PREVENTING PRIVACY ATTACKS ON IOT DEVICES

By

Justin Kizhakkayil Joshuva

Li Yang

Associate Professor of Computer Science

(Chair)

Dalei Wu

Associate Professor of Computer Science

(Committee Member)

Lani Gao
Associate Professor of Mathematics
(Committee Member)

Hong Qin
Associate Professor of Computer Science
(Committee Member)

PREVENTING PRIVACY ATTACKS ON IOT DEVICES

By

Justin Kizhakkayil Joshuva

A Thesis submitted to the Faculty of the University of Tennessee at Chattanooga in partial Fulfillment of the requirements of the Degree of Doctor of Philosophy in Computational Science

The University of Tennessee at Chattanooga
Chattanooga, Tennessee

May 2022

ABSTRACT

Today, people use many connected devices to make people’s lives easier in a connected environment. Devices like fitness trackers, smartwatches, smart home appliances, and other devices make people’s lives easier. People can use their smartphones to control the thermostat, television, vacuum cleaner, and other connected devices. While IoT devices make their lives easier, they also concern security threats like privacy. Organizations like the U.S. DoD forbid having fitness trackers on some of their buildings, while other organizations discourage patrons from using them in their spaces.

The question of how to use IoT devices and simultaneously safeguard users' privacy is a big challenge. Let’s look at a couple of different ways to secure IoT devices' privacy. Since IoT devices are very vast and very different, no universal scheme exists to prevent privacy attacks; thus, a variety of techniques need to be used. Some blockchain applications and transformations will be used to protect privacy in IoT devices.

These algorithms that transform data or use blockchain to manage the data or the flow can prevent privacy attacks. Using such algorithms protects the data of IoT/Smart devices and secures them so that people do not have to worry about not being safe while these devices are being used.

DEDICATION

To my family: Thank you for your support, without it I would not have made it.

To my friends: Thank you for your encouragement and support.

ACKNOWLEDGEMENTS

I have received support from many people throughout my years as a Doctoral student at the University of Tennessee at Chattanooga. First, I sincerely thank my advisor, Professor Li Yang, for her continuous support. You have supported me in my academic journey, especially with the doctoral program.

I would also like to express my gratitude to the rest of the committee. I also want to thank all my friends in the Computer Science Department. I also would like to thank the faculty and staff of the Computer Science Department. I want to thank all of my colleagues at work for their support and help. To friends at Ruatech, thank you for providing the data and helping with the experimentation.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

$=$, Equal to

$\neq$, not equal to

$\leq$, Less than or equal to

$\geq$, Greater than or equal to

α, alpha

β, Beta

δ, delta

ϵ, Epsilon

N, Natural Numbers

R, Real numbers

G, Groups

Z, Integer

$\forall$, For all

$\in$, element of

$\left||x, y|\right|_1$, norm

exp, exponent

$P(x|b)$, conditional probability of the event x given that event b has already occurred

X, Random variable X

x, value of x

Y, Random variable Y

y, value of y

b, scale value of Laplace distribution

f, function

$\sqrt{\ }$, square root

log, logarithm

$\prod$, single Product

$\sum$, single summation

P, Plaintext

C_t, Ciphertext

k_s, Symmetric

C_{tk}, Ciphertext key

d, digital signature

h_q, Hash value of original data

h_n, Hash value of received data

sk_{spb} Public key of sender for digital signature

sk_{spr}, private key of sender for digital signature

rk_{rpb}, Public key of receiver for digital signature

rk_{rpr}, private key of receiver for digital signature

sk_{pb}, Public key of sender for Cryptography

sk_{pr}, private key of sender for Cryptography

rk_{pb}, Public key of receiver for Cryptography

rk_{pr}, private key of receiver for Cryptography

LIST OF ABBREVIATIONS

AA - Attribute Authority

ABE - Attribute-based Encryption

CA Server - Certificate Authority Server

CSPENG - Cryptographically-Secure Pseudorandom Number Generator

DDoS - Distributed Denial of Service

IoT - Internet of Things

NSA - National Security Agency

DHKEY - Diffie-Hellman Key Exchange

DoD - Department of Defense

ARX - Add-Rotate-XOR

CHAPTER I

BACKGROUND

The evolution of humans over the years gave the world new technologies that make lives easier, from metal tools to wheels to industrial revolutions to electrical advancement to the invention of computing devices. Each generation invents or discovers new devices to make communications, work, entertainment, and accessing information more manageable. The computing devices like desktops, laptops, cellphones, and tablets make people’s lives easier to access information and entertainment. One such device is the Internet of Things (IoT).

IoT devices exist in all areas of people’s lives. Healthcare, hospitality, information gathering, security, data communications, etc. In healthcare, IoT devices provide doctors and other medical representatives the information about 'patient's health and other essential knowledge required to treat the patients. Insecurity and information gathering IoT devices can act as sensors to get information from various devices. Smart meters, temperature sensors, pressure sensors, gas, and air quality sensors, and proximity sensors convey information about the environment. One of the most common examples of such devices is smartwatches and fitness trackers. Smartwatches like Samsung watches or Apple Watches combine smart sensors like gyroscope, accelerometer, heart-rate, and many others to give the user better information about the environment and health.

There are various benefits to using an IoT system. The benefits of IoT can be categorized into multiple factors like communication, automation and control, information, monitoring, time, money, and better quality of life. IoT encourages communication between various devices, known as Machine-to-Machine (M2M) communication. Using M2M, the physical devices can stay connected. Since IoT is designed to function as fully automated, this can lead to better outputs. IoT leads to a better quality of life by saving time money and becoming more efficient in getting information and monitoring data.

IoT devices make people's lives easier, but they also come with a considerable security risk. All these devices get people's personal information or other sensitive information. Privacy is critical when these devices are used. Suppose bad actors can gain access to one's private information stored or transmitted through these devices. In that case, they will be able to steal one's identity and/or use that information to hurt user or their family. Therefore, protecting these devices from unauthorized access is extremely important.

This research aims to (i) show how valuable IoT data are to malicious attackers and how they can use it to destroy people's lives. (ii) Find how the privacy of the data can be maintained using various algorithms or mathematical techniques. (iii) How effective are blockchain for preventing privacy attacks on IoT devices.

The current architecture of IoT is represented by four (4) main areas: things, gateways, Network infrastructure, and Cloud infrastructure. Things are uniquely identifiable modes, primarily made of sensors that communicate without interaction from humans using various connectivity protocols. Gateways are the middleman between things and the cloud to provide connectivity, security, and manageability. The Network Infrastructure is a device that controls and secures the data flow. Examples of these devices are routers, gateways, repeaters, etc. The cloud infrastructure consists of pools of virtual servers and storage networked together with computing and analytical capabilities.

Figure 1 shows how these four (4)   areas are connected to each other.

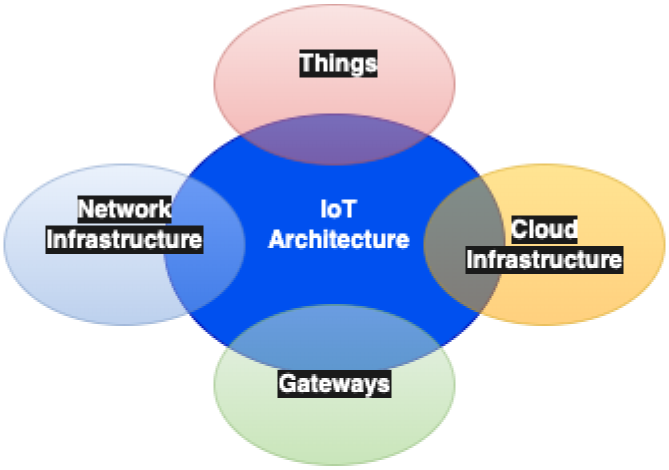


Figure 1 Current Architecture

The security of IoT systems deals with multi factors like hardware, operating systems, software, networking, and data. Privacy attacks can occur anywhere in these factors [31]. Figure 2 shows the intersection of these factors.

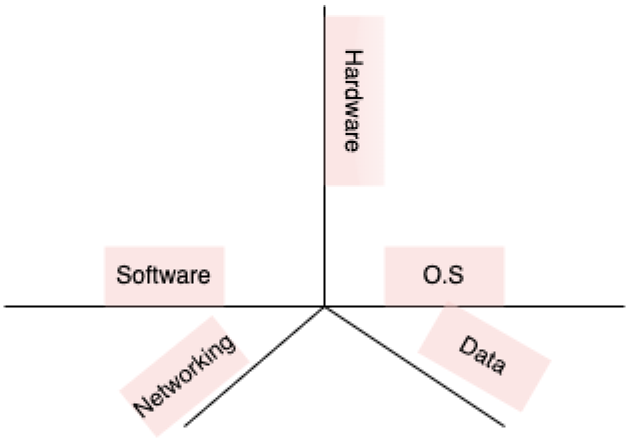


Figure 2 Aspects of IoT Security

If bad actors have physical access to the IoT devices, then that device is compromised; thus, ' 'it's critical to have hardware security.

Privacy attacks come in many different directions in an IoT device. These attacks come from hardware, OS, and network. One privacy attack happened on October 21, 2016; a huge DDoS attack was deployed against Dyn DNS servers and shut down many web services, including Twitter [40]. Hackers also exploited the default passwords and usernames installed on compromised IoT devices by the Mirai botnet [41]. Phillips Hue Lightbulbs were attacked through its Zigbee link protocol, and Belkin IoT devices were compromised by SQL devices [43-44].

If one look at some of the devices, one can see how much data is transferred and how much personal data is in the transmitted data. Smart meters record the current electric usage in a household; they can also distinguish between the usage of different appliances. If a bad actor could get into the smart meter data, they can use it to determine when the house is occupied. If they sell the data, that data can aid in theft or other malicious attacks. To prevent this, one can mask the data or transform it so that data is not distinguishable. Some mathematical models can be used to convert the data.

Differential Mechanism for Privacy

Differential Mechanism for privacy is a mechanism for quantifying privacy using a mathematical model. Differential privacy is said to be ϵ-differentially private. The definition of ϵ-differentially is

let ϵ be a positive real number and A be a random algorithm that takes a dataset as the input. Let $\mathcal{A}$ be the image of A. The algorithm provides

ϵ-differential privacy if for all datasets D_1, D_2 and datasets D_1, D_2 that differ by one element and all the subsets S of $\mathcal{A}$.

$$\Pr\,[\{A\}(D_1)\ \in \{S\}]\ \leq\ \exp\,(\epsilon) \cdot\ \Pr\,[A(D_2) \in S$$

Laplace Mechanism

The Laplace mechanism is a technique to add noise to the data to achieve differential privacy. The Laplace mechanism uses the Laplace distribution to add noise. The Laplace distribution has a mean of 0 ($\mu =\ 0$) and has a scale value of b.The Laplace distribution is a symmetrical version of the exponential distribution, and it adds the noise from a symmetric continuous distribution. The Laplace distribution is

$$Lap(x|b) = \frac{1}{2b} exp\left(-\frac{|x|}{b}\right)$$

The Laplace mechanism states that for any given function $f: N^{|X|} \rightarrow R^k$ the Laplace mechanism is defined as: $\mathrm{M\_L}(\mathrm{x}, \mathrm{f}(\epsilon = \mathrm{f}(\mathrm{x}) + (\mathrm{Y\_1}, \dots, \mathrm{Y\_k}))$, where Y_i are the random variables from the Laplace distribution defined as

$Lap\left(\frac{\Delta f}{\epsilon}\right)$.

The Laplace mechanism adds noise to the data if and only if the data is accessible. It will not work in a decentralized system. In order to secure privacy in data, blockchain technology can be used. Since the principle of blockchain is to work on a decentralized ledger than a centralized server, the blockchain is perfect. One of the best ways to use blockchain to combat the lack of privacy is to introduce a hierarchy model which can also increase network stability and optimize resource consumption.

Lagrange Interpolation

This new hierarchy model uses the math of bilinearity pairing, secret sharing, and Lagrange Interpolation. Lagrange Interpolation is a polynomial interpolation that gives a certain value according to the characteristics of the polynomial. The general form for the Lagrange interpolation is:

$$P(x) = \sum_{i=1}^{n} P_i(X) Y_i$$

The advantages of using Lagrange Interpolation are this can be used when the divisions are not spaced equally. One can find the value of the independent variable when the corresponding value is given. The disadvantages of this technique are it can be slow for higher-order polynomials, and if the order changes, then new calculations are needed.

Bilinear Pairing

Bilinearity pairing is a technique used in cryptography that can be used to pair two groups to form a map. The generalized form of bilinearity pairing is

$$f: G \times G \rightarrow G_T$$

where G, G_T are both cyclic of prime order r.

