: An overview," *Journal of Industrial Information Integration*, Volume 1, 2016, Pages 3-13,],

[8] A. Burg, A. Chattopadhyay and K. Lam, "Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things," *Proceedings of the IEEE*, vol. 106, No. 1, January 2018, pp. 34-60

[9] P. O'Donovan et al., "An industrial big data pipeline for data-driven analytics maintenance applications in large-scale smart manufacturing facilities," *Journal of Big Data*, 2015, pp 1-26

[10] C Wang et al, "A Dependable Time Series Analytic Framework for Cyber-Physical System

of IoT-based Smart Grid," ACM Transactions on Cyber-Physical Systems, vol. 3, No. 1, August 2018, pp. 7:2 -7:18

[11] N. F. Junior et al, "IoT6Sec: reliability model for Internet of Things security focused on anomalous measurements identification with energy analysis," Wireless Networks, vol. 25 no. 4, May 2019, pp. 1533-1556

[12] A. Kim, J. Oh, J. Ryu and K. Lee, "A Review of Insider Threat Detection Approaches with IoT Perspective," in *IEEE Access*, vol. 8, pp. 78847-78867, 2020

[13] M. Nawir, A. Amir, N. Yaakob and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, 2016, pp. 321-326

[14] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials (Volume: 21 , Issue: 3 , thirdquarter 2019),* vol. 21, no. 3, pp. 2702-2733, 11 April 2019.

[15] X. Li et al., "An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things," Wireless mobile technologies for the Internet of Things, vol 2016, 2015 pp. 1- 11.

[16] P. Anand et al., "IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges," *IEEE Access*, 2020, pp. 1-29

[17] D. Cornell," Threat Modeling for IoT Systems," https://2018.appsec.eu/presos/CISOThreatModelingforIOTDan-Cornell AppSecEU2018.pdf

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0
https://creativecommons.org/licenses/by/4.0/deed.en_US