BLOCKCHAIN APPLICATIONS INIoTTO SMART HOMES

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By
SODRULDEEN TEMITAYO MUSTAPHA

In Partial Fulfilment of the Requirements for the Degree of Master of Science in Software Engineering

NICOSIA, 2019

SODRULDEEN TEMITAYO MUSTAPHA
BLOCKCHAIN APPLICATIONS IN IoT TO SMART HOMES
NEU
2019

BLOCKCHAIN APPLICATIONS INIoTTO SMART HOMES

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By
SODRULDEEN TEMITAYO MUSTAPHA

In Partial Fulfilment of the Requirements for the Degree of Master of Science in Software Engineering

NICOSIA, 2019

SodruldeenTemitayo MUSTAPHA: BLOCKCHAIN APPLICATIONS IN IoT TO SMART HOMES

Approval of Director of Graduate School of Applied Sciences

Prof.DrNadire CAVUS

We Certify that this thesis is satisfactory for the award of the degree of Master of Science in Software Engineering

Examining Committee in Charge:

Assoc. Prof. Dr. MelikeSahDirekoglu	Chairperson Department of Computer, Engineering, NEU
Asst. Prof. Dr. KaanUyar	Supervisor,Department of Computer Engineering, NEU
Asst. Prof. Dr. UmitIlhan	Co-Supervisor,Department of Computer Engineering, NEU
Asst. Prof. Dr. YöneyKırsal EVER	Department of Software Engineering, NEU
Asst. Prof. Dr. BoranSekeroglu	Department of Information SystemsEngineering, NEU

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Lastname :SodruldeenTemitayo, Mustapha

Signature :

Date :

ABSTRACT

The growth of investment in automated systems to ease our daily activities is growing at a significant pace. Multinational corporations, smart kettles, self driving carsand a lot of other devices are now holding their data on the cloud, our daily lives are increasingly being managed from a single centralized information system: the Internet of Things. The IoT brings with it many pros, but also numerous risks. 30 billion new devices are estimated to come on board by 2020, our security and our privacy could be the price to pay.

Ensuring privacy and security is getting more attention as the faster the world develops technologically, so are the threats. Mechanisms have been deviced to secure the flow of data, but their still exist computational overhead that is not suitable for most resource-constrained IoT devices.

Thesecreates range of problems for firms and individuals, not least the potential for data sabotage, malfunctions anddevice hijack. By storing data on a distributed network, the it eliminates the risks that come with data being held centrally in a data farm, Blockchain makes use of powerful SHA256 encryption and generates a secret key only known to the user, this secret key is then used to sign transaction which will be attached to a public key.

This thesis presents a survey on the Blockchain application in IoT to smart homes. The objective of the research is to survey the existing research trends on the applications of Blockchain approaches and technologies similar to IoT context. Also, howblockchain technology can be implemented in keeping track of all communications or transactions between connected devices, blockchain makes use of permanent ledger, which means it cannot be altered nor remodeled by outside forces, this will help in eliminating the threats faced by traditional centralized server models. It can be used to ensure safety by micromanaging home or company internet ecosystems, also by monitoring communications between connected devices on the network and those devices with the wider, external IoT while cutting off access whenever a rogue connection is detected.

Keywords: Blockchain, internet-of-things, decentralized server model.

OZET

Günlük faaliyetlerimizi kolaylaştırmak için otomatik sistemlere yapılan yatırımın büyümesi önemli bir hızla artmaktadır. Çok uluslu şirketler, akıllı su ısıtıcıları, kendi kendine sürüş arabaları ve bir çok başka cihaz artık verilerini bulutta tutuyor, günlük yaşamlarımız giderek artan bir şekilde tek bir merkezi bilgi sisteminden yönetiliyor: Nesnelerin İnterneti. IoT beraberinde birçok artı, ama aynı zamanda çok sayıda risk getiriyor. 2020 yılına kadar 30 milyar yeni cihazın piyasaya sürüldüğü tahmin ediliyor, güvenliğimiz ve gizliliğimizin ödediği fiyat olabilir.

Dünyanın teknolojik olarak daha hızlı gelişmesiyle birlikte gizlilik ve güvenliği sağlamak, tehditler gibi daha da dikkat çekiyor. Veri akışını güvence altına almak için mekanizmalar geliştirilmiştir, ancak bunların çoğu hala kaynak kısıtlı IoT cihazları için uygun olmayan hesaplama yükü vardır.

Bunlar, firmalar ve şahıslar için çeşitli problemler yaratıyor, en azından veri sabotajı, arızalar ve cihaz ele geçirme potansiyeli değil. Dağıtılmış bir ağda veri depolayarak, verilerin bir veri çiftliğinde merkezi olarak tutulması ile ortaya çıkan riskleri ortadan kaldırır, Blockchain güçlü SHA256 şifrelemesini kullanır ve sadece kullanıcı tarafından bilinen bir gizli anahtar oluşturur, bu gizli anahtar daha sonra ortak anahtara eklenecek imza işareti.

Bu tez, Blockchain ve IoT'nin entegrasyonu hakkında kapsamlı bir anket sunuyor. Araştırmanın amacı, IoT bağlamına benzer Blockchain yaklaşımları ve teknolojilerinin uygulamaları hakkındaki mevcut araştırma eğilimlerini araştırmaktır. Ayrıca, blok zincir teknolojisinin bağlı cihazlar arasındaki tüm iletişimi veya işlemleri takip etmede nasıl uygulanabileceği, blockchain kalıcı defter kullanmaktadır, yani dış kuvvetler tarafından değiştirilemez veya tadilat yapılamaz, bu, geleneksel merkezileştirilmiş tehditlerin ortadan kaldırılmasına yardımcı olacaktır. sunucu modelleri Ev veya şirket internet ekosistemlerini mikro yöneterek, ayrıca ağdaki bağlı cihazlar ile daha geniş, harici IoT'li cihazlar arasındaki iletişimi izleyerek bir hileli bağlantı tespit edildiğinde erişimi keserek güvenliği sağlamak için kullanılabilir.

Anahtar Kelimeler: Blokzincir, IoT, merkezi olmayan sunucu modeli.

TABLE OF CONTENT

ACKNOWLEDGEMENTS …….. i

ABSTRACT …… iii

OZET …… iv

TABLE OF CONTENT …… vi

LIST OF TABLES …… ix

LIST OF FIGURES …… x

LIST OF ABBREVIATIONS …… xi

CHAPTER 1: INTRODUCTION

1.1 Introduction ……. 1

CHAPTER 2: PROBLEM FORMULATION

2.1 Research Objective ……. 4

2.2 Structure ……. 4

2.3 Literature Review ……. 5

2.3.1 Internet of Things ……. 5

2.3.2 Blockchain ……. 7

2.3.3 IoT Deployment Challenge ……. 8

2.4 Existing Centralised Model ……. 9

2.5 Decentralised Model ……. 10

CHAPTER 3: ANALYSIS OF BLOCKCHAIN FOR SMART HOMES

3.1 Definition of Research Questions …… 11

3.1.1 What Findings Have Been Addressed in Existing Research on IoT and Blockchain …… 11

3.1.2 What Applications or Platform Have Been Produced With And For Blockchain Technology …… 12

3.1.3 What Are The Recent Research Irregularities In Blockchain IoT Model …… …… 12

3.1.4 How Can The Security Threats Posed By IoT Be Contained WithBlockchain Technology… …… 12

3.1.5 What Are The Subsequent Research Directions For IoT …… 12

3.2 Conducting The Research …… 12

3.3 Collating Data for The Survey …… 17

3.3.1 Are The Current Security Mechanism In The Industry Efficiently Addressing Iot? …… 24

3.3.2 Are You Certain That You Can Control The Access To Your Data Captured By Iot Devices Installed In Your Home? ……..…… 24

3.3.3 Why Do We Need More Security For Connected Devices. …… 25

CHAPTER 4: BLOCKCHAIN AND IoT MODEL

4.1 Blockchain And IotModel Architecture …… 28

4.2 Smart Home ……. 29
4.2.1 Transactions …… 29
4.2.2 Local Blockchain …… 31
4.2.3 Home Miner …… 33
4.2.4 Local Storage …… 34
4.3 Overlay Network …… 34
4.4 Cloud Storage ……. 35
4.5 Transaction Handling …… 35
4.5.1 Storing……. 35
4.5.2 Accessing …… 36
4.5.3 Monitoring …… 38
4.6 Security Evaluation …… 38
4.6.1 Distributed Denial of Service Attack (DDOS) …… 39
4.6.2 Man-In-The-Middle-Attack …… 39
4.7 Evaluation Performance …… 40

CHAPTER 5: PROPOSED DECENTRALISED MODEL

5.1 Public / Private keys Pairs…….. 41
5.2 Signature……..…..……..…..…….. 42
5.2 Transaction……..…..……..…..…….. 44

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion ……..…..…….. 46
6.2 Recommendations….…..……..…..…….. 46

REFERENCES ……. 47

APPENDICES …….. 52

LIST OF TABLES

Table 3.1: Papers considered valid for this study ……. 14

Table 3.2: IoT connected devices worldwide from 2015 to 2025 (in billions)…….. 17

Table 3.3: IoT installed base by category 2014-2020……. 20

Table 4.1: Security Requirements Evaluation…….. 38

LIST OF FIGURES

Figure 2.1: IoT Architecture ……. 6

Figure 3.1: Graphical illustration of IoT growth worldwide ……. 18

Figure 3.2: IoT devices adoption in a different sector and the region as of January 2018 ……..……. 19

Figure 3.3: IoT installed based on category from 2014-2020 ..…… 20

Figure 3.4: Number of IoT units in the security industry in the European Union (EU) in 2017,2020 and 2025 (in million)…….. 22

Figure 3.5: IoT world wide security spending from 2016 to 2021 in million US Dollars …….. 23

Figure 3.6: Response from IoT users about if existing standards in the industry adequately addresses IoT security issues …… 24

Figure 3.7: Response from respondents about control to access to information produced by IoT devices …….. 25

Figure 3.8: The anticipated result of successful cyber-attacks worldwide as at 2017 …….. 26

Figure 4.1: Applications of IoT …….. 27

Figure 4.2: Access Transaction ……. 30

Figure 4.3: Monitor Transaction ……. 31

Figure 4.4: Smart home overview (Devices, Miner, Storage, and Blockchain) ….. 32

Figure 4.5: An example of a typical message with meta data and content. …… 37

LIST OF ABBREVIATIONS

AI	Artificial Intelligent
CH	Cluster Head
DDOS	Distributed Denial Of Service
DOS	Denial of Service
EU	European Union
FIFO	First In First Out
IoT	Internet Of Things
M2M	Machine to Machine
MAS	Monetary Authority of Singapore
RFID	Radio-Frequency Identification
SHA	Secure Hashing Algorithm
VPN	Virtual Private Network
UID	Unique Identification Number
CCTV	Close Circuit Television

CHAPTER 1
INTRODUCTION

The upcoming technological transformation orchestrated by Internet-of-Things (IoT) as hardware, Artificial Intelligence (AI) as its software and Blockchain as its network will strategically redefine the global economic environment and create an endless0 business opportunities.

Blockchain integration with IoT has been a topic researchers have been trying to research in recent years. Reyna et al. (2018) analyzed the challenges that could arise as a result of integrating IoT and blockchain technology.

The term “IoT” was initially aimed atreferring to exceptionally identifiable interconnecteddevices communicating with Radio-Frequency Identification (RFID) technology (Ashton, 2009), even till present date RFID still have a great impact and is one of the major driving force for IoT Presser and Gluhak (2009). IoT entails the interoperability of a ready-made physical environment with information systems through the aid of sensors and actuators to create smart adaptive objects and environments. The connection of billions of devices could have a lot of pros in our daily lives as it comes with numerous, but also, it increases the risk of having security loopholes, data leakagesandother privacy threats; some of these threats are new. Information leakage and denial of service were the most popular security threats known beforethe emergenceof IoT, threats can now be potentially related to the lives and properties, due to increase in the amount of personal information delivered and shared between connected devices.

Traditional security protection mechanisms have the difficulty in scaling up to meet the security demands of IoT because they are almost centralized. A very notable challenge for IoT is its distributed architecture. Typically, Cyber-attacks such as Distributed Denial-of-Service (DDoS) can be launched by exploiting a failure in each node in an IoT network. IoT data can be exploited and inappropriately used if there’s no provision made for data security.

Security solutions that are capable of providing an equivalent level of security for various IoT systems are increasing in demand, also is are the mechanisms that could efficiently audit and access control in a smart environment brought about the introduction of blockchain technology.

Blockchain technology can be used to authenticate, authorize, and audit data generated by devices. Also, the need to trust in the third party is eliminated due to its decentralized nature which cannot be altered by the unauthorized user. Blockchain ensures adequate security and protection for IoT systems with its distributed nature through the cryptographic processes it uses. Moreover, the hashing algorithm built upon blockchains provides it with the opportunity to create a reliable sensitive IoT application operating without many dependencies on environmental trust. The convergence of blockchain technology and IoT is on the agenda for many firms in different sectors, and there are already projects, solutions, andideas in countless possible IoT applications, including smart city, smart cars,smart grid, smart health, supply chain, and digital identity management and in some other applications yet to be pronounced.

In a blockchain network, every single block that follows the other must be changed in orderto make a change to a single block as they are all connected and the next block contains information about the previous block and it continues like that in a chain. And even if all the subsequent blocks following the altered block were changed, verification would still fail, because it will be recorded in blocks that the subsequent copies of the chain had tampered with it.

The financial services industry making use of technology, popularly known as FINTECH happens to be among the first few to experiment the usage of blockchain technology. The Monetary Authority of Singapore (MAS) implemented blockchain for interbank payment with no point of failure. They are taking it to be the first step in using blockchain technology to verify and authenticate finance invoices, auditing, and control money laundering activities.

This research will look into the recent applications of blockchain technology in ensuring efficient security and adequate privacy, and also how their use can improve IoT. The approach

used in this research is a survey of the previous research in which the Blockchain is leveraged to ensure privacy and improved security ofIoT.

CHAPTER 2
PROBLEM FORMULATION

In this chapter, first of all, the research question will be presented. Subsequently, it will be explained further and possible sub-questions will be presented.

2.1 Research objective

The main objective of this thesis is to survey researches related to security of IoT systems with Blockchain. The term ‘security’ if the question is put out to public opinion, enterprises might say revenues, consumers might say utility, but interoperability, security, compliance, privacy, and reliability are major barriers to IoT growth.

IoT provides support for the development of advanced applications for easy use but, ifthe security measures are not adequately put into effect, it may result to life threatening attacks, issues such asindividuals subjected to physical attacks such as robbery or kidnapping may as a result of the breach of the smart alarm and other devices connected to the network.

Even with 30 years of development of IoT, there is still no universally shared architecture to interconnect distributed machines. IoT architecture varies from solution to solution, based on the type of solution which we intend to build.

Having a secure ecosystem is one of the major bottlenecks of IoT, and it encompassesunderstanding all the building blocks of IoT architecture and its area of vulnerability and technologies required to mitigate each of the weaknesses needed in dealing with the IoT security.

2.2 Structure

This thesis is divided of fivedifferent parts. With the first chapter reviewing relevant literature in order to get an idea of the research topic beforeanalyzing our research objective. Also, the research method adoptedwere introduced and explained.

Afterward, the findings of various study from various scholarly articles, journals, and slides related to the objective of these findings werebrought forward and analyzed.

Finally, the research conclusions regarding the questionsweredrafted and recommendations for further possible research was given.

2.3 Literature review

An introduction to the literature on the blockchain, internet-of-things, and artificial intelligence will be given in order to point out thelikely areas where this thesis will contribute. Also, the frequently used terms and theories inexplaining the convergence will be shown. Subsequently, the general ideology of blockchain and, finally, how blockchain technology can be integrated to ensure safety of Internet-of-things systems and platforms will be considered.

2.3.1 Internet of Things

The Internet of Things (IoT) can be said to be the use of interoperability of devices and systems to process raw informationcollected by embedded sensors and actuators in a device. The concept of IoT can be traced back to the 19th century, mentioning the way in which computer controls various individual things (Ashton, 2009).

A person with a pulse monitoring device, a dog with a biochip transponder, an object with a unique identification number (UID) could be refer to as thing in the concept of Internet-of-things. It could also bea built-in sensors in vehicles that notify the driver about low tire pressure and other conditions or simply a device that can be allocated a unique IP address and is able to communicate over a network could also be refer to as thing.

The aim of IoT is for devices to connect and transfer information securely, and hence, reshaping the globe into gigantics information system.

We obviously cannot mention IoT without talking about Artificial Intelligence (AI) evolving over decades of research. Itsmajorideology didn’t change but its application keeps evoluting. However, AI at least for now is not about superior machines colonizing our planet and making

human race slaves to machines as its popularly portrayed in movies, it is not yet advanced to that level, though technology keeps advancing.

The way AI was seen and believed to be in the 19th century is not the same way it's actually implemented today. Theoretically, AI refers to the technology that machine can think and act independently without dependence on human control or a specifically written program or instruction (Shane, 2007). AI can be defined as any machine intelligent enough to act independently, from your mobile phone virtual, to the daily search engine, oursmart tv's or car remote control,all this areproducts by AI. Although they are only the preliminary AI application (Deloitte, 2017).

IoT architecture building blocks display how IoT systems are connected to connect, store and process data. The diagram in fig 2.1 shows the IoT architecture subdivided into the Application, Network, and Machine to Machine (M2M) device infrastructure.

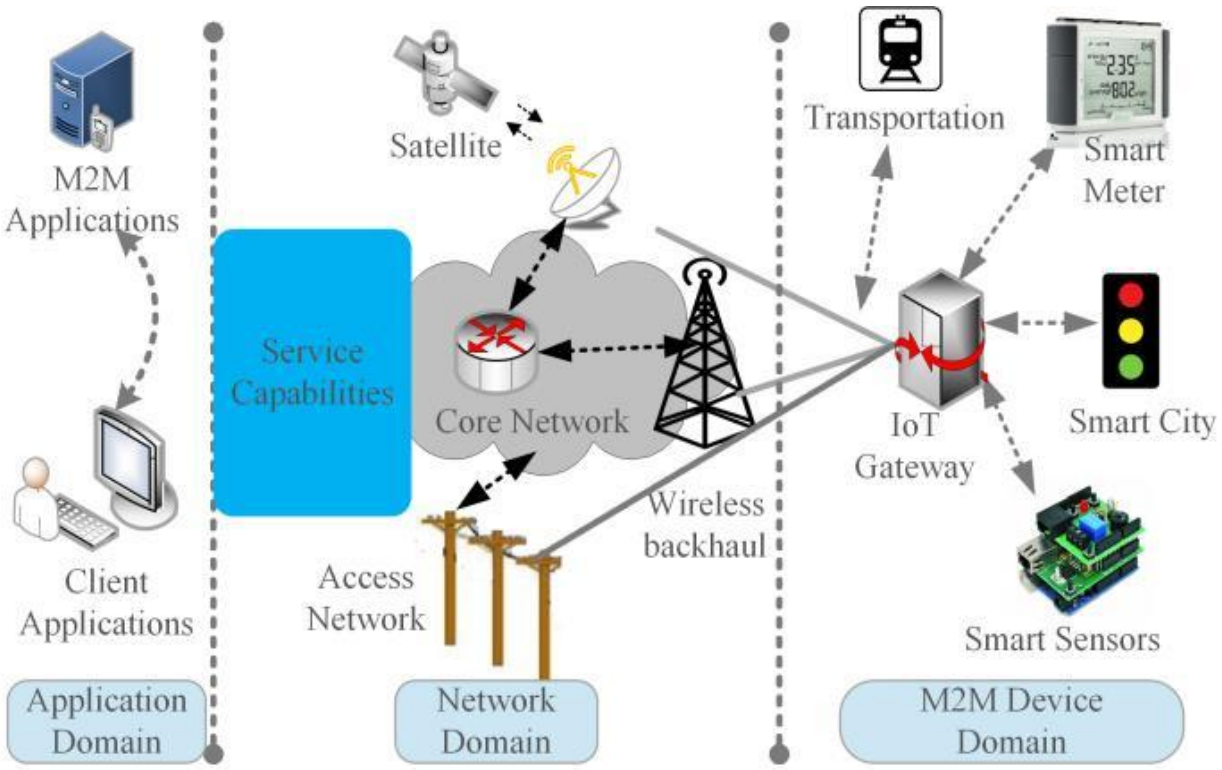


Figure 2.1*:* IoT Architecture

The major IoT architecture building blocks in the above diagram are

- Network Infrastructure
- Cloud Infrastructure
- Gateways
- Things

Network Infrastructure: These comprises of devices such as that controls and secure data flow back and forth, devices such as routers, aggregators, gateways, repeaters etc.

Cloud Infrastructure: These are large puddle of connected servers as well as storages with huge computing and analytical capabilities.

Gateways: Thesefunctions as intermediaries needed for connectivity and security between the cloud and device.It also provides an ease to manageability of device.

Things: These are merelydetectabledevices, nodes, primary sensors which independently interactbeyond human intercommunication adopting distinct approaches of connectivity.

2.3.2 Blockchain

The blockchain is network of incorruptible digital ledger of informationexchange whichdoes not store only history of financial transactions like in bitcoin which its popularly known for, but capable of storing everything of value (Dop Tapscott & Alex Tapscott,2016).

To a layman, blockchain is a giant collection of public records which cannot be erased, deleted or edited.As there exist nocentral computer or device on which the entire chain are saved making it a distributed and decentralized network. Rather, each block nodes involved in transactionskeeps a copy of the transactions and the data of the previous are saved in the new blocks continuosly.

Data records are continuously added to the chain, which made it ever-growing.

A major elements that constitute blockchain are:

- **Transactions:** These are the actions initiated by each participating nodes in the system.

- **Blocks:** These are the recorded transactions, they are arranged in sequence and are in their original form. The block also record timestamp of when the transactions were added.

Blockchain application is numerous, which include cryptocurrency, smart contracts, music, real estate, fraud detection, identity, internet of things etc In this research, we will be looking into the application of Blockchain to the security of internet of things.

It has already proved its worth in the world of cryptocurrency transactions, and many innovators are already looking to the ways it can be scaled up to future-proof the burgeoning yet risk-prone IoT.

Arecentideathat has to do with our newly adopted technology: Internet-of-Things is being powered by blockchain. Spending on the IoT market keeps growing and it is predicted to reach about $1 Trillion mark in few years. Blockchain-Internet-of-Things convergence have the opportunity to provide the paramountmechanism to monitor the billions of smart-devices coming online histories over the coming years by making use of its incorruptible permanent ledger.

2.3.3 IoT Device deployment challenge

There are security technologies and measures taken to ensure IoT device security and mitigate risk but these measures effectiveness is not enough. The objective is to securelyretrieve datafrom the desired place, at the desired time, in the desired format and to be delivered to the right place.

Below are few of the challenges faced by in securing IoT devices.

- The design and implemention of many IoT systems is poor, they are created by using diverse protocols and technologies which sometimes have conflicting configurations.
- Internet-of-Thingsintegrity concerns are complicated aren'tusually readily noticed.
- Authentication and verification standards does not exist for IoT edge devices.
- Qualitysetup ofindependentIoT platforms that supportsserving multiple users.
- Insufficient steps for lifecycle and continuous management of operations of IoT devices.
- The uses of IoT scope and technologies are expanding and experiencing fast evolution.

With about 20.8 billion devices predicted to be connected through IoT by 2020 (Gartner, 2014), new security technologies and advanced measures will be required to protect IoT systems and platforms in order to mitigate information leakage, physical tampering. In order to encrypt informations and tackle new challenges such as impersonation of "things" or popularly known denial-of-sleep attacks which drains batteries and lead to denial-of-service attacks (DoS).

Although most "things" uses simple processors that may not support the sophisticated security approach and are needed as a matter of urgency, for example, the not too long ago massive Distributed Denial of Service attack (DDoS) that crippled the servers of giants like Netflix, Twitter, PayPal, and NY Times across the United States on October 21^{st,} 2016 which occurred as a result of an extreme assault that include millions of web addresses and dangerous software. The attack was reported amid a rising number of cybersecurity breaches. It was suspected thata malware was used on all connected devices that powerday to dayactivities like vehicle remote control, CCTV and other devices and was used against the server.

2.4 Existing model

Currently, IoT sectordepends on a model known as server/client paradigm, a centralized model which first of allidentifies all connected device are, authenticate them and then connectthemvia cloud servers that hashigh storage and processing power.

This model has been in use to connect several devices for about a decade now and itis still supportingIoT devices on small-scale networks, but itssufficiencyin responding to the continuous growth need of IoT ecosystem wouldn't be enough.

Also, the current solutions proffered for IoT platforms are outrageous due to the sophisticated infrastructure and cost of maintenance associated with large server farm, and networking apparatus. The unit of communications to handle billions IoT devices is one of the cause for thesubstantial increase in cost. Even if the engineering and economic bottleneck are solved, another notedbottleneck which can alter the network is that the cloud connectivity will remain a challenge.

2.5 Decentralized model

A decentralized approach to IoT will substantively reduce the cost of installation and maintenance of large centrally located data farms and allocate computational and storage requirementto other billions of deviceswhich IoT network ismade up of, by adopting homogenizepeer-to-peer communication model in the processing the billions ofinformation that passesthrough various devices. With this approach, a halt or fault in a node will not bring the whole network down as transactions are recorded on every participating node. The use case we will be surveying for this research is the smart home how to use blockchain technology to improve its security.

It was seen in previous findings thatabout 54% more people leaves in bigger cities while about 46%them leaves in rural areas, and by 2050 this number is projected to further increase by about 66%, this will in turn have an impact on the growth of IoT (United Nations).

CHAPTER 3

METHODOLOGY

The method used for this survey is referred to as systematic mapping and the aim is to achieve a more clearer overview of previous research carried out and also to institute if there are investigative proof that could back up and validate this survey.

In this study,relevant papers, journals, articles and website were reviewed as described by Kitchenham and Charters (2007), and Petersen et al (2008).

These method chosen is due to the fact that it provide a better review of previous literature and researches done in relation to blockchain technology.

The outcome from these various source will serve as a guide to identify our research interest related to blockchain technology convergence with IoT as well as pointing out conceivable research gaps.

3.1 Definition of research questions

The Systematic mapping process defines the research questions first. Of which, itsobjective of this research is to give an overview ofexisting research direction withinblockchain and how it can be used to improve IoT security. These made us define four questions pertaining to these research:

3.1.1 What findings have been addressed in the existing research on IoT and Blockchain?

It is very important to first of allhave a knowledge onBlockchain and IoT modeland this is done byaggregating helpful papers either from IoT related website or databases.From this, we can get to understand the research and methods used.

Mapping the previous work done will encourage analyst to further understand the topic and makes blockchain and IoT modelbetter.

3.1.2 What applications or platform have been produced with and for blockchain technology?

Bitcoin cryptocurrency is the most popular application related to blockchain techology . The Bitcoin currency transactions has blockchain technology as its backbone. However, Blockchain technology have a lot of other applications other than the bitcoin. Consequently, ing the current platforms created with Blockchain technology is important and how it can be used in conjuction with other technologies. These will aid the understandingof furtherareas and ways to implementthe technology.

3.1.3 What are the recent research irregularities in blockchain and IoT model?

The methodology used will also enable us to percieve the existing research gaps in blockchain. It will allow other researchers and analyst to channel their findings on further studies on other areas rather than starting afresh. Finding research gaps will aid the understanding and answer various research questions in current Blockchain technology, this particular survey looks into how blockchain technology can be used to secure IoT devices.

3.1.4 How can the security threats posed by IoT be contained with Blockchain Technology?

The major problems and risk posed by IoT systems is privacy and data leakage, which can be contained by introducing encryption for each of the transactions to and from each devices and also setting permissions to each device.

3.1.5 What are the subsequent research directions for IoT?

The answer to this question will determine where the findings on IoT should be concentrated and theareasthat need to be addressed.

3.2 Conducting the search

Another step ofthis method after the research questions issearching for various relevant sources on the research. The systematic literature search is undertaken with the use of search

protocols to define the method. An alreadydefinedmodel is required to reduce the chances of incompetence.

Sources relevant to this research objective were gathered from the various platforms. After searching with various keywords, the terms securing IoT with blockchain search string was one of our preffered keywords, another possible search string would have been blockchain, but we needed more than information on just blockchain, how it can be used to ensure integrity should be considered. Eventhough,blockchain part of the search term, variouspre researched documents that were similar to usually to cryptocurrencies economic topics were majority of the search results, instead of findings that are similar to thetechnicalarea of blockchain technology.

Hence, the objective of the usedmethodology was to search and analyse similar researches to the technical aspects of blockchain technology and more importantly how it can be utilized in securing IoT systems, we decided to drop the single term blockchain. It is believed that by making use of the search string blockchain and IoT, most of the research materials that considers theworking perspective on blockchain were brought forward. Also, it looks like when a Bitcoin-related research materialommits the term blockchain and IoTwithin its meta-data, the material willlikely be about the cryptocurrency economic aspect of it.

Peer-review of respectedresearch materials from various conferences, workshops, symposiums, books, and journals related to our research areawere considered, also are materials from the internet. After scanning through several sources for related material retrieval. Some related papers were retrieved from the likes (1) IEEE journal, (2) ARXIV, (3) Springer Link, (4) Research Gate, and (5)ScienceDirect. Grey literature e.g. from Google searches, Google scholar, bing etc were also given much consideration.

The papers tabulated in Table 3.1 below were considered and considered valid for this study.

Table 3.1: Papers considered valid for this study

Source	Title	Multiple Encryption	Keys Signing	Mutable	Refrences
IEEE Xplore	⁃ Privacy-preserving data analytics for smart homes," in Security and Privacy Workshops (SPW).	⁃ Yes	⁃ No	⁃ Yes	⁃ Chakravorty A, Wlodarczyk T, and Rong C, (2013). "Privacy-preserving data analytics for smart homes," in Security and Privacy Workshops (SPW), IEEE,(pp. 23–27).
	⁃ Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT.	⁃ Yes	⁃ Yes	⁃ No	⁃ Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, *5*, 1184-1195.
	⁃ Improving IoT Service in the smart home using blockchain smart contract.	⁃ Yes	⁃ Yes	⁃ No	⁃ Yiyun Z, Meng H, Liyuan L, Yan W, Yi L, Ling T. (2018).Improving IoT Service In The Smart Home Using Blockchain Smart Contract.In Proceedings of the 11th IEEE International Conference on Internet of Things(iThings 2018),Halifax, Canada.DOI: 10.1109/Cybermatics_2018.2018.00047

	⁾ Privacy-preserving data analytics for smart homes," in Security and Privacy Workshops (SPW). ⁾ DDoS in the IoT: Mirai and other botnets computers.	⁾ Yes ⁾ No	⁾ No ⁾ No	⁾ Yes ⁾ Yes	⁾ Chakravorty A, Wlodarczyk T, and Rong C, (2013). "Privacy-preserving data analytics for smart homes," in Security and Privacy Workshops (SPW), IEEE,(pp. 23–27). ⁾ Kolias, C.; Kambourakis, G.; Stavrou, A. (2017).;Voas, J. DDoS in the IoT: Mirai and other botnets Computer malware. v50, pp 80–84.
ARXIV	⁾ Blockchain in the Internet of Things: Challenges and Solutions.	⁾ Yes	⁾ Yes	⁾ No	⁾ Dorri A, Kanhere S, and Jurdak R, (2016) "Blockchain in internet of things:Challenges and solutions," arXiv preprint arXiv:1608.05187.
ScienceDirect	⁾ On blockchain and its integration with IoT. Challenges and opportunities.	⁾ Yes	⁾ Yes	⁾ No	⁾ Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. (2018) Onblockchain and its integrationwith IoT Challenges and opportunities. Future Generation Computer Systems, 88, 173–190.

	⁾ Guidelines for Performing Systematic Literature Reviews in Software Engineering;	⁾ No	⁾ No	⁾ No	⁾ Kitchenham B, Charters S. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering.
Research Gate	⁾ A Review on the Use of Blockchain for the Internet of Things. ⁾ That 'Internet of Things' Thing	⁾ Yes ⁾ Yes	⁾ Yes ⁾ No	⁾ No ⁾ Yes	⁾ M. Fernández-Caramés T,Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access, 6*, 32979-33001. ⁾ Ashton K. (2009). That 'Internet of Things' Thing. RFID Journal. (Vol 22, pp. 97-114).
ACM Digital library	⁾ A Collection of Definitions of Intelligence.	⁾ No	⁾ No	⁾ No	⁾ Legg, S; Hutter, M. (2007). A Collection of Definitions of Intelligence. arXiv:0706.3639 .157, pp 17-24.

3.3 Collating data for the survey

The IoT is a very promising area, as researchindicates that itsrapid growth both in terms of market value and connected devices in the coming years. The estimated worthof connected device globally was predicted to exceed the a trillion U.S. dollars threshold by the year 2017 for the first time ever, an increase worth paying attention to, taking into consideration that in 2014, the market was worth about 600 billion U.S. The unit of devices installed worldwide is predicted to double from around 15 billion in 2015 to 30 billion by the end of 2020.

The speedy growth in the Internet of Things (IoT) ecosystem has resulted in to increase in growth of data generated by these devices and sensors put on the Internet. Growth spanning from a different aspect of our daily lives to different consumer and industrial sectors.

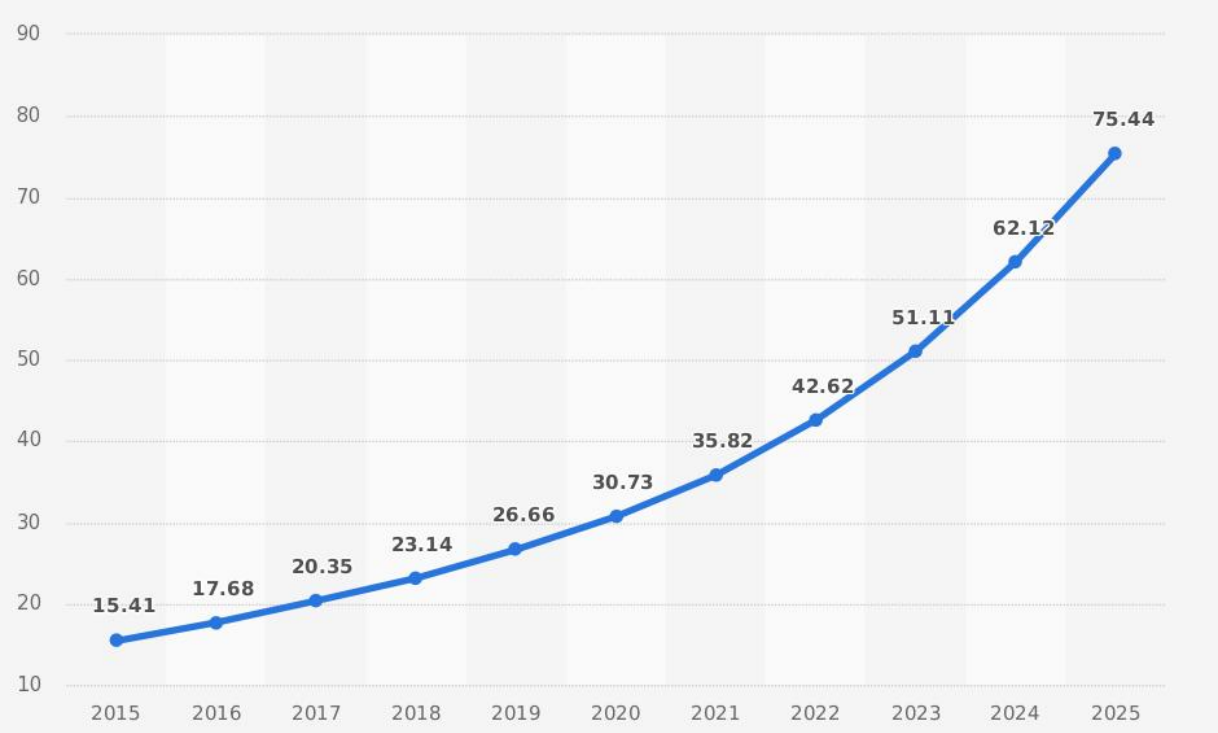
The table below shows the worldwide growth of IoT from the year 2015, projected to the year 2025.

Table 3.2: Connected IoT devices worldwide from year 2015 to year 2025 (in billions)

Years	**Unit of devices connected in billions**
2015	15.41
2016	17.68
2017	20.35
2018	23.14
2019	26.66
2020	30.73
2021	35.82
2022	42.62
2023	51.11
2024	62.12
2025	75.44

Source: Statista.com

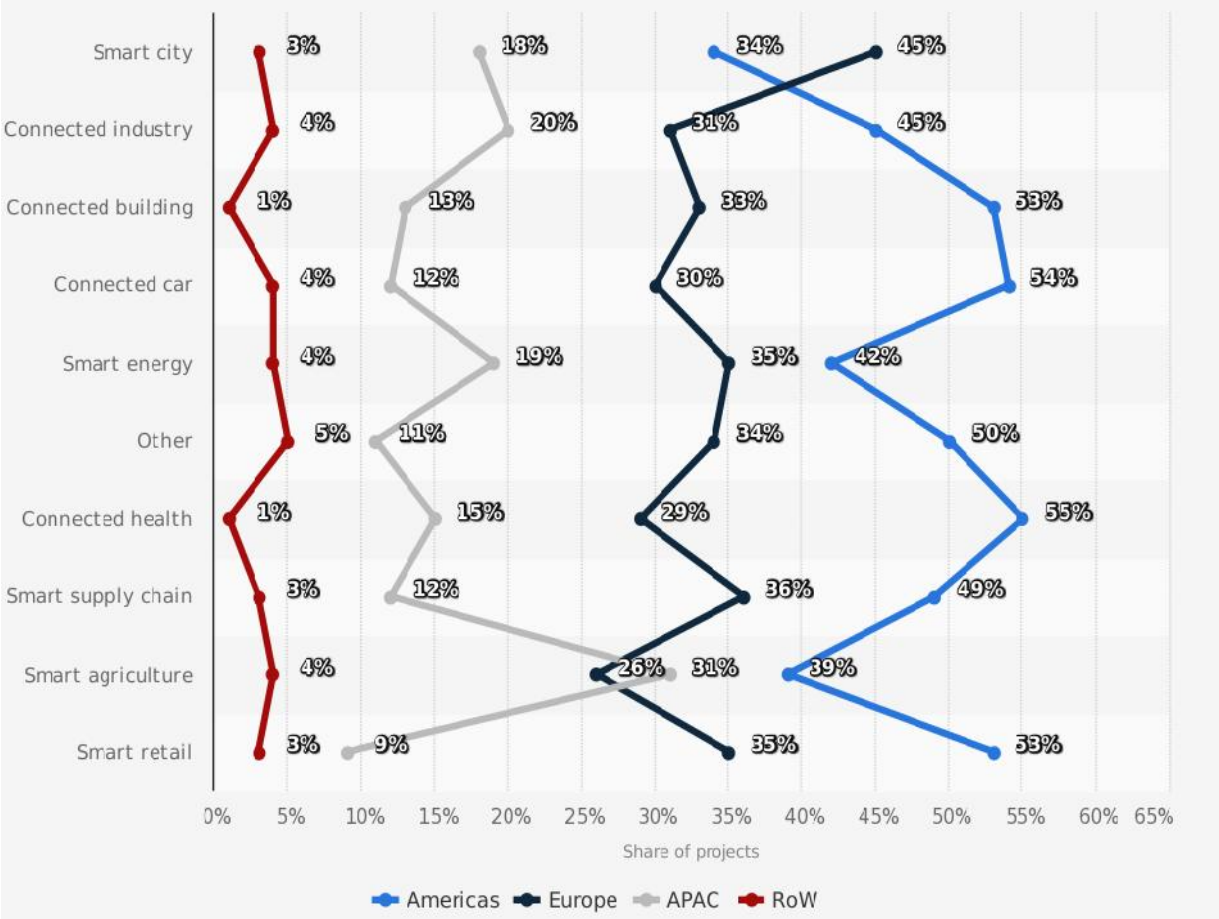
In the year 2015, 14.41 billion devices were connected, and the growth kept increasing yearly up to this current year 2018 where we have 23.14 billion connected devices and a projected 75.44 billion to be connected by 2025 as illustrated in the chart in fig 3.1.



Source: Statista.com

Figure 3.1: Graphical illustration of IoT growth worldwide

This growth is further breakdown into segment and region, America accounted for 54 percent of enterprise connected cars while Europe has the highest number of connected homes, also enterprise IoT solutions are making great impact in the health sector with America accounting for about 55 percent as at January 2018 worldwide analysis, healthcare devices such as Depression-fighting Apple Watch app, activity tracker and then continuously for several months over the course of multiple treatments, coagulation testing system which enable patients to monitor their blood clots etc. are few among IoT devices already shaping the globe. The chart below displays the even distribution of IoT adoption according to region and segment as of January 2018.



Source: Statista.com

Figure 3.2: IoT devices adoption in different sector and region as of January 2018

The unit of devices installed is projected to climb to nearly 31 billion by 2020from about five billion in the year 2015, consumer sector will be accounting for the most of the unstalled units. In theconsumer sector, theunit of devicesinstalled by the end of the year 2020 is predicted to reach 13.5. Also,car production industry is a amazing sector for IoT usage and will make for about 14 percent of the devices installed in year 2020 alone. By the fifth month of the year 2015, an average of around 93.5 million U.S. dollars on IoT devices will be spent by various industries. Hospitality sector, such as airlines and transportation spent about 129 million U.S. dollarswhich is considered to be the highest annual investor on Internet-of-Things.

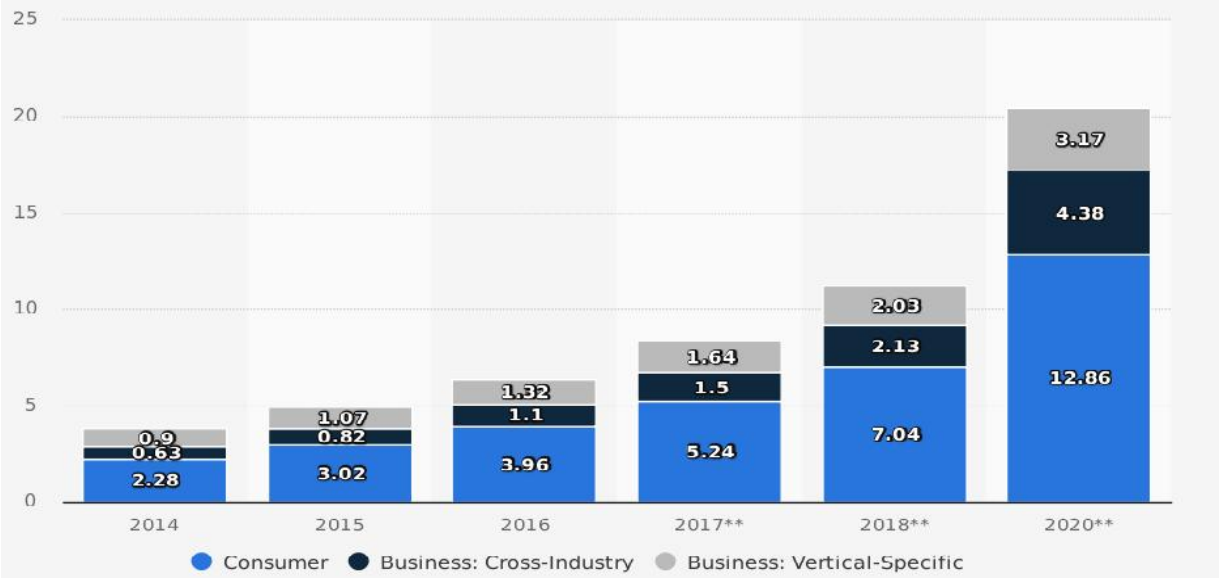
Manufacturing Industries, and financial sectorsare also spending big on IoT systems as seen in Table 3.3.

Table 3.3: IoT installed base by category 2014-2020

Year	Consumer	Cross-industry business	Capital-specific business
2014	2.28	0.63	0.9
2015	3.02	0.82	1.07
2016	3.96	1.1	1.32
2017	5.24	1.5	1.64
2018	7.04	2.13	2.03
2020	12.86	4.38	3.17

Source: Statista.com

The chart in Figure 3.3 shows a graphical illustration of the dataset in table 3.3 above.



Source: Statista.com

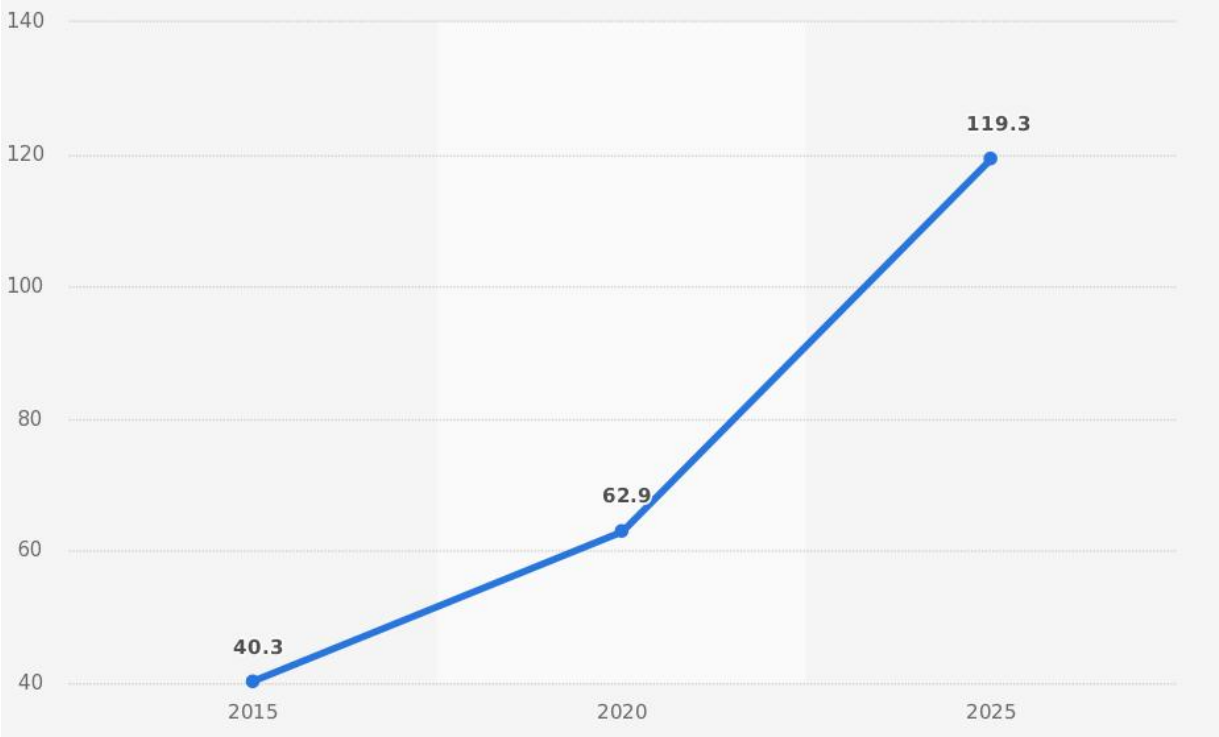
Figure 3.3: IoT installed based on category from 2014-2020

This research is more concentrated on the security review of the IoT security, we cannot talk about IoT security without reviewing the spending on the security of the devices involved. Enterprise spends billions of US Dollars in order to prevent data leak and all sort of security breach that could occur as a result of an attack on a single device on a connected network of devices.

Sometime in the year 2015, man-in-the-middle attack was implemented by two cyber securityprofessionalsto override a moving vehicle (e.g., controlling its air-conditioning, sound system, windshield wipers and brakes). In spite of the fact that it was planned, it showed the possibilitiesof the danger man-in-the-middle attacks could theoreticallyled to the recall of over 1.4 million vehicles which will, in turn, lead to loss of billions of dollars.

Also, a telecommunication and internet provider based in the UK was subjected to numerous cyber attacks in which clientsdata was leaked as because they werenot encrypted before they got to the cloud storage. It became possible for the attackersto easily access and steal several clients credit card and bank informations.

These show much reason why we need to strongly protect our devices without leaving one behind by installing several security units. The number of IoT units in the security industry is expected to increase over the years. It was at 40.3 million units in 2017, and it was expected that it would reach 119.3 million units by 2025, and since the security industry relies on a lot of automation of processes, utilizing IoT devices would be a huge step forward. The chart in fig 3.3 illustrates the units installed so far and the projected units to be installed up to the year 2025.



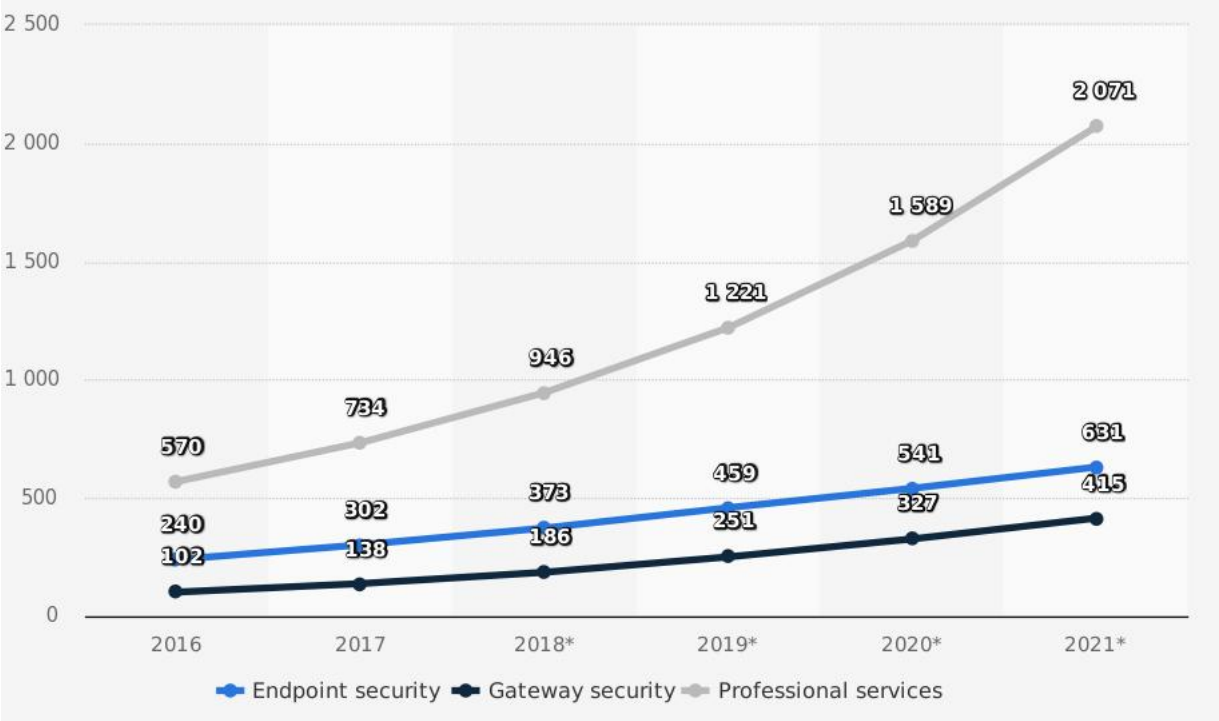
Source:statista.com

Figure 3.4: Security industry in the European Union (EU) units of installed devices in the year,2017, 2020 and 2025 (in million) respectively.

Several security measures have been put in place to ensure the safe use of IoT devices, measures ranging from procuring professional services to gateway security, to endpoint security.

More money is seen to be spent on professional security services as the quality of security they provide is seen to be top notch. In 2016, about 570 million US Dollars was spent on procuring professional security services it continues to increase as the number of connected device increases too, 2071 million US Dollars is projected to be spent on professional services alone by the year 2021, 631 million dollars on endpoint security and 415 million dollars on gateway security all in the year 2021.

Figure 3.4 shows the security spending in millions of US Dollars from 2016 and projected up till 2021.



Source:statista.com

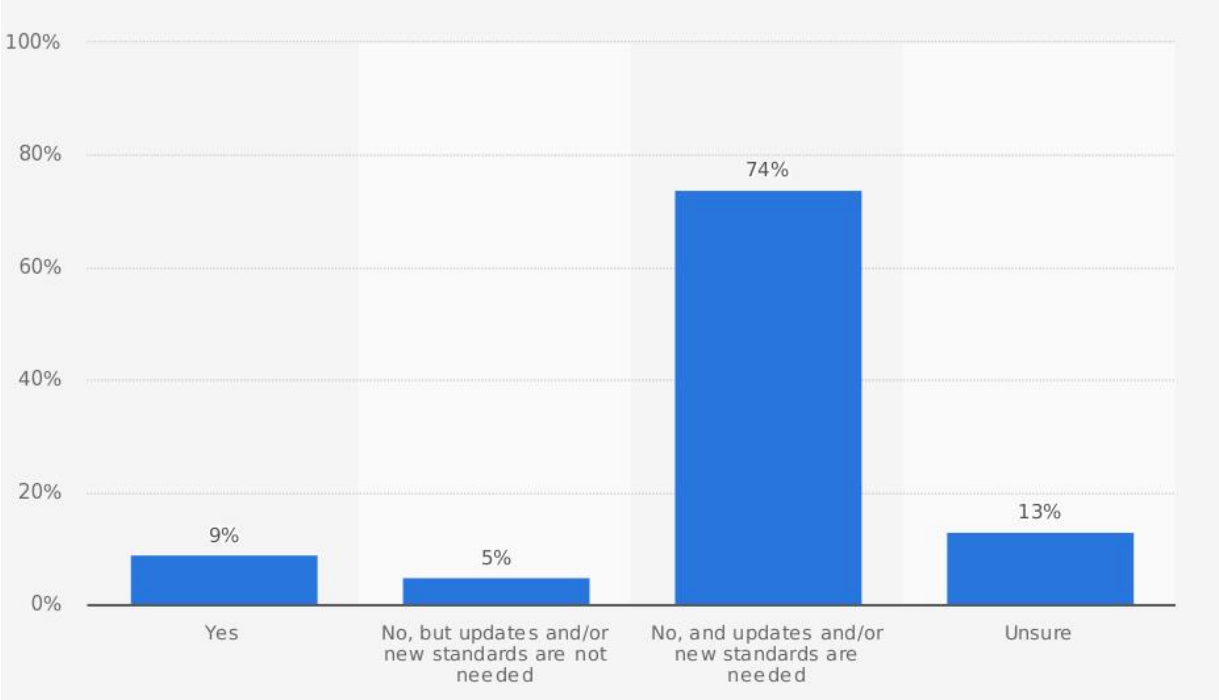
Figure 3.5: IoT world wide security spending analysis for a 5 years period from 2016 to 2021 in million US Dollars

After getting all these information about IoT and the need for improving it security, we decided to ask few more questions to get response from people suing IoT devices, but as a result of the difficulty in getting respondent from people that actually use this device, and also in order to get actual data, we picked our questions from an online pool which was already targeted at IoT device user. We came up with the following questions.

- Are thecurrent security mechanism in the industry efficiently addressing IoT?
- Are you certain that you can control the access to your datacaptured by IoT devices installed in your home?
- Is there a need for more security in connected devices

3.3.1 Arethe current security mechanism in the industry efficiently addressing IoT?

Sometime in2015, in the United Kingdom (UK) in. A nine percent share of respondents said: "No, but updates and/or new standards are not needed." The chart below shows the data according to the respondent.



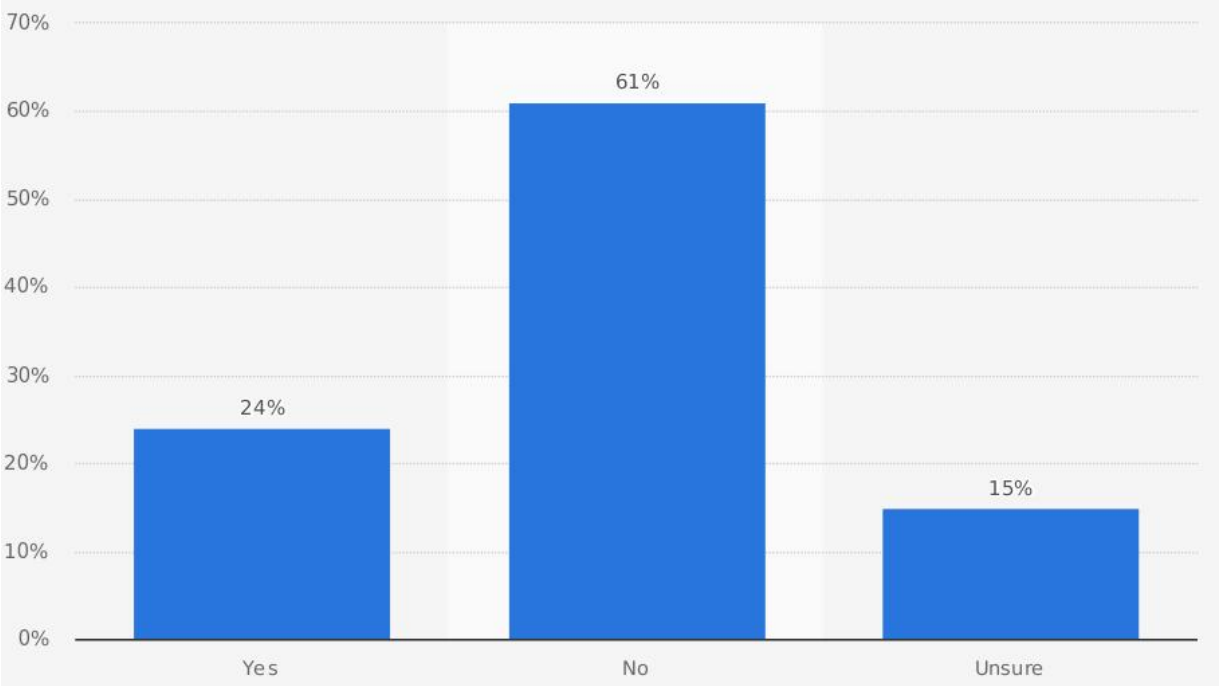
Source:statista.com

Figure 3.6: Response from IoT users about if existing standards in the industry adequately,

address IoT security issues

3.3.2 Are you certain that you can control the access to your datacaptured by IoT devices installed in your home?

A 24 percent share of respondents were confident they could control access to their device in their home. Of which, 61 percent don't agree that their device is totally secured from attackers as seen in Figure3.6.

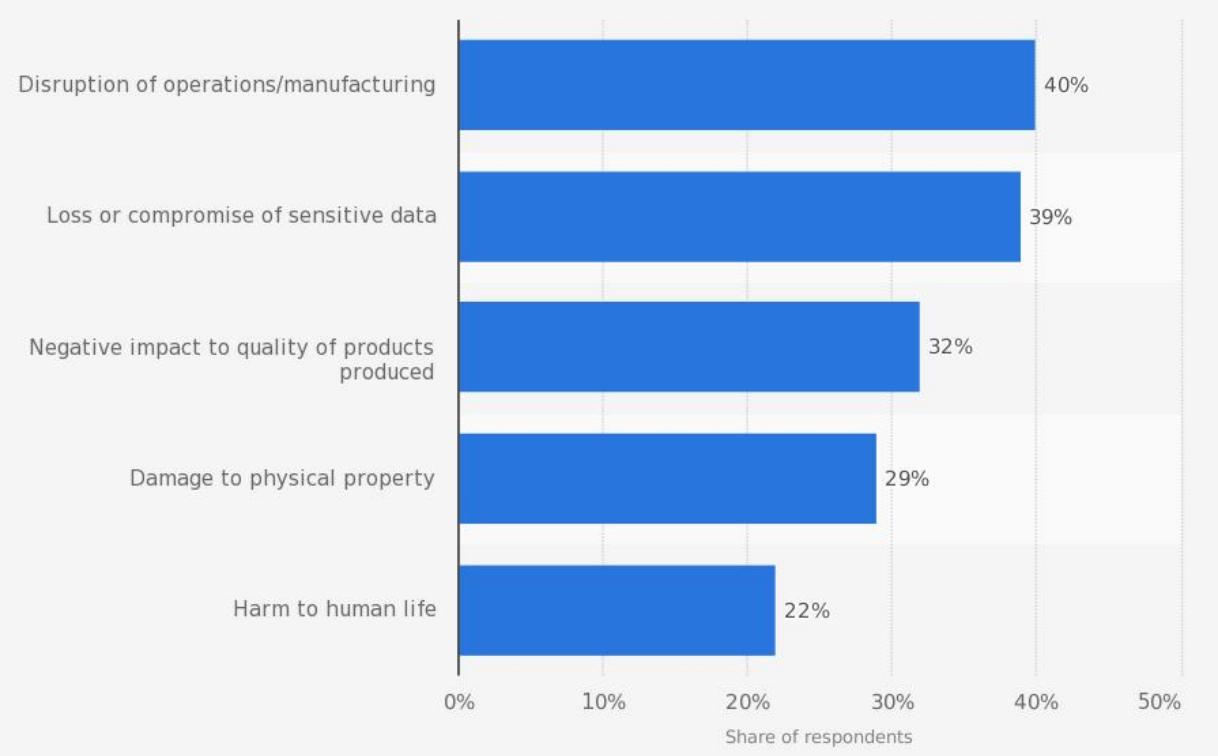


Source:statista.com

Figure 3.7: Response from respondents about control to access to information produced by, IoT devices.

3.3.3 Why do we need more security for connected devices

In 2017,40 percent of the respondents in a survey conducted by PWC revealed that successfulcyberattack would bring about the disruption of operations/manufacturing, 39 percent showed loss or compromise of sensitive data, 32 percent showed its negative impact. The graphical illustration of this response is below.



Source:statista.com

Figure 3.8: The anticipated result of successful cyber-attacks worldwide as at 2017

CHAPTER 4
BLOCKCHAIN AND IoT MODEL

Diversity IoT applications are numerous. It is fast remodeling the globe into a world, which allows computations to become “invisible” for the user, making the world more efficient and effective through human-machine relationship through its applications in businesses, lifestyle and the society as a whole..

The diagram in Figure 4.1 display several applications of IoT to real-world problems.

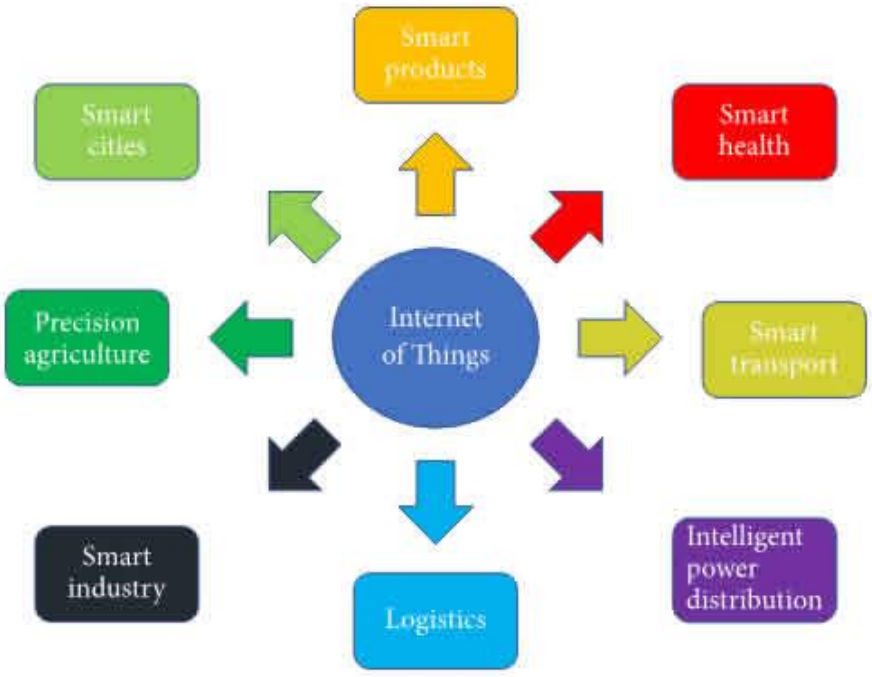


Figure 4.1: Applications of IoT

Examples of the work of IoT are:

Smart products: products purchased by consumers, such as smartphones, smart house, smart car, smart TV, and wearable.

Smart health: monitoring and controlling pulse during exercise and monitoring patients health condition in anywhere they are. This reduce health risk with a real-time capture of data from

patients body and also it improves diagnoses accuracy, hence treatment information and health-related services can be received by patients remotely and almost immediately (Reshmi, 2018)

Intelligent transport: Notification of traffic information, intelligent control of routes, remote tracking of vehicle, highways coordination, and integration of intelligent platforms.

Smart Grid (smart power distribution): observation of energy installations, smart substations, power distribution, and remote measurements of residential power meters.

Smart industry: Saving enegry, pollution observation, providing industrial safety, managing products life-cycle, fire and gas leak alarm, managing of goods supply, environmental conditions observations, and control of production processes.

Quality agriculture: Management of precisions, observation of production and cultivation environment, and also management of production process.

Smart cities: observation of structures, and situations of materials used in constructions.

Security: access control, fire control, and alarm systems.

4.1 Blockchain and IoT model architecture

The initialization process of IoT device is first outlined, followed by understanding the process of transactions. In order to ensure authorised control and access to IoT devices and its data, a local blockchain is used. Then, unalterable time-ordered records of transactions that are related to the defined services is then generated by the blockchain. The design security arose as a result of various features including various transaction structure involving the smart home ,overlay, and indirectly connected device access. Qualitative arguments is provided to show the level of confidentiality, integrity, and availability that the smart home tier achieves and also explain how security attacks such as Distributed Denial of Service (DDOS) and linking attack could be mitigated.

The overall proposed structure depends on stratified structure and distributed trust to ensure security and privacy without compromising it suitability for defined requirement of IoT.

These architecture is divided into 3 namely

Smart Home

Overlay Network

Cloud Network

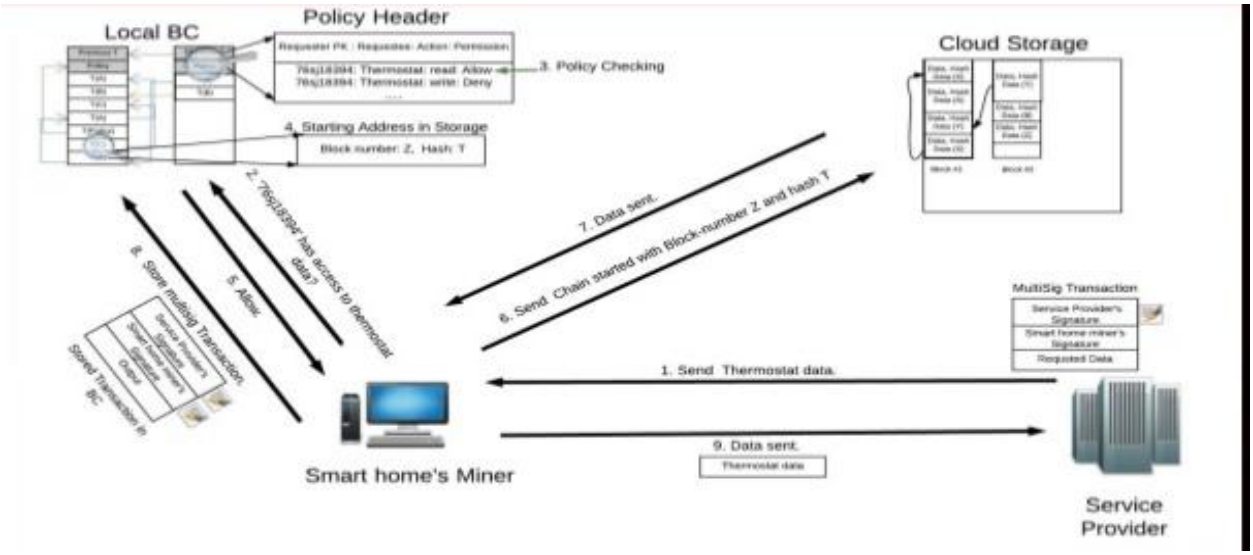
4.2 Smart home

The smart home is another product IoT which is related to a smart city but with focus on user-orientation and geographical limitation (Mathieu, 2016). The smart home allows the home owners to manage many internal functions in their home even from outside the home. Activation, deactivation and control of all devices are made possible without having to be physically present at home. Since our desire case study is securing smart home devices with blockchain technology, we have to look into the core components of smart homes, i.e. the devices involved.

4.2.1 Transactions

A transaction can be defined as a small unit of the task that is stored in public ledger. These records also known as blocks. These blocks are executed, implemented and stored in blockchain only after the validation by all nodes involved in the blockchain network.However, there exist several transactions involved in a blockchain backed smart home with a different function.

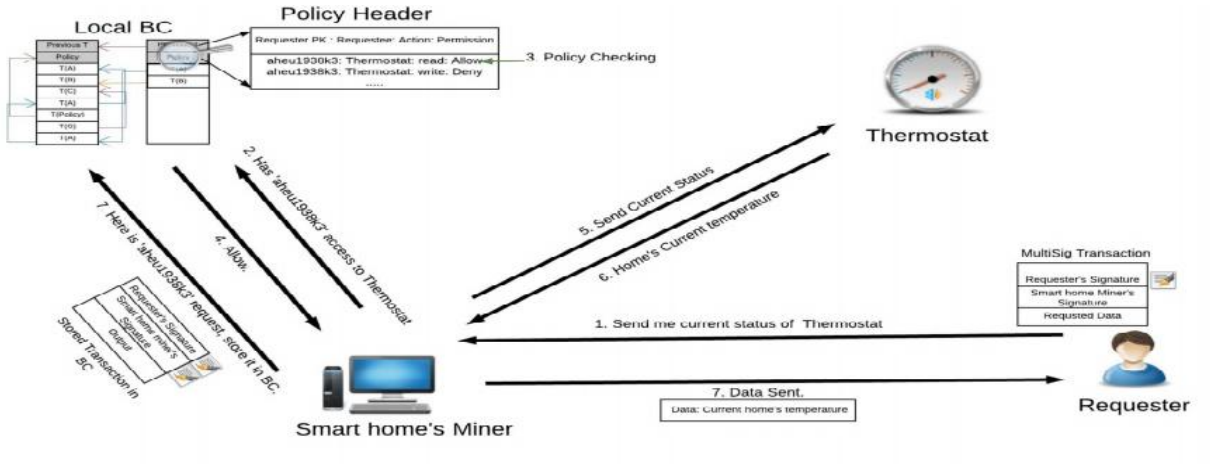
*Access Transaction*is created by a smarthomeowner in order to access the cloud storage as shown in Figure 4.2.



Source: allquantor.at

Figure 4.2: Access Transaction

Monitor Transaction is generated by a homeowner for periodic monitoring of each device information as shown in Figure 4.3.



Source: allquantor.at

Figure 4.3: Monitor Transaction

Genesis Transaction is implemented in including a new device to the smart home(Decker and Wattenhofer, 2013) while *remove transaction* is the one implemented in removing a transaction from the smart home.

The concept of shared keys and digital signature is used to secure communication of all the resources and transactions on the network. The concept of public key cryptography is applied in generating requester and the requestee keys. A public key that can be shared and a secret that only the owner has access are created. The entire transaction requires the verification of resources ownership before it can be considered valid after which transactions are saved in the local private blockchain.

4.2.2 Local Blockchain

A local private blockchain records all incoming and outgoing transactions in each device in the smart. Right from the Genesis transaction, transactions done by the devices are attached together in chains as an unchangeable ledger on the blockchain network. Each of the block contains a block header which keeps the record of the previous block to ensure immutability and also a policy header that ensures device authorization and also to enforce homeowner defined. These makes use of four parameters namely;

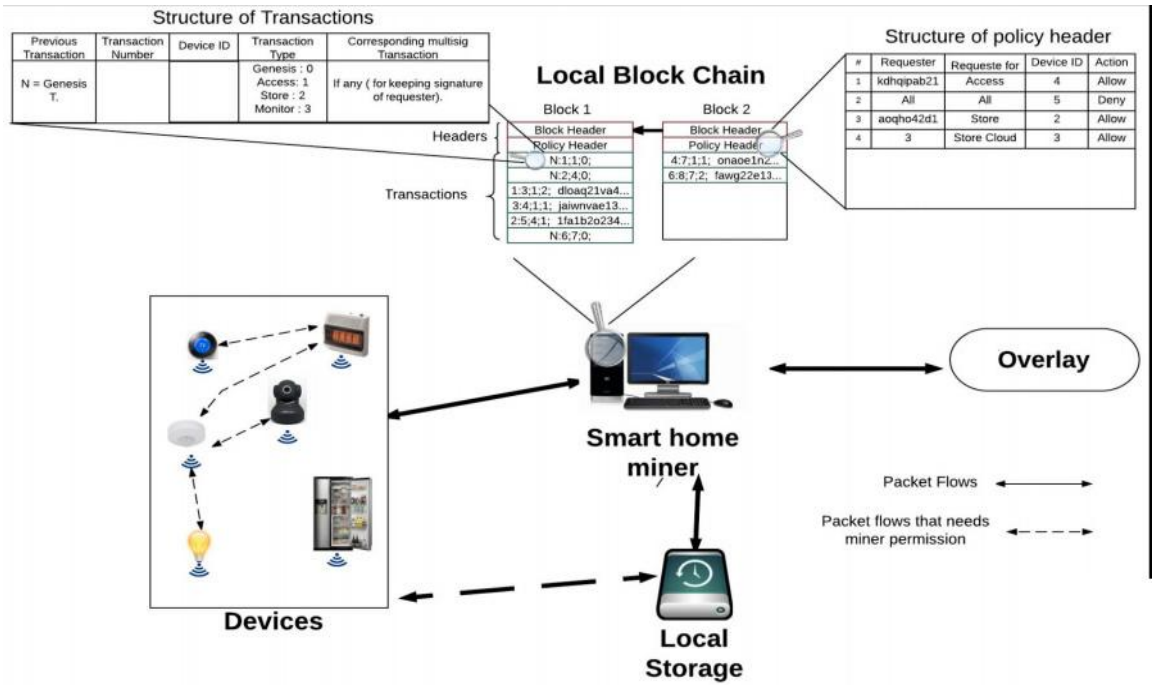
Requester: This is the public key (PK) requesters in the overlay transaction.

Requested Action: Action between the store data locally and on the cloud, access stored data and monitor real-time access to a particular device.

ID: The device identifier or unique key in the smart home.

Action Flag: Used in acceptance and denial of requested action.

Figure 4.4 shows an overview of the smart home which involves an IoT device, miner, storage, andblockchain.



Source: allquantor.at

Figure 4.4: Smart home overview (Devices, Miner, Storage, and Blockchain)

A number of transactions is contained in each block aside the block header and the policy header. Five parameters are stored in each transaction on the blockchain, of which the *previous transaction and transaction number* parameters respectively are used in chaining transactions done by the the device to each other, also in order to be able to identify each

transaction exceptionally in the blockchain. A corresponding device *transaction ID* is saved into its third column.

Transaction types which were discussed earlier i.e store, access and monitor will be inserted into the fourth while the returned *corresponding transaction* from the overlay network is saved in the last field, otherwise,it's left blank if nothing is returned.

The smart home miner maintains and manage the local blockchain.

4.2.3 Home miner

All incoming and outgoing transactions are centrally processed by the smart home miner. The miner could be integrated with a stand-alone device or even the home internet gateway as the owner wishes. All the transactions are recorded into a block by the miner and chains the full block to the blockchain. Its computing power is used as an edge on bookkeeping right for the next block (Zheng, 2017).

The miner encrypts every transaction going back and forth using Secure Hashing Algorithm (SHA256), which is a cryptographic measure used in hashing values, it always produces fingerprint hash values of length 256 bits, SHA256 is considered as one of the most efficient ways to ensure data integrity, it gives data a unique fingerprint. A hash function is a one-way function, f(x) = y, that takes data of any length, x, and has a seemingly random but unique mapping to a specific fingerprint hash value, y. For a hash function to be regarded secure, three properties need to be ensured Douglas (2006).

- Pre-image resistance – Assumed fingerprint y, it should be hard to find data x so that f(x) = y.
- Second pre-image resistance - Assumed data x, it should be difficult to find another data x^0
  where $x \neq x^0$ so that $f(x) = f(x^0)$.
- Collision resistance - Given the hash function f() it should be hard to find two different datasets x, $x^0$where $x \neq x^0$ such that $f(x) = f(x^0)$.

The miner generates genesis transactions, distributes and update the keys, changes the structure of the transaction and also forms and manage the clusters formed. Furthermore, the miner manages the local storage in order to provide additional capacity.

4.2.4 The local storage

Local storage can be defined as a backup drive on which datas by smart home devices can be stored locally. The data are saved in the queue using the First in First out (FIFO) in a chained ledger to the starting point of a specific device. The device storage could be linked with the home miner or implemented as a stand-alone device.

4.3 The overlay network

These is similar to the network having various nodes which could be smart the home miners, home owner smartphone or computer. Individual node o the network uses the TOR to ensure anonymity at the IP layer on the overlay network. A user may have multiple nodes in the overlay network, but in the nodes could be arranged into clusters so as to reduce network overhead, furthermore, a Cluster head (CH) is chosen among the clusters grouped. These clusters can be changed if excessive delays are being experienced, also, the nodes in the cluster can change the cluster head at any time.

Each cluster head decides whether or not to maintain a new block independently depending on its communication with the participants of the received transactions. Although, discovering a particular block or transaction causes a high delay in some cases, in a situation where a user has multiple home to manage at a time, a shared overlay consisting of high resources device can be formed in the multiple homes with each device chaining its a starting transaction to its parent starting transaction.

Each of the cluster head(CH) contains:

Public Keys of Requesters: These allow access to data for the smart home connected to this cluster.

Public Keys of Requestees: These allow access to the smart homes connected to this cluster.

Forward List: These contains the the transactions sent for other cluster heads in the network.

4.4 Cloud storage

If the Smart Home wants to make use of the services provided by a third party service provider, he may decide to store some of his device data in cloud storage and then allow access to a particular data set in that storage to the service provider. The Smart