Privacy is one of the most important rights of all civilized beings. IoT devices make people’s lives much easier to interact with the world. While that interaction is significant, 'it's also essential to keep the data safe while interacting with the world. If the data is not safeguarded when the IoT devices are used, personal identifiable information, personal health information, or financial information can be leaked to bad actors and used to maliciously attack users. The algorithms and techniques in this paper help to prevent attacks on privacy.

Attacks on Blockchain

There are various threats to traditional IoT security and also against the blockchain. The threats against blockchain include 51%, Sybil attacks, Eclipse attacks, Vulnerable signatures, Double spending, and others.

51% attack is also known as majority attacks. The 51% attack occurs when an individual gains control over 50% of the blockchain's hashing power. Sybil attack is arranged by having multiple miners on the same node. Eclipse attacks is a version of the Sybil attack where the attacker uses a botnet and uses it to overwrites the user's IP address.

Vulnerable signature attacks are where cryptographic technology uses a weak signature like the ECDSA algorithm. A double-spending attack is an attack that exploits the transaction verification [48-49]. While there are many attacks against blockchain technology, many safeguards prevent it from getting attacked.

Questions

1. The questions answered in this research are about how to safeguard privacy while using IoT devices.

2. Is blockchain capable of securing privacy for IoT devices?

Limitations

The limitations of this research were: access to data like smart devices, data, and blockchain data to do analysis. To overcome the limitations, a sample data is created on the blockchain and used for testing.

Overview

This research is divided into Six (6) chapters. Chapter 1 introduces the IoT devices and some keywords and function that helps to solve the questions asked in the research. Chapter 2 consists of related works, which take some research work done by others relevant to the research and compare this research with theirs. Chapter 3 shows one way to protect IoT devices using an algorithm's data transformation. Chapters 4 and 5 show how people can use blockchain technology to prevent privacy attacks on IoT devices. Chapter 4 uses a blockchain method for managing devices and thus preserving privacy, and chapter 5 uses a blockchain technique that preserves privacy in IoT devices. Chapter 6 concludes the research, answering the questions raised in the introduction and showing the future research path.

CHAPTER II

RELATED WORKS

Wearable IoT devices gained popularity over the last few years. It also led to a massive scale of personal data since wearable IoT devices gained popularity and a rise in personal data to preserve the privacy of the data. Liu and Li chose a k-anonymity method to share the data. K-anonymity is a general conception to share data in a privacy-preserving way. The dataset could be divided into several equivalent sets according to K-anonymity, and each set contains at least K and less than 2K records. To calculate the two 'records' similarity, the distance between the two records is calculated and then clustered or grouped together. This type of privacy-preserving algorithm is suitable against attacks like the link attack on privacy [1].

Blockchain-based credibility verification method for IoT entities is a research article that discusses the challenges in security and privacy and how to overcome those challenges. In this article, blockchain structure is used to verify IoT entities. The traditional security and privacy policies based on asymmetric encryption are challenging to implement in IoT due to needing a centralized management system, and they tend to be expensive in terms of energy consumption. In this credibility verification structure framework, the structure is made of several blockchains with different layers, and the blockchain node in the upper layer manages a blockchain of the lower level. The register data in the lower level is transmitted to the upper blockchain sequentially and recorded in each blockchain in the path. The verification process records the addition or deletion of entities, and also checks the credibility verification process of the accessing entity. Then, credibility verification of data is achieved [28].

In the traditional sense of IoT security, CA server authentication is used. In this paper,

they use public-key cryptography to authenticate IoT entities, and they introduce a peer-to-peer authentication methodology. The blockchain uses smart contracts to interact with the system and uses CSPENG-based key generation. The consensus algorithm in the blockchain is Practical Byzantine Fault Tolerance, which helps discover abnormal behavior, and data synchronization of data in the ledger. The idea of blockchain for authentication gives better security like preventing malicious actors from tampering with data, preventing backdoors in the firmware, and resisting DDos Attacks [2].

While exciting, IoT technologies are littered with challenges for achieving security and privacy. The characteristics of IoT are low processing power, distributed nature, and the lack of standardization. Using blockchain fundamentals, these challenges can be overcome. A proposed hierarchical structure to optimize resources and increase network scalability [33].

The works of [37] exploits blockchain technology to avoid a central server. Since the blockchain uses decentralized servers, the sensor data can be stored in those decentralized servers. Similar to how individuals manage cryptocurrencies, the blockchain supports the devices and users to maintain a distributed database that contains sensor data. The attribute-based encryption (ABE) technique addresses the privacy and confidentiality of the data shared in blockchain-based IoT ecosystems. This technique is known for the simplicity where a single encryption provides both the confidentiality and access control, and it can be used for sharing data in decentralized networks like blockchain systems [32].

CHAPTER III

SMART METER PRIVACY

In a connected environment today, peopleuse many connected devices to make people's lives easier. Devices like fitness trackers, smartwatches, and smart meters make people's lives easier, but they also give concern to security threats like privacy. All the connected devices ease people's lives, but they keep track of personal data like movements, locations, and energy uses. Smart meters give the ability to accurately and remotely measure the watts usage of a house by measuring the usage of appliances. There are many advantages to the smart meter, but the disadvantages are also very concerning. If a malicious user were able to access the data, they could detect the occupancy of the household based on the peak times of the utility usage. Since the smart meter data can distinguish between different appliances and their usage on a given day, this data contains useful information such as peak times, which can lead to detecting the occupancy of a household. Privacy among smart devices is a high-security threat. If a malicious user were able to detect the occupancy from the data, they would be able to do a more malicious activity in the household.

There are various researches done in the area of smart meters and privacy. Most will require extra hardwire or another energy source to safeguard privacy [45-47]. While the above approaches work, they also include either an additional vector of attack surfaces or extra computation to safeguard the data, neither of which is ideal.

A privacy mechanism is an algorithm that takes an input and produces an output of a string. One of the most common privacy mechanisms is the differential privacy mechanism. Differential mechanism is defined as a randomized algorithm M with domain

$N^{|X|}$ is (ϵ, δ) -differentially private if for all $S \subset \text{Range}(M) \forall x, y \in N^{|x|}$ such that $\left\| x - y \right\|_1 \leq 1$:

$$Pr(M(x) \in S \ \leq exp(\epsilon)\ Pr(M(y) \in S) \ + \ \delta$$

One of the most common types of differential privacy algorithm is Laplace Mechanism. The Laplace Mechanism is based on the Laplace distribution. The Laplace distribution is a distribution with the probability density function:

$$Lap(x|b) = \frac{1}{2b} exp\left(-\frac{|x|}{b}\right)$$

where b is the scale with a mean of 0.

The Laplace mechanism states that for any given function $f: N^{|X|} \rightarrow R^k$ the Laplace mechanism is defined as: $M\_L(x, f(\epsilon = f(x) + (Y\_1, \ldots, Y\_k))$, where Y_i are the random variables from the Laplace distribution defined as $Lap\left(\frac{\Delta f}{\epsilon}\right)$.

I propose an algorithm called exponential additive that works with the exponential distribution and the additive method to guarantee the privacy of data. The algorithm (Algorithm 1) is defined as (ϵ, δ)-differentially private with probability of at least $1 - \beta$. The algorithm returns a data y such that: $\{f \ \in Q\}_{max} |f(x) - f(y) \ \leq \alpha$, where

$$a \leq \frac{16\sqrt{log(|x|)log\frac{1}{\delta}}\,log\left(\frac{2nlog|X|}{\beta}\right)}{\sqrt{n}\epsilon}$$

The dataset was gained from the University of Massachusetts Trace Repository. This repository contains smart meter data between 2014 and 2016 with usage for individual outlets and appliances. The figures below show the voltage used for the year 2014 with every 30 min usage. The first figure (3) shows the overall usage, while the second figure (4) shows the usage for lights in various rooms and the appliances.

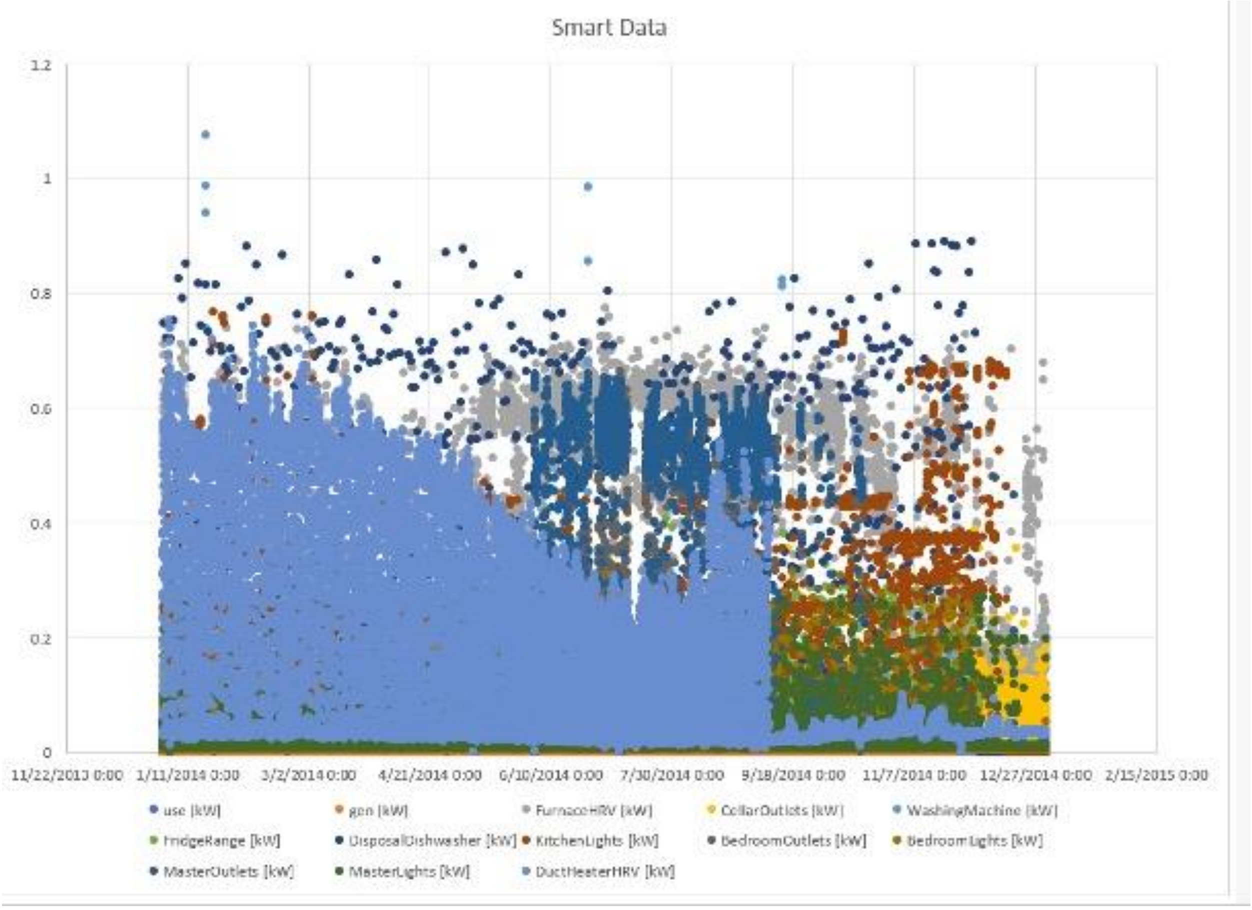


Figure 3 Overall Usage

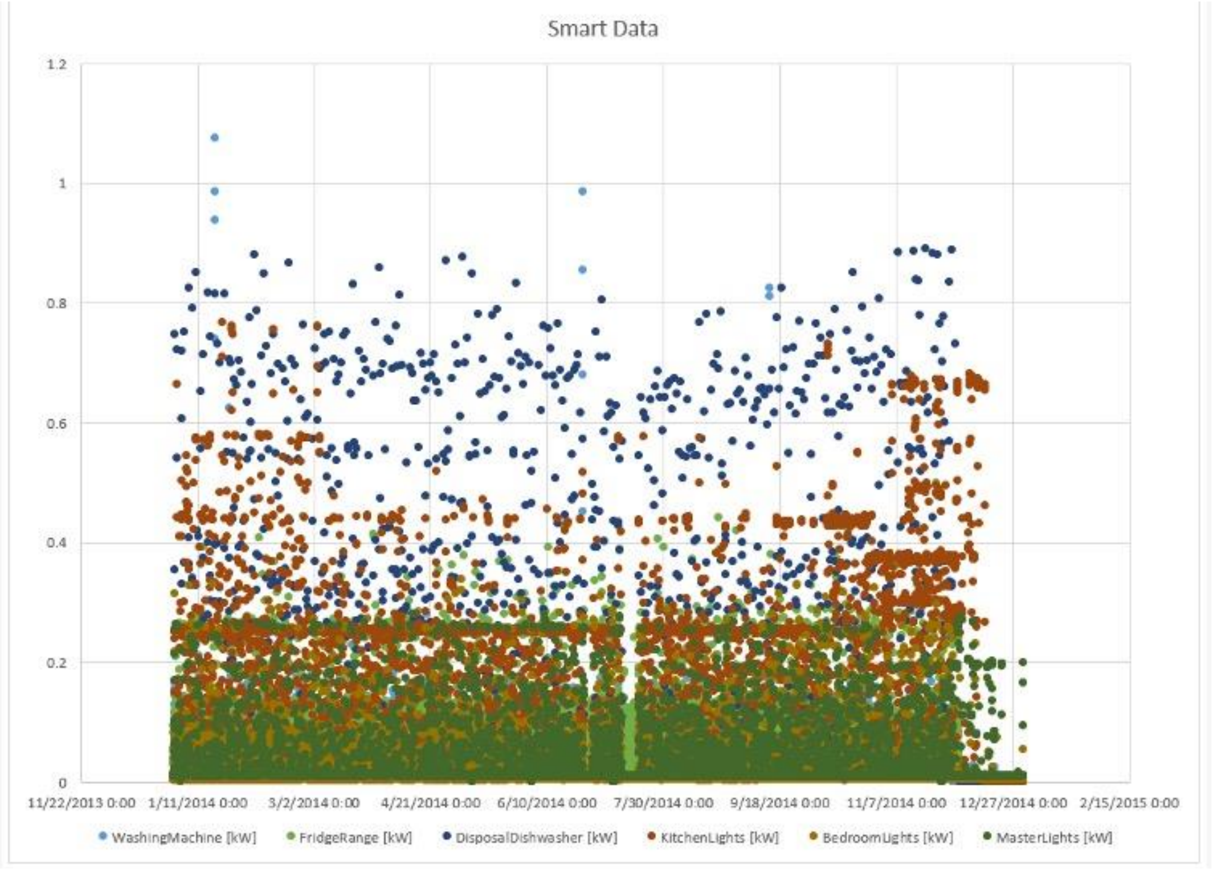


Figure 4 Appliance + Lights Usage

The implementation of this method is taking all data points and transforming the data with the aid of the algorithm 1. The δ, ϵ are small values and β is value from the results are compared methods will prevent occupancy detection by either adding noise to the data or masking the peak points of the data (algorithm 3). When the additive noise method is applied to the dataset, it is transformed to the figures (5 & 6) below.

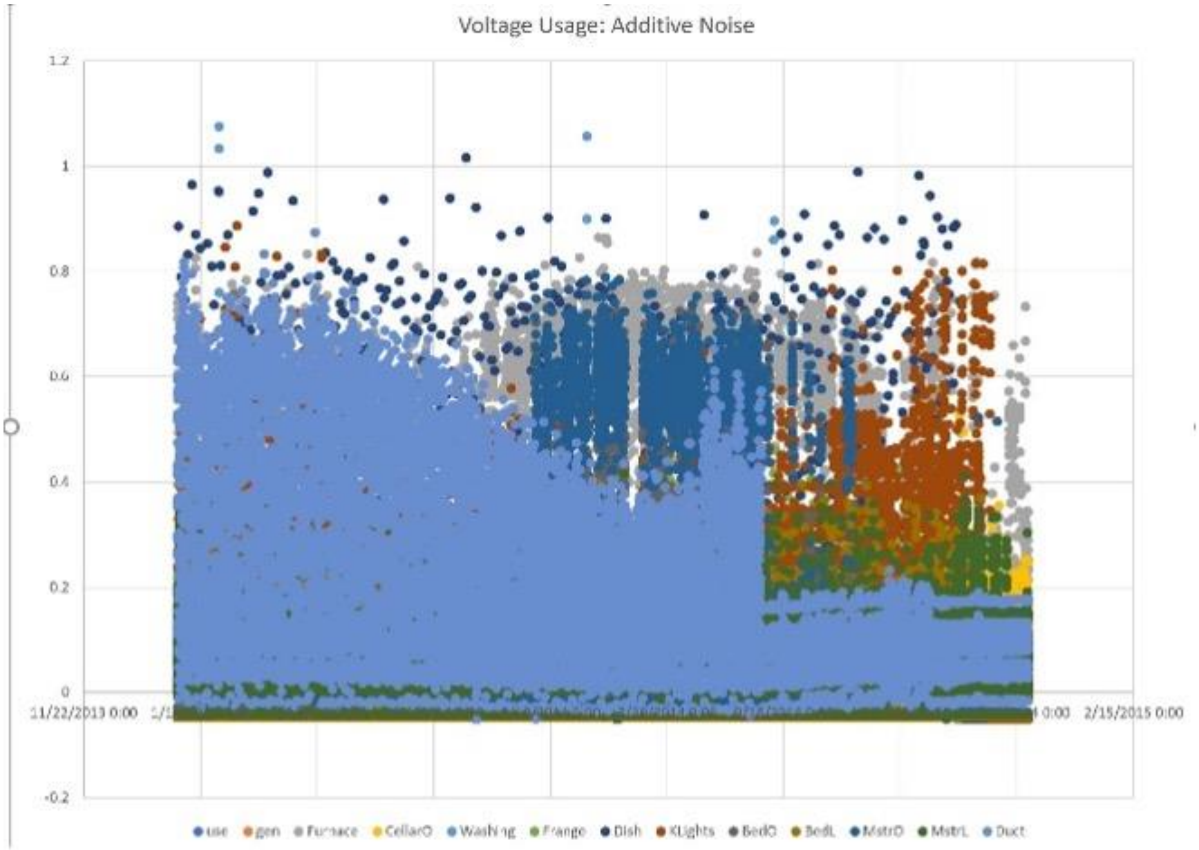


Figure 5 Overall Usage: Additive Noise

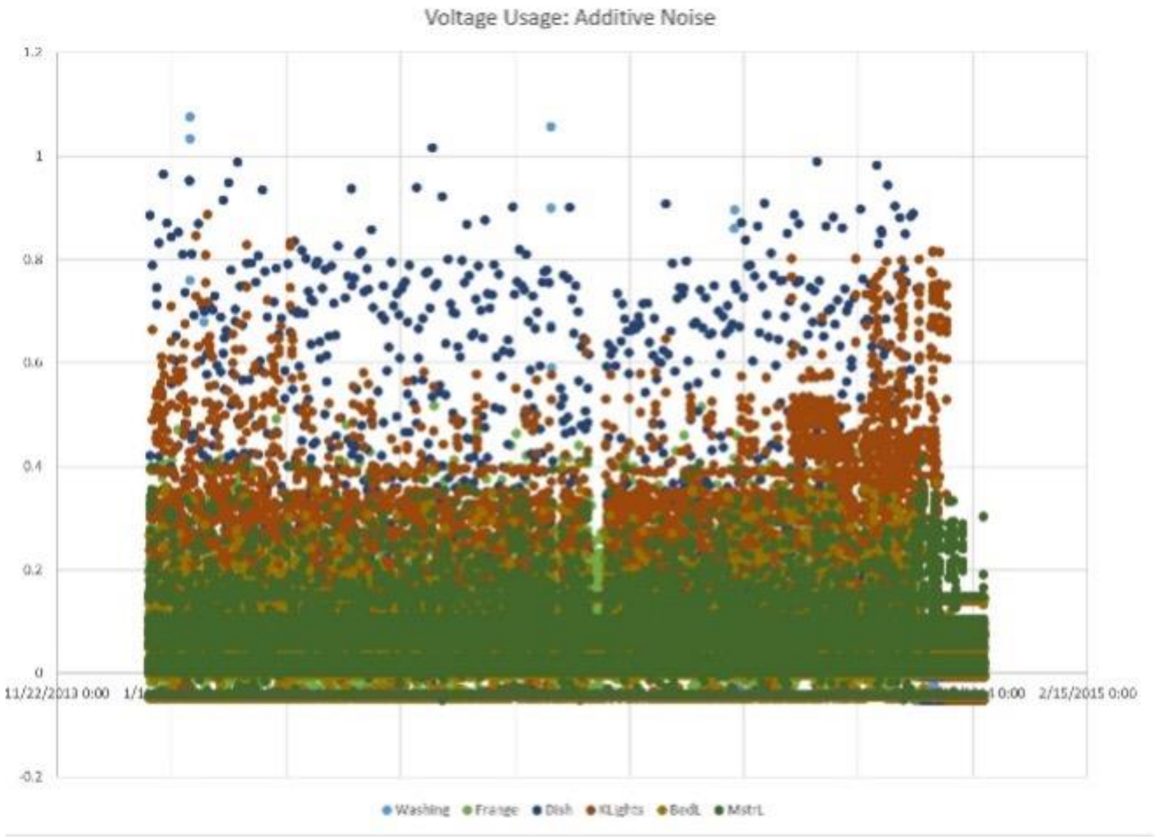


Figure 6 Usage of Lights+ Appliances: Additive Noise

Algorithm 1 Additive Algorithm

```
function CALCULATE
    mean, standard deviation
end function
Add noise with mean and standard deviation
```

Algorithm 2 Laplace Algorithm

```
Input: b
Transform the data using $Lap(x|b) = \frac{1}{2b} exp\left(-\frac{|x|}{b}\right)$
```

```
Algorithm 3 exponential additive Algorithm
  Input: $\delta, \epsilon, \beta$
  Transform the data using $a \leq \frac{16\sqrt{log(|x|)log\frac{1}{\delta}}log(\frac{2nlog|X|}{\beta})}{\sqrt{n\epsilon}}$
```

It is not different than the original data. When the Laplace method is applied (Algorithm 2), the data is transformed into the figure (7 & 8) below.

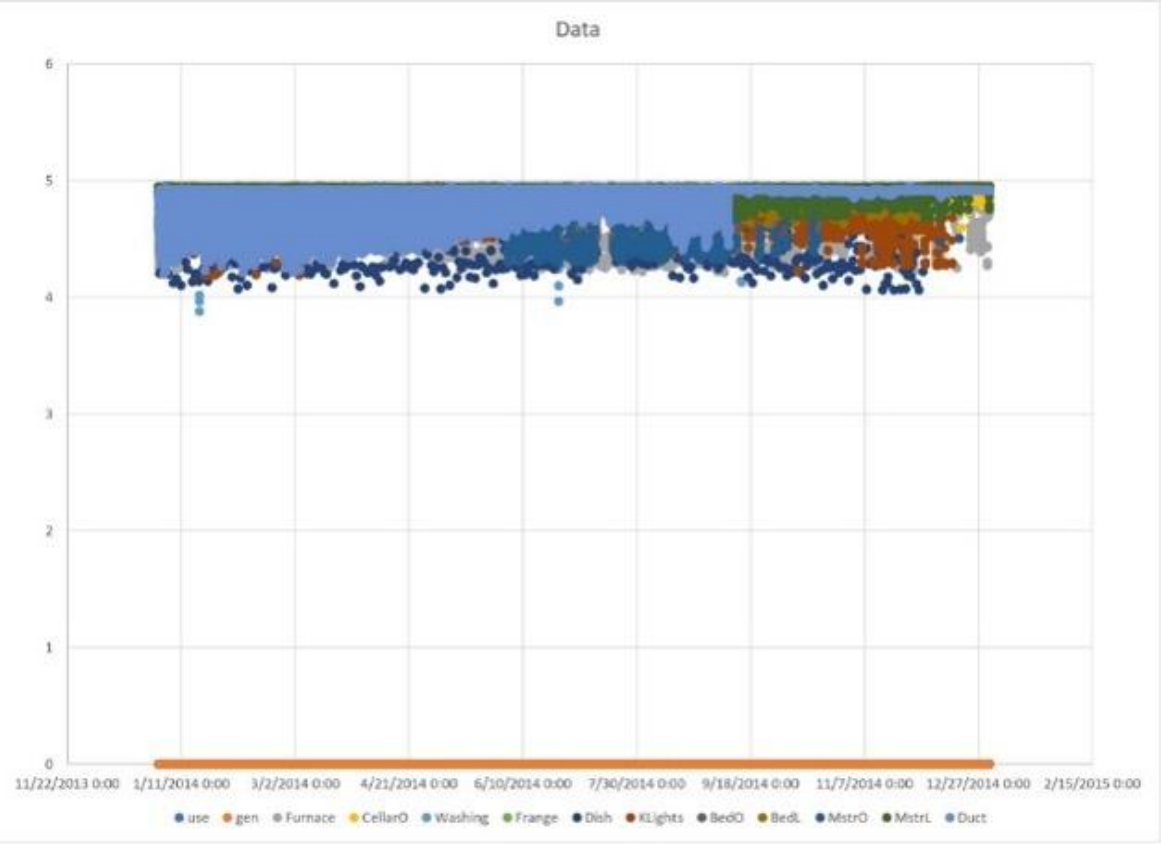


Figure 7 Overall Usage: Laplace Transform

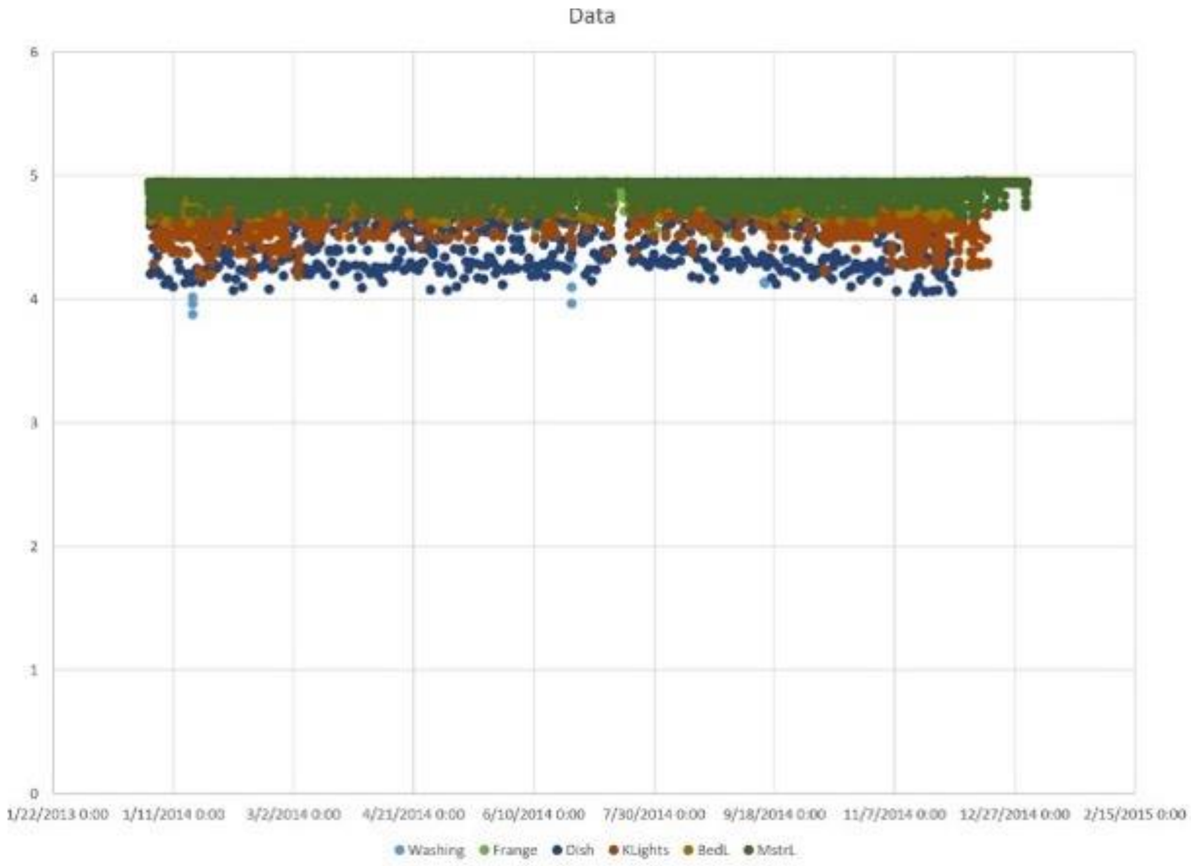


Figure 8 Usage of Lights + App: Laplace Mechanism

The Laplace mechanism masked the data better than the additive noise method. When the data is transformed by the algorithm, the data becomes The Laplace mechanism masks the data better than the additive noise method and the exponential additive algorithm.

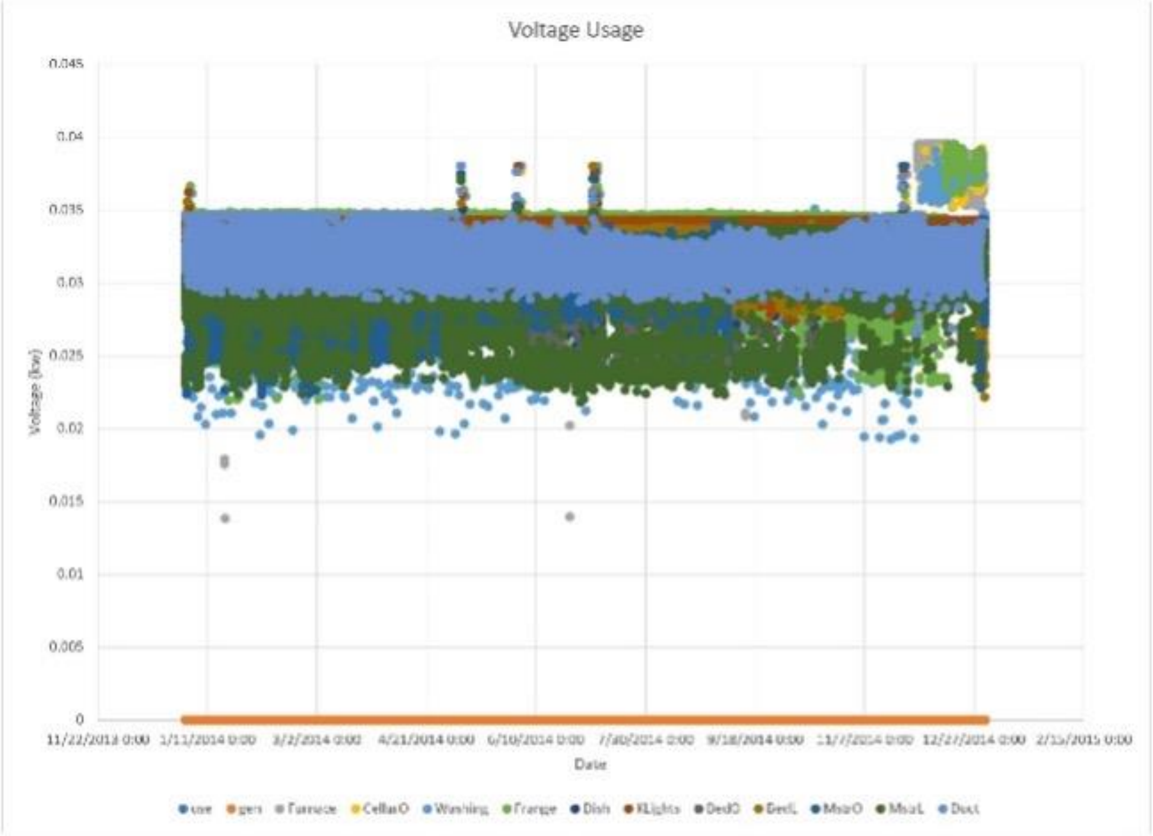


Figure 9 Overall Usage: Algorithm

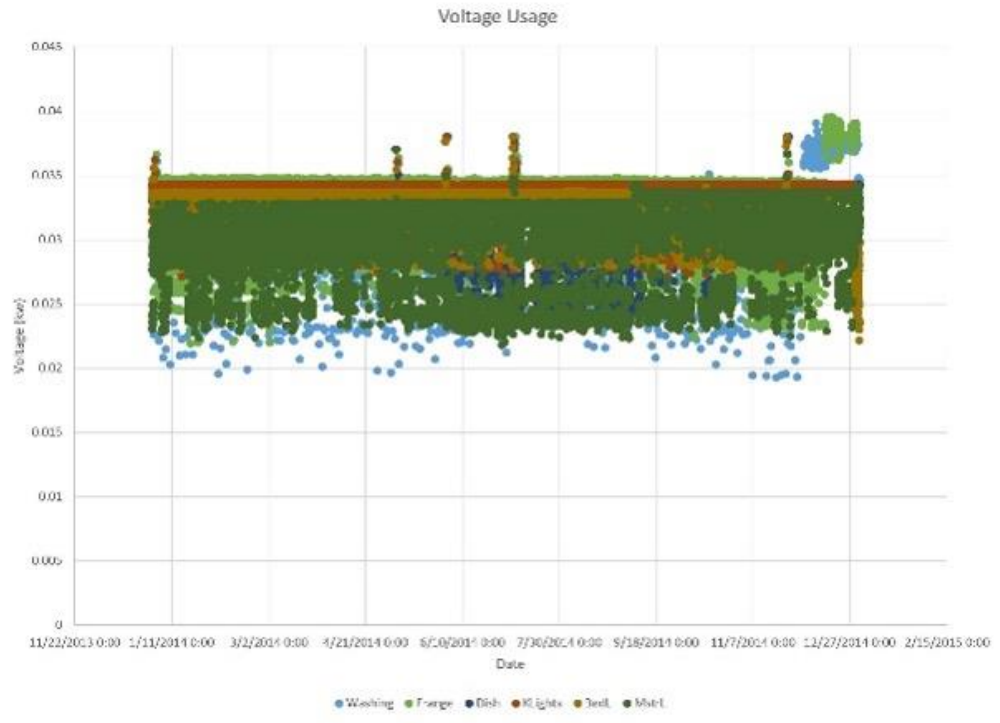


Figure 10 Usage of Lights + App: Algorithm

CHAPTER IV

Blockchain-based Management and Authentication

Since there are many different IoT devices, it can be hard to manage them all. If these devices can be managed and authenticated using a secure system, privacy attacks can be reduced.

Using blockchain to authenticate and manage devices has some advantages. Since all transactions are visible to the public, it will be easier to identify if some changes are made to the blocks. Using blockchain for IoT devices to address security and privacy is attractive for several reasons. The lack of central control ensures the scalability and sturdiness by using all of the resources of the participating nodes and thus eliminating the many to one traffic flows, which will decrease delay and avoid a single point of failure. The blockchain also gives anonymity. The blockchain uses a secure network which is suitable for many IoT devices.

Ethereum is a blockchain-based distributed computing platform. Ethereum combines the computing system with blockchain. The Ethereum can be described as a transaction-based state machine. A state machine is defined as something capable of getting inputs and changing to a new state based on the inputs. When the execution of the transaction occurs, the machine changes to a new state. A smart contract is a program that is written in Ethereum. The smart contract contains the protocols that allow the contract to be executed based on the predefined conditions. Since the blockchain network is formed around the principle of consensus, fraudulent activity cannot occur without forming a new fork.

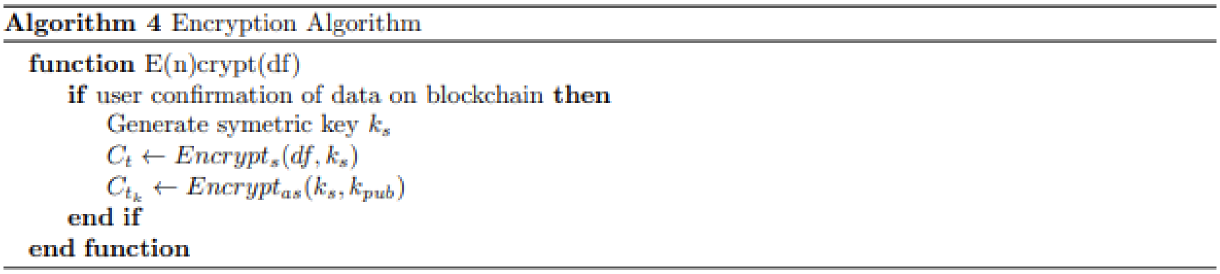
In order to secure the data, two types of encryption techniques are used. The symmetric key algorithm, also known as the private key encryption, uses the same key for both encryption and decryption. The asymmetric algorithm, also known as public-key encryption, uses different keys for encryption and decryption. SPECK is a lightweight algorithm developed by National Security Agency (NSA) [31]. SPECK uses ARX algorithms, which uses the simple operations such as Addition, Rotation, and XOR. In SPECK, each block size is divided into two parts, the left, and the right. The SPECK Round function uses three (3) basic functions on the n-bit word in each round. The operations are bitwise XOR, addition modulo 2^{n} and the left/right circular shift by r_1 and r_2 bits. The left n-bit word is denoted by $X_{r-1,L}$ and the right n-bit word is denoted by $X_{r-1,R}$ to the rrth round and n-bit round key. The rrth round is denoted by $k_r, X_{r,L}$ and $X_{r,R}$.The computation of the output words from the round r is

$$X_{r,L} = \Big(\big(X_{r-1,L} \gg r_1\big) 2^{n} X_{r-1,R}\Big) \oplus k_r$$

$$X\_\{r, R\} \; = \; (\big(X_{r-1,R} \ll r_2\big) \oplus X_{r,L}$$

The key sizes of the SPECK family vary, and the total number of rounds depends on the key size. The r_1,r_2 are specified as $r_1 = 7, r_2 = 2$ or $r_1 = 8, r_2 = 3$.

Algorithm 4 is used to encrypt the data using the symmetric key k_s and it produce a ciphertext C_t. A double encryption technique is used to encrypt the k_s after encryption. The public key k_{pub} is used to encrypt the symmetric key k_s and the encrypted key is send with the ciphertext C_t.



```
Algorithm 4 Encryption Algorithm
function E(n)crypt(df)
    if user confirmation of data on blockchain then
        Generate symetric key $k_s$
        $C_t \leftarrow Encrypt_s(df, k_s)$
        $C_{t_k} \leftarrow Encrypt_{as}(k_s, k_{pub})$
    end if
end function
```

To authenticate the data, a digital signature is added. A lightweight digital signature is needed because of the limit in resources in IoT devices. Digital Signatures are the primitives of message authentication. Each user has a separate private/public key pair. The keys are denoted as sk_{pr}, sk_{pb} and rk_{pr}, rk_{pb} for sender/receiver private/public key.

The sender's private key is used to sign the data and is also called the signature key. The public key of the sender is used for the verification key. The signer sends the plaintext to the *Hash function* and generates the hash value h_q. The hash value (h_q) of the plaintext and the signature key (sk_{pr}) is sent to the signature algorithm and sent along with the encrypted data. During the verification algorithm, the public key of the signer, the original hash value is extracted and matched the data is verified.

Since there are limitations of the resources of existing IoT devices, a lightweight digital signature like the ring digital signature is used. The ring digital signature allows the signer to sign the data anonymously. The signature is mixed with other groups, and everyone except the signer is unaware of who signed the message. In a ring digital signature, a user who wants to mix the transaction sends a request to the blockchain network. The request will contain sk_{pb}. Once the network receives the request, it will send back a fixed number of public keys $sk_{pb_1}, sk_{pb_2}, \dots, sk_{pb_n}$ which comes from other users. The ring signature allows for signers' anonymity and signature correctness [28-29].

Diffie-Hellman key exchange protocol for exchanging the public/private key. Diffie-Hellman Key Exchange (DHKE) is a cryptographic method to securely exchange cryptographic keys over a public network in a way that overheard communication does not reveal the keys. The exchanged keys are used later for encrypted communication [30]. Figure 13 explains the Diffie-Hellman Key Exchange protocol.

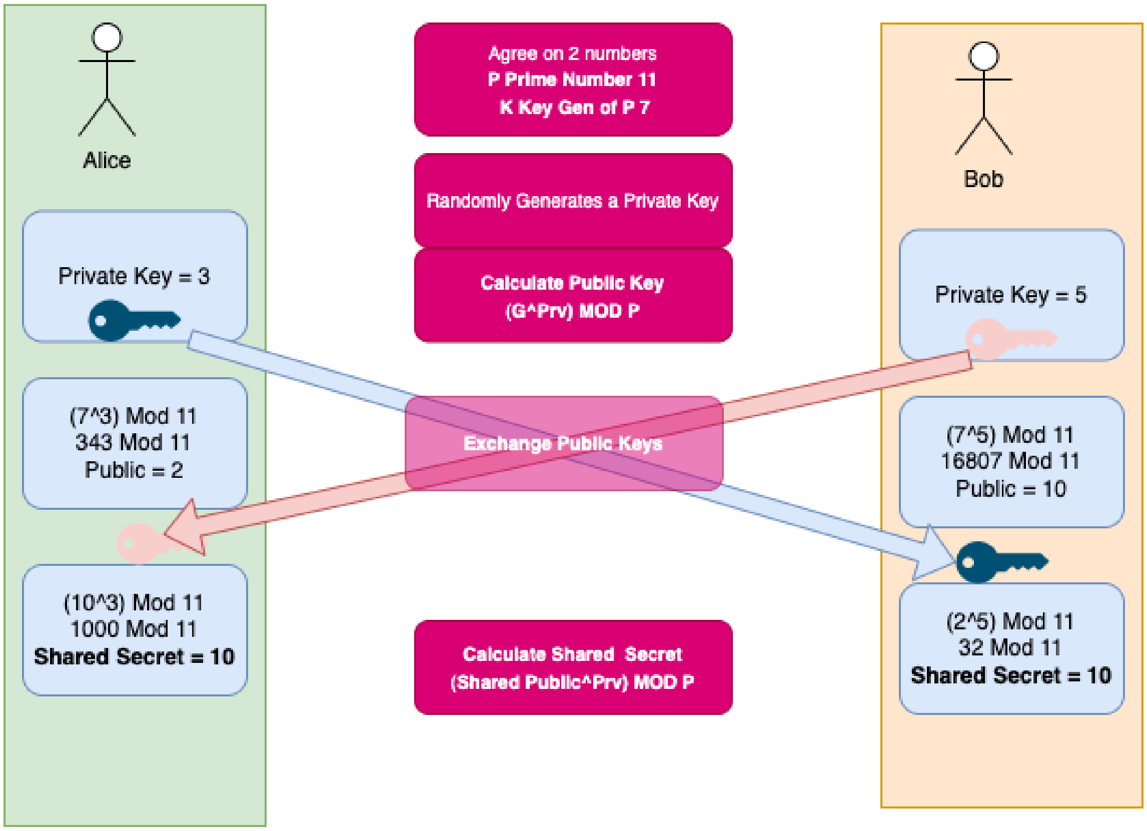
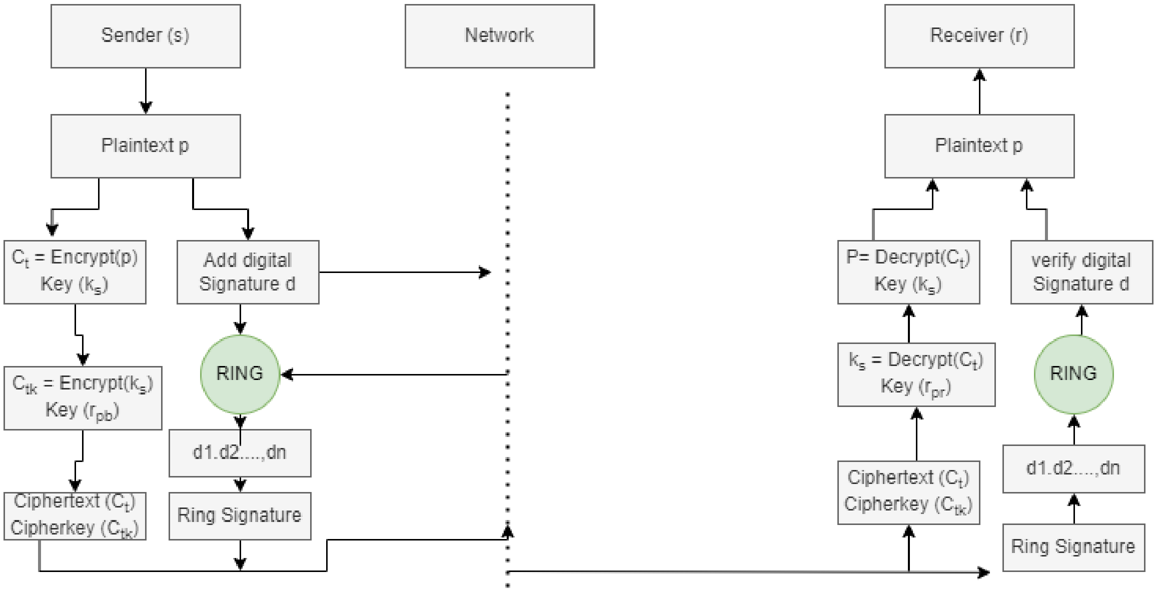


Figure 11 Diffie-Hellman Explanation

```
Algorithm 5 Ring Signature and sharing
function S(i)gnature(df)
    if user anonymity on the blockchain then
        Generate asymetric keypair $sk_{pb}$, $sk_{pr}$
        $h_q \leftarrow$ calculate hash of df
        Create the digital signature using $h_q$ and private key $sk_{pr}$
        Share the public key to the receiver using DH key exchange
        mix the signature with another network group form a ring
    end if
end function
```

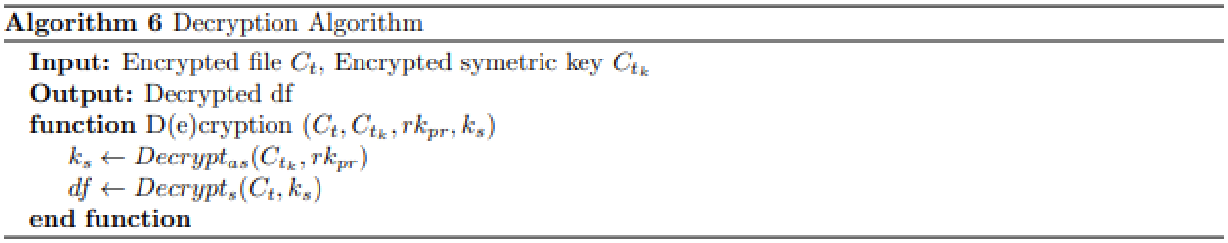
Algorithm 5 is used to preserve the user's anonymity. The user will ask the network for other accounts that also want to use the ring signature. The sender's transaction is then mixed with the other transactions and sent over the network. Since the message is mixed with others, no one can identify the sender. This can be seen in figure 14.



Sender (s)
Network
Receiver (r)
Plaintext p
C_t = Encrypt(p) Key (k_s)
Add digital Signature d
C_{tk} = Encrypt(k_s) Key (r_{pb})
RING
d1.d2....,dn
Ciphertext (C_t) Cipherkey (C_{tk})
Ring Signature
Plaintext p
P= Decrypt(C_t) Key (k_s)
verify digital Signature d
k_s = Decrypt(C_t) Key (r_{pr})
RING
Ciphertext (C_t) Cipherkey (C_{tk})
d1.d2....,dn
Ring Signature

Figure 12 Block diagram of Ring Signature model

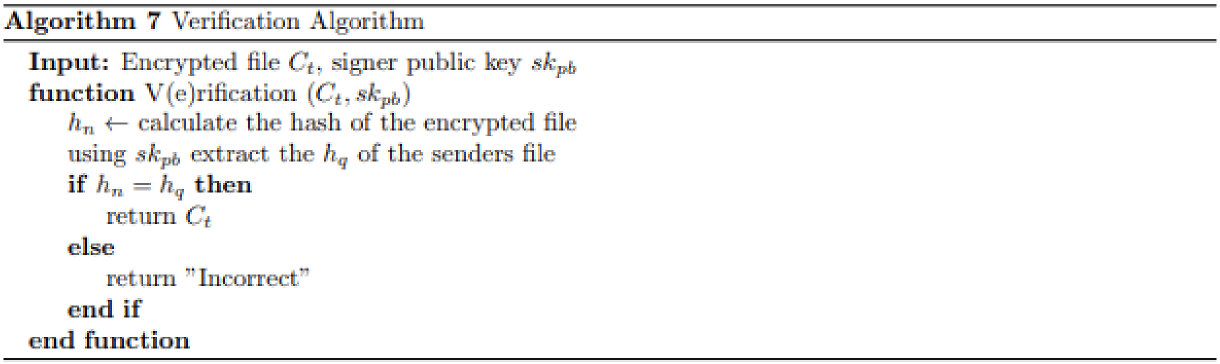
The data (df) which was encrypted using the encryption algorithm (4) can be decrypted using the decryption algorithm (6). In the decryption algorithm, the symmetric key k_{sym}, which was encrypted using the public key rk_{pb} of the receiver. The private key rk_{pr} can only decrypt the symmetric key. The C_{t_k} is decrypted using the private key rk_{pr} get the original symmetric key. The key is applied to the ciphertext C_t, revealing the original text.



Algorithm 6 Decryption Algorithm

```
Input: Encrypted file $C_t$, Encrypted symetric key $C_{t_k}$
Output: Decrypted df
function D(e)cryption ($C_t, C_{t_k}, rk_{pr}, k_s$)
    $k_s \leftarrow Decrypt_{as}(C_{t_k}, rk_{pr})$
    $df \leftarrow Decrypt_s(C_t, k_s)$
end function
```

The verification process (algorithm 7) the verifier generates the hash value h_n of the received data using the same hash function. The verifier also sends the digital signature and verification key to the verification algorithm and the h_q is extracted. If both hash values match, then the files have not been modified between the exchange.



Algorithm 7 Verification Algorithm

```
Input: Encrypted file $C_t$, signer public key $sk_{pb}$
function V(e)rification ($C_t, sk_{pb}$)
    $h_n \leftarrow$ calculate the hash of the encrypted file
    using $sk_{pb}$ extract the $h_q$ of the senders file
    if $h_n = h_q$ then
        return $C_t$
    else
        return "Incorrect"
    end if
end function
```

In order for any security system to be successful, it needs to address the basic principles of Information Security, the CIA model. Confidentiality, Integrity, and Availability. Confidentiality makes sure that only authorized users can access any systems or files. Integrity is responsible for messages sent to the destination without any change in the data. Availability means the data is always available to authorized users when the users request it.

Table 1 Security Requirements

Requirements	**Solution**
Confidentiality	Public Key
Integrity	Hashing of blocks
Availability	Limitations of transactions
Authorization	Use of Public Key and Ring Signature
Anonymity	Ring Signature

Table 1 shows how this security model deals with the CIA security model. The public key encryption guarantees Confidentiality. The integrity is guaranteed by hashing of the blocks. The hash will create a unique value that needs to be matched in the verification process. During verification, if the hashes do not match, the user will know that the integrity of the blocks has been compromised. Since there are limitations to the transactions within a blockchain, availability is guaranteed. While not part of the CIA model, anonymity and authentication are extremely important. The ring signature guarantees both anonymity and authentication. Authentication is also given by the use of public-key encryption.

CHAPTER V

Blockchain-based Privacy Preserving for IoT Devices

Internet Of Things (IoT) devices are very prevalent these days. They come with different functions. Let's take a Samsung Galaxy watch as an example. The watch will let a person call, text, check the weather, read the news, and listen to music. These watches also record a ‘person's steps heart rate, track a ‘person's sleep pattern, and many more activities. While IoT devices are great for tracking and getting information, they also process a great security risk. A malicious actor can get this information, or the privacy of these devices can be breached. Privacy in IoT is very challenging because of the lack of standardization, low power, and distributed nature. To meet the challenge, one can create a customized blockchain-based model.

In order to increase network stability and optimize resource consumption, a hierarchy model can be used. This hierarchy model consists of three (3) hierarchies. The hierarchies are cluster head, miners, and attribute authorities. The cluster heads are used to process data and for encryption. The IoT records the data and transmits to the cluster head for processing and transmission. The miners verify transactions and contribute to the blockchain. The attribute authorities are used to provide Attribute-based Encryption.

The four parties involved in ABE are the cluster head, miners, attribute authorities, and the distributed ledger. The cluster head processes the data from different sensors and encrypts it before the transaction. This encryption lets the miners see the transactions and verify if they have the right attributes. The data owners can control the privacy through fine-grained access control.

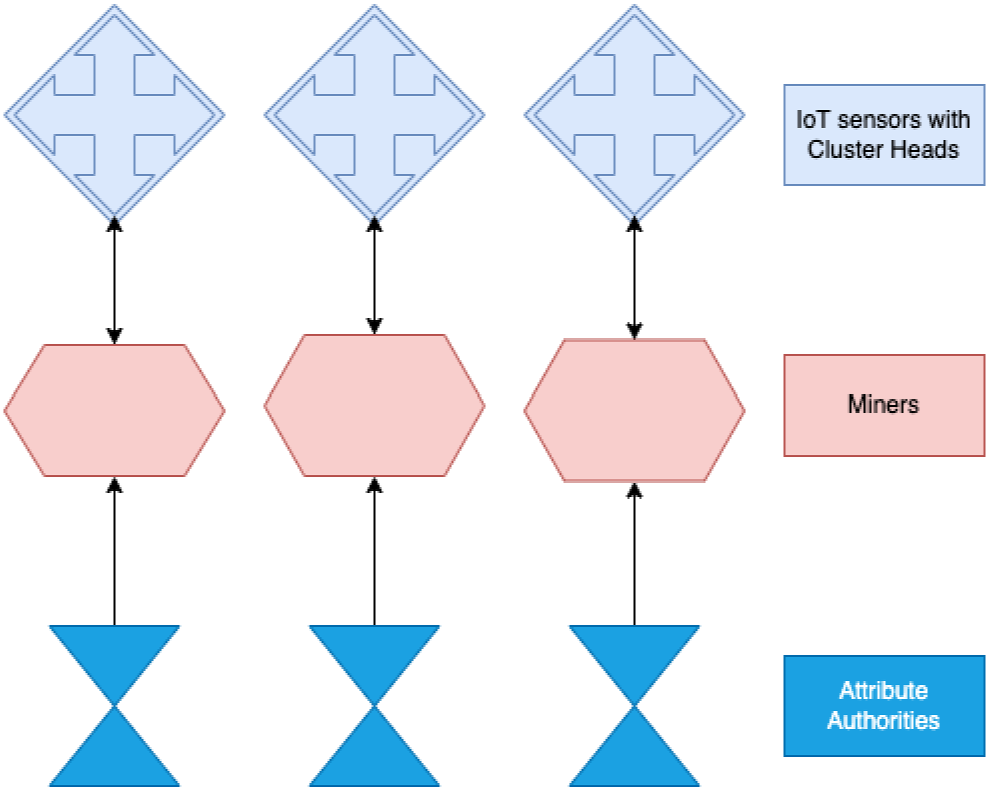
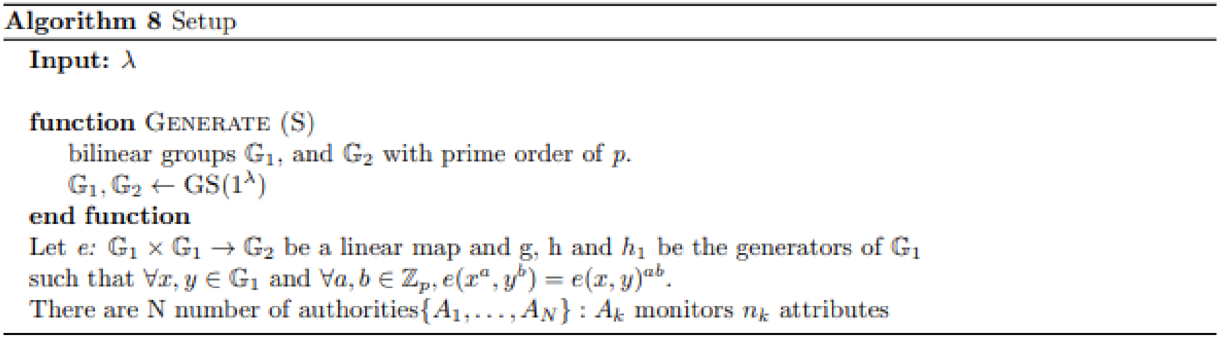


Figure 13 System Model

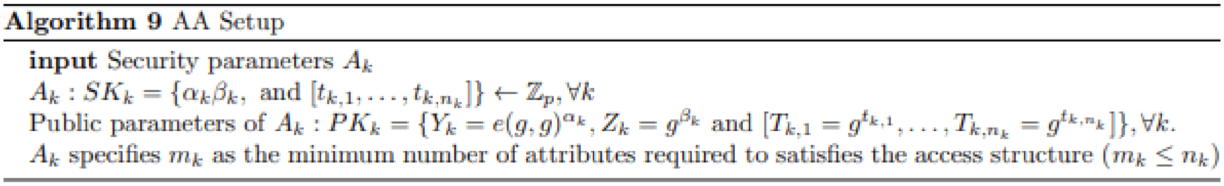
The attribute authority will verify and issue credentials to different miners and other users based on the attributes. A decentralized version of the Attribute-based Encryption will allow the authority attribute to issue credentials for miners and users. The decentralized ABE uses the five protocols: setup, attribute authority (AA) setup, Key Issuing, Encryption, and Decryption

The setup (algorithm 8) takes a security parameter as input and outputs system parameters that can be used by the AA who join the system. The AA setup (algorithm 9) will take the security parameters to generate a pair of public and private keys for the attributes that it will maintain.



Algorithm 8 Setup

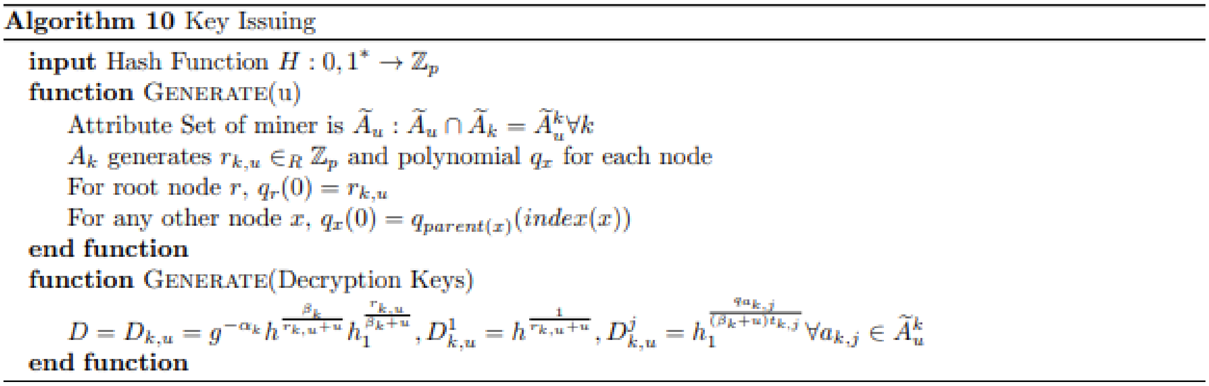
```
  Input: $\lambda$

  function GENERATE (S)
      bilinear groups $\mathbb{G}_1$, and $\mathbb{G}_2$ with prime order of $p$.
      $\mathbb{G}_1, \mathbb{G}_2 \leftarrow \mathrm{GS}(1^\lambda)$
  end function
  Let $e$: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a linear map and g, h and $h_1$ be the generators of $\mathbb{G}_1$
  such that $\forall x, y \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_p, e(x^a, y^b) = e(x, y)^{ab}$.
  There are N number of authorities$\{A_1, \ldots, A_N\}$ : $A_k$ monitors $n_k$ attributes
```



Algorithm 9 AA Setup

```
  input Security parameters $A_k$
  $A_k : SK_k = \{\alpha_k \beta_k,$ and $[t_{k,1}, \ldots, t_{k,n_k}]\} \leftarrow \mathbb{Z}_p, \forall k$
  Public parameters of $A_k : PK_k = \{Y_k = e(g, g)^{\alpha_k}, Z_k = g^{\beta_k}$ and $[T_{k,1} = g^{t_{k,1}}, \ldots, T_{k,n_k} = g^{t_{k,n_k}}]\}, \forall k$.
  $A_k$ specifies $m_k$ as the minimum number of attributes required to satisfies the access structure $(m_k \leq n_k)$
```

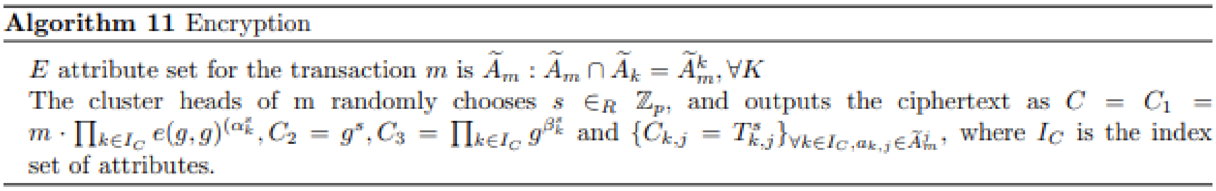
The key issuing protocol (algorithm 10) allows the miner or users and the authority attributes in order to determine the set of attributes belonging to the user. The attribute authority generates the decryption credentials for the user and transmits them to the user.



Algorithm 10 Key Issuing

```
  input Hash Function $H : 0, 1^* \rightarrow \mathbb{Z}_p$
  function GENERATE(u)
      Attribute Set of miner is $\widetilde{A}_u : \widetilde{A}_u \cap \widetilde{A}_k = \widetilde{A}_u^k \forall k$
      $A_k$ generates $r_{k,u} \in_R \mathbb{Z}_p$ and polynomial $q_x$ for each node
      For root node $r$, $q_r(0) = r_{k,u}$
      For any other node $x$, $q_x(0) = q_{parent(x)}(index(x))$
  end function
  function GENERATE(Decryption Keys)
      $D = D_{k,u} = g^{-\alpha_k} h^{\frac{\beta_k}{r_{k,u}+u}} h_1^{\frac{r_{k,u}}{\beta_k+u}}, D_{k,u}^1 = h^{\frac{1}{r_{k,u}+u}}, D_{k,u}^j = h_1^{\frac{q_{a_{k,j}}}{(\beta_k+u)t_{k,j}}} \forall a_{k,j} \in \widetilde{A}_u^k$
  end function
```

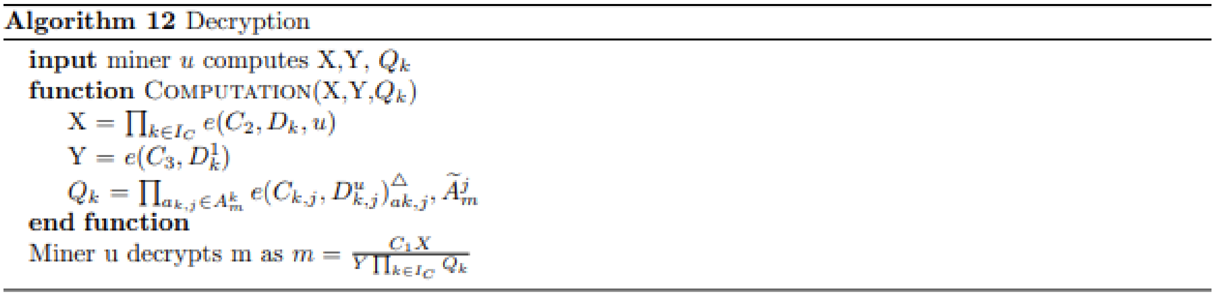
The encryption protocol (algorithm 11) is used by the cluster heads; the cluster heads take the set of attributes from the AA and the data from the sensors as input. The output will be the ciphertext of the data, which is added to the transaction.



Algorithm 11 Encryption

E attribute set for the transaction m is $\widetilde{A}_m : \widetilde{A}_m \cap \widetilde{A}_k = \widetilde{A}_m^k, \forall K$
The cluster heads of m randomly chooses $s \in_R \mathbb{Z}_p$, and outputs the ciphertext as $C = C_1 = m \cdot \prod_{k \in I_C} e(g,g)^{(\alpha_k^s}, C_2 = g^s, C_3 = \prod_{k \in I_C} g^{\beta_k^s}$ and $\{C_{k,j} = T_{k,j}^s\}_{\forall k \in I_C, a_{k,j} \in \widetilde{A}_m^j}$, where I_C is the index set of attributes.

The Decryption protocol (algorithm 12) is used by miners/blockchain users. The miners will take decryption credentials from the AA and the ciphertext from the transaction. In order for the decryption to be successful, the miner attributes satisfy the access structure of the ciphertext. The ABE uses bilinear sharing, secret sharing, and the Lagrangian interpolation.



```
Algorithm 12 Decryption
  input miner $u$ computes X,Y, $Q_k$
  function COMPUTATION(X,Y,$Q_k$)
      $X = \prod_{k \in I_C} e(C_2, D_k, u)$
      $Y = e(C_3, D_k^1)$
      $Q_k = \prod_{a_{k,j} \in A_m^k} e(C_{k,j}, D_{k,j}^u)_{ak,j}^{\triangle}, \widetilde{A}_m^j$
  end function
  Miner u decrypts m as $m = \frac{C_1 X}{Y \prod_{k \in I_C} Q_k}$
```

Bilinear Pairing: let G_1, G_2 be two multiplicative groups of prime order q and let g_1 and g_2 be generators of G_1 and G_2, respectively. A bilinear map $e: G_1 \times G_2 \rightarrow G_T$. The map has the following three properties:

1. Bilinearity: $\forall_x \in G_1, \forall_y \in G_2$, and a,b ∈ Z_q, there is $\hat{e}(x^a, y^b) = \hat{e}(x,y)^{ab}$.
2. Non-degeneracy: For $\forall_x \in G_1, \forall_y \in G_2$, there is $\hat{e}(x,y) \neq 1$.
3. Computability: $\hat{e}$ is an efficient computation.

Lagrange Interpolation: The secret sharing uses the Lagrange interpolation technique to obtain secret from shared-secrets. Suppose that $p(x) \in Z_p[x]$ is a $(k-1)$ degree polynomial and secret $s = p(0)$. Let us denote $S = x_1, x_2, \cdot, x_k$ and the Lagrange coefficient for x_i in S as

$$\delta_{x_i}, S(x) = \prod_{x_j \in S, x_j \neq x_i} \frac{x - x_j}{x_i - x_j}$$

For a given k different number of values $p(x_1)p(x_2) \cdot, p(x_k)$,the polynomial $p(x)$ can be reconstructed as follows,

$$p(x) = \sum_{x_i \in S} p(x_i) \prod_{x_j \in S, x_j \neq x_i} \frac{x - x_j}{x_i - x_j} = \sum_{x_i \in S} p(x_i) \delta_{x_i}, S(x),$$

hence the secret s can be obtained as:

$$s = p(0) = \sum_{x_i \in S} p(x_i) \prod_{x_j \in S, x_j \neq x_i} \frac{0 - x_j}{x_i - x_j}$$

Assume that there are \$N\$ number of attribute authorities $(A_1, A_2, \cdot, A_k)$ and denote the set of attributes for A_k as $A_k = \{a_{k,1}, \cdot, a_{k,nk}\} \forall k$. d_k is the value which a miner must have at least d_k number of attributes of this authority to obtain the private key associated with this attribute authority.

Initially, for a given security parameter λ, the setup algorithm S generates the bilinear groups $G_{\mathbb{1}}$ and $G_{\mathbb{2}}$ with the prime order p, $\{G_{\mathbb{1}}, G_{\mathbb{2}}\} \leftarrow GS(1^{\lambda})$. The authority setup algorithm AS is executed by each attribute authority to randomly generate public Keys and private keys (PKs and SK). The key pars for A_k are given as $\{(Y_k, Z_k, [T_{k,1}, \cdot, T_{k,nk}]), (\alpha_k, \beta_k, [t_{k,1}, \cdot, t_{k,nk}])\}$.

The attribute set belonging to user u as $\widetilde{A_u}$ and the common attribute set between user u and authority k as $\widetilde{A_u^k}, \widetilde{A_u^k} = \widetilde{A_u} \cap \widetilde{A_k}$. The key generation $\mathcal{KG}$ algorithm is used to issue the decryption keys to the user u with a set of attributes $\widetilde{A_u}$.

The set of attributes used to encrypt messages m as $\widetilde{A_m}$ and the common attribute set between message m and the authority k as $\widetilde{A_m^k}, \widetilde{A_m} = \{\widetilde{A_m^1}, \cdot, \widetilde{A_m^k}, \cdot, \widetilde{A_m^N}$. Let's denote the index set of authorities involved in the ciphertext of message m as I_c. The encryption algorithm $\mathcal{E}$ encrypts the message $m \in G_{\mathbb{2}}$ using an attribute set $\widetilde{A_m}$. To encrypt the message, the message owner randomly generates s and computes the ciphertext as $C = \left[C_1, C_2, C_3, C_{k,j}, \forall_{a_{k,j}} \in \widetilde{A_m^k}\right]$. The Decryption Algorithm $\mathcal{D}$ can be used to obtain the message \$m\$ from the cipher text if the user has the decryption keys.

Using blockchain technology in IoT has three security advantages: (1) The number of miners in the network verifies the sensor data generated by the IoT before the data is accepted. Since the data is verified, the adversary cannot manipulate the data. (2) The data cannot be tampered with once the data is accepted and added to the blocks. (3) The trust of each node is built by reputation since the lack of central authority. Since each node has its own reputation if the data on that node is damaged, the ' 'node's reputation is damaged.

The cluster head generates transaction data. The cluster head can be a smartphone or router, or a combination of both. The Process owner can determine what kind of sensors the frequency of collection. During the registration, the cluster data receives a unique ID. The cluster data create a pair of public and private keys. The public key is sent to the data process ' 'owner's server, where it is stored against the unique identifier. The miners can retrieve the unique identifier, public key, and the types of sensors. The unique identifier cannot be used to obtain private information.

Once the setup is completed, the cluster head collects the sensor data and distributes the transaction to peers for validation. Once the transaction data is verified, the application type is appended, and based on that data, the cluster head will decide the attribute for encryption. Once the access structure is decided based on the attribute, the cluster head will apply the Attribute-Based Encryption to encrypt the data and append the ciphertext in the transaction. The hash value of the transaction data is signed by the private key of the cluster head to generate a digital signature, and this is added to the transaction data. The transaction data is announced to the blockchain network by the cluster head.

The verification is done by the miners who are directly connected with the cluster head. The first miner will send the transaction data to others until all the miners in the network receive it. The miner will check if they have the right attributes to verify the transaction. If they have the right attributes, they will retrieve the public key and other details to the ID. The miner will use the attribute to decrypt the data, and they will cross-check the types of sensor data, and if it's in the range, then it will be accepted. When the transaction is verified by most of the miners, then ' 'it's passed and added to the block.

The new blocks are mined in the IoT system, similar to how the new blocks are mined in blockchain currency systems. In the blockchain currency systems, new blocks are mined periodically. The new blocks are mined with the verified transaction data. The miners will find the new hash value for the pending transaction data, which is subject to restrictions. The restrictions are increased in relation to the increment of computation power by the miners in the network. The miners will get tokens to get access the data in the future as rewards.

The security of this solution depends on the number of miners. If the cluster head chooses too many attributes, then the number of qualified miners is few, and that can impact the security. To avoid this issue, the blockchain will need to specify the minimum number of miners needed for verification. If there are only a small number of miners who are qualified, then the attribute authority will need to wait until the minimum number of miners are met.

To compare the performance of ABE, AES encryption can be used. If AES is used for encryption, then the number of keys used in the system is proportional to the number of cluster heads times the number of unique keys used by the cluster heads. This leads to the key management complexity. For example, if the system consists of 10000 sensors, then the cluster heads need to manage 10000 AES keys. In ABE, the IoT system with 10000 sensors with 25 attributes, with only 25 attributes. While the key management is minimal with ABE, the computation time will increase when compared to AES. In ABE, only the decryption protocol and encryption protocol are needed for computation.

The encryption time of the attribute based technique is given by

$$\big((2+n)k+1\big)c_e + \big((2k+1)c_m\big)2$$

and the decryption time is given by

$$\big((n+1)k+1\big)c_p + nkc_e + \big(3+(2+n)\big)k + cm$$

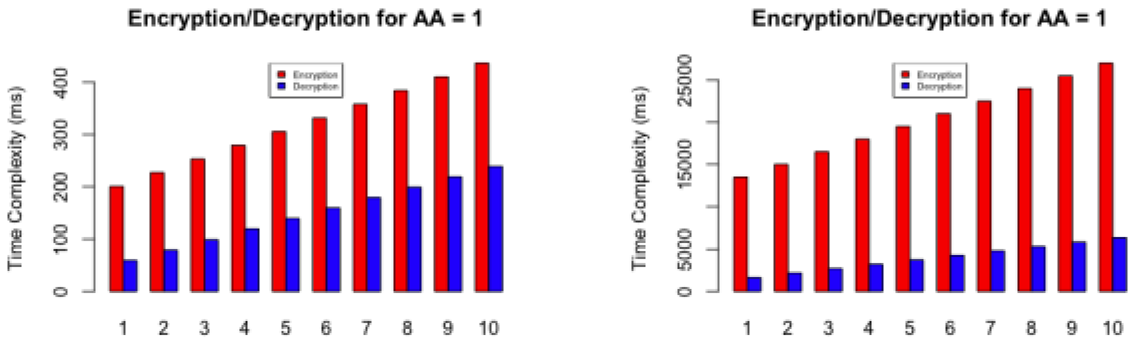
The Java Pairing-based Cryptographic library is a library used to perform pairing-based cryptographic systems. Two testbeds are used to test the ABE results. The benchmarks record the value of pairing (c_p), exponential function (c_e), and multiplication (c_m). The benchmarks for both testbeds are given below.

Table 2 Testbed 1

Operation	Times (ms)
Exponential (c_e)	2.623
Pairing $\left(c_p\right)$	15.72
Multiplication (c_m)	1.593

Table 3 Testbed 2

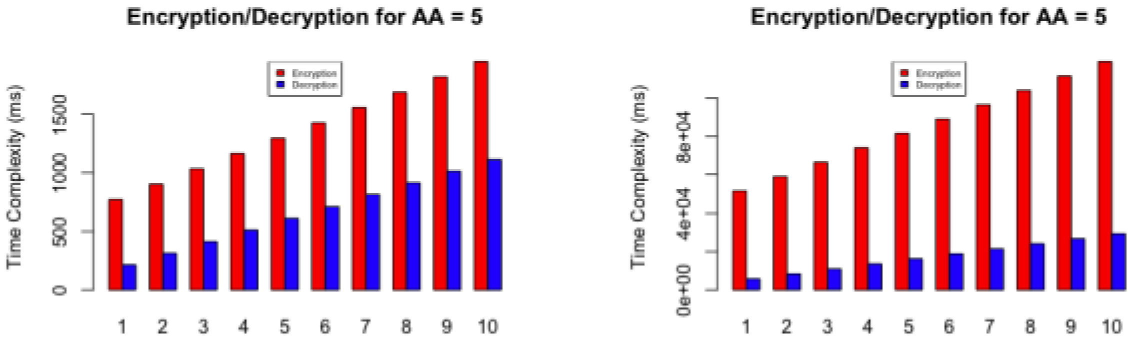
Operation	Times (ms)
Exponential (c_e)	15.323
Pairing $\left(c_p\right)$	250.042
Multiplication (c_m)	125.241



(a) Testbed 1: Attribute Authorities of 1

(b) Testbed 2: Attribute Authorities of 1

Figure 14 Encryption/Decryption times for 1 Attribute Authorities



(a) Testbed 1: Attribute Authorities of 5

(b) Testbed 2: Attribute Authorities of5

Figure 15 Encryption/Decryption times for 5 Attribute Authorities

From the figures 16 and 17, the encryption and decryption time have grown linearly with the increase of the number of attributes, and when more attribute authorities are present, the times go up by a factor of 50.

CHAPTER VI

Conclusion

Cyber attacks are increasing in people’s lives every day. While the attacks against traditional computing devices can be blocked to a certain degree, attacks against IoT devices are hard to prevent. The attacks are more challenging to prevent due to various reasons such as hardware of IT, connection protocols, the architecture of the devices, and others. Three (3) different ways to secure the private data on the IoT devices are explored in this research.

The first technique to hide private data on smart meters is to obfuscate the exciting data points to the reminder of data adding noise to the data. The addition of noise in the data and translating the data using the Laplace mechanism hides the data so that the original data cannot be identified. This is important because if the bad actor were looking at peak times to find out when the house or building is occupied, this would prevent it because it will "flatten" the peaks. Since the "peaks" are not available, the bad actors will not use occupancy detection to access the personal data.

The second and third technique uses blockchain techniques to safeguard the data. The two methods are different, one uses a hierarchical design, and the other uses symmetric encryption and ring digital signature on blockchain to protect the data. One method is used for managing devices and using the device information to safeguard the data, while the ABE blockchain model uses the data on the blockchain to protect privacy. In both blockchain techniques, verification is essential. In the attribute system, the verification process is the miner who has the correct attribute to verify the transaction is given the public key and other details to verify. The miner will decrypt the data and check the types of sensor data, and if the data is within range, it will be accepted. Once a majority of users/miners verify the verification, then it's added to the block. In management and authentication, verification is done with hash values. The verification algorithm receives the encrypted file and the ' 'sender's public key. The hash value of the encrypted file is extracted, and using the ' 'sender's public key, the hash value of the ' 'sender's file is extracted. Once the extraction is completed, both files are compared; if the hash values match, then the encrypted file is passed and sent to the decryption algorithm to decrypt the file.

Both algorithms with the blockchain mentioned above have significant computation time associated with them. Both algorithms have significant encryption, decryption, and verification time associated with them. In the ABE, the increase in the number of attributes per attribute authorities will provide better security, the time of encryption and decryption will also increase. The generation and verification using the ring signature does not take any additional time.

Both blockchain solutions are designed with IoT in mind, with the limitations of resources in IoT devices. Since the limitations of resources are an issue, using blockchain principles is the best solution for IoT Devices.

The two questions asked in the beginning were (1) how to safeguard privacy while using IoT devices (2). Is blockchain capable of securing privacy for IoT devices?

Blockchain can secure privacy in IoT devices, and this work showed three (3) different ways to secure privacy while using IoT devices. How do these algorithms perform against attacks and threats?

Both blockchain-based device management and attribute authority algorithms resist the Sybil attacks. Since many miners verify the data before the transaction is accepted, the transaction must be added to a new block for Sybil to have any large impact. Since random users cannot join the network without the correct authority, a DoS attack will fail. These algorithms are strong against the storage attack because the has is used to verify the transaction and the user. These algorithms are very strong against most attacks on traditional IoT system attacks and attacks against the blockchain.

The two questions asked in the beginning were (1). how to safeguard privacy while using IoT devices. (2). Is blockchain capable of securing privacy for IoT devices? Blockchain can secure privacy in IoT devices, and this work showed three (3) different ways to secure privacy while using IoT devices. There is much more work that can be done with blockchain and IoT devices to protect privacy. One particular question is, can both blockchain techniques be combined to have a stronger, faster protocol? In the techniques mentioned above, the underlying algorithm for blockchain is Proof of Work (PoW). Would Proof of Stake or Proof of History work better to prevent privacy leakage?

REFERENCES

[1] G. Zyskind, O. Nathan and A. '. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, 2015.

[2] W. Zhou and S. Piramuthu, "Security/privacy of wearable fitness tracking IoT devices," in *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, 2014.

[3] A. Yang, C. Zhang, Y. Chen, Y. Zhuansun and H. Liu, "Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms," *IEEE Internet of Things Journal,* vol. 7, pp. 2521-2530, 2020.

[4] J. Xiong, J. Ren, L. Chen, Z. Yao, M. Lin, D. Wu and B. Niu, "Enhancing Privacy and Availability for Data Clustering in Intelligent Electrical Service of IoT," *IEEE Internet of Things Journal,* vol. 6, pp. 1530-1540, 2019.

[5] F. Wu, L. Xu, S. Kumari and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *Journal of Ambient Intelligence and Humanized Computing,* vol. 8, pp. 101-116, 2017.

[6] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys Tutorials,* vol. 18, pp. 2084-2123, 2016.

[7] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks,* vol. 6, pp. 147-156, 2020.

[8] R. L. Rivest, A. Shamir and Y. Tauman, "How to Leak a Secret," in *Advances in Cryptology — ASIACRYPT 2001*, Berlin, 2001.

[9] D. B. Rawat, L. Njilla, K. Kwiat and C. Kamhoua, "iShare: Blockchain-Based Privacy-Aware Multi-Agent Information Sharing Games for Cybersecurity," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, 2018.

[10] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan and R. Lu, "User Collusion Avoidance Scheme for Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," *IEEE Transactions on Computers,* vol. 65, pp. 2939-2946, 2016.

[11] G. Rabinowitz, *Israeli hackers show light bulbs can take down the internet,* 2016.

[12] C. Qu, M. Tao, J. Zhang, X. Hong and R. Yuan, "Blockchain Based Credibility Verification Method for IoT Entities," *Security Communication Networks,* vol. 2018, pp. 7817614:1-7817614:11, 2018.

[13] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov and A. V. Vasilakos, "The Quest for Privacy in the Internet of Things," *IEEE Cloud Computing,* vol. 3, pp. 36-45, March 2016.

[14] T. Pecorella, L. Pierucci and F. Nizzi, "“Network Sentiment” Framework to Improve Security and Privacy for Smart Home," *Future Internet,* vol. 10, p. 125, December 2018.

[15] M. Mutamaie, "Blockchain Technology :“ The Next Computing Paradigm Shift," 2018. [Online].

[16] Y. Meng, W. Zhang, H. Zhu and X. S. Shen, "Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures," *IEEE Wireless Communications,* vol. 25, pp. 53-59, 2018.

[17] G. Mcshane, *What is a 51% attack?*, CoinDesk, 2021.

[18] D. Man, W. Yang, S. Xuan, X. Du and K.-K. R. Choo, "Thwarting Nonintrusive Occupancy Detection Attacks from Smart Meters," *Sec. and Commun. Netw.,* vol. 2017, January 2017.

[19] L. Malina, J. Hajny, P. Dzurenda and S. Ricci, "Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions," in *ICETE,* 2018.

[20] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu and M. Atiquzzaman, "Privacy Protector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems," *IEEE Communications Magazine,* vol. 56, pp. 163-168, 2018.

[21] J. Liu, Y. Yu, J. Jia, S. Wang, P. Fan, H. Wang and H. Zhang, "Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks," *Tsinghua Science and Technology,* vol. 24, pp. 575-584, 2019.

[22] F. Liu, T. Li and Z. Liu, "A Clustering K-Anonymity Privacy-Preserving Method for Wearable IoT Devices," *Security and Communications Networks,* vol. 2018, January 2018.

[23] Z. Ling, K. Liu, Y. Xu, Y. Jin and X. Fu, "An End-to-End View of IoT Security and Privacy," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference,* 2017.

[24] F. Li, Y. Rahulamathavan and M. Rajarajan, "LSD-ABAC: Lightweight static and dynamic attributes based access control scheme for secure data access in mobile environment," in *39th Annual IEEE Conference on Local Computer Networks*, 2014.

[25] D. Li, W. Peng, W. Deng and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 2018.

[26] E. Kovacs, *Twitter, others disrupted by ddos attack on DYN DNS service.*

[27] E. Kovacks, *Belkin Wemo Devices expose smartphones to attacks,* 2016.

[28] P. Kasireddy, *How does ethereum work, anyway?,* Medium, 2019.

[29] Y. H. Hwang, "IoT Security & Privacy: Threats and Challenges," in *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*, New York, NY, USA, 2015.

[30] H. Hasanova, U. Baek, M. Shin, K. Cho and M. Kim, "A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures," *International Journal of Network Management,* vol. 29, March 2019.

[31] M. T. Hammi, B. Hammi, P. Bellot and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security,* vol. 78, pp. 126-142, 2018.

[32] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," New York, NY, USA, 2006.

[33] B. Ge and W.-T. Zhu, "Preserving User Privacy in the Smart Grid by Hiding Appliance Load Characteristics," in *Cyberspace Safety and Security: 5th International Symposium, CSS 2013, Zhangjiajie, China, November 13-15, 2013, Proceedings*, Berlin, 2013.

[34] Ethereumbook, *Ethereumbook/07smart-contracts-solidity.asciidoc at develop · ethereumbook/ethereumbook,* 2021.

[35] A. Dorri, S. S. Kanhere and R. Jurdak, "Towards an Optimized BlockChain for IoT," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI),* 2017.

[36] M. Conoscenti, A. Vetrò and J. C. De Martin, "Peer to Peer for Privacy and Decentralization in the Internet of Things," in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, 2017.

[37] R. Chirgwin, *Get pwned: Web CCTV CAMS can be hijacked by single HTTP request*, The Register, 2016.

[38] D. Chen, P. Bovornkeeratiroj, D. Irwin and P. Shenoy, "Private Memoirs of IoT Devices: Safeguarding User Privacy in the IoT Era," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, 2018.

[39] D. Chen, S. Kalra, D. Irwin, P. Shenoy and J. Albrecht, "Preventing Occupancy Detection From Smart Meters," *IEEE Transactions on Smart Grid*, vol. 6, pp. 2426-2434, 2015.

[40] K. K. C H Lee, "Implementation of IoT System using BlockChain with Authentication and Data Protection," *International Conference on Information Networking*, 2018.

[41] E. Bertino, "Data Security and Privacy in the IoT," 2016.

[42] R. Bensont and E. Harmoush, *Diffie-Hellman*, 2021.

[43] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers, "SIMON and SPECK: Block Ciphers for the Internet of Things," *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 585, 2015.

[44] A. Assiri and H. Almagwashi, "IoT Security and Privacy Issues," in *2018 1st International Conference on Computer Applications Information Security (ICCAIS)*, 2018.

[45] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan and N. Feamster, *Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic*, 2017.

[46] Apriorit, *Blockchain attack vectors: Vulnerabilities of the most secure technology,* ApriorIT, 2021.

[47] M. Antonakakis, *Understanding the Mirai botnet,* 1970.

[48] M. S. Ali, K. Dolui and F. Antonelli, "IoT Data Privacy via Blockchains and IPFS," in *Proceedings of the Seventh International Conference on the Internet of Things*, New York, NY, USA, 2017.

[49] U. M. Aïvodji, S. Gambs and A. Martin, "IOTFLA : A Secured and Privacy-Preserving Smart Home Architecture Implementing Federated Learning," in *2019 IEEE Security and Privacy Workshops (SPW)*, 2019.

APPENDIX

Equations

The Laplace Distribution

$$\mathrm{Lap}(\mathrm{x}|\mathrm{b}) = \frac{1}{2\mathrm{b}}\exp\left(-\frac{|\mathrm{x}|}{\mathrm{b}}\right)$$

The Lagrange Interpolation

$$P(x) = \sum_{i=1}^{n} P_i(X)Y_i$$

Differential Privacy Mechanism

$$Pr(M(x) \in S \ \leq exp(\epsilon)\ Pr(M(y) \in S)\ +\ \delta$$

Bilinearity Pairing

$$f\colon G \times G \to G_T$$

Exponential additive

$$a \leq \frac{16\sqrt{log(|x|)log\frac{1}{\delta}}\,log\left(\frac{2nlog|X|}{\beta}\right)}{\sqrt{n}\epsilon}$$

SPECK Output Computation

$$X_{r,L} = \left(\left(X_{r-1,L} \gg r_1\right)2^n X_{r-1,R}\right) \oplus k_r$$

$$X\_\{r, R\}\ =\ ((X_{r-1,R} \ll r_2\right) \oplus X_{r,L}$$

VITA

Justin Joshuva was on April 8, 1984, in Kerala, India, to the parents of Yossuva Kuruvilla and Saramma Kizhakkayil. He is the older of two children with one younger sister, Annie. He and his family moved to New York in 1996. He has attended Museum Jr. High school and then onto Gorton High School. He has finished high school at Tyner High School in Chattanooga, TN. Justin attended the University of Tennessee at Chattanooga, where he studied Applied Mathematics with a concentration in General Mathematics and minored in Computer Science. He obtained a Master's degree in Computer Science: Information Security Assurance from U.T.C. Justin is employed at United States Army as a Data Scientist while finishing the doctoral degree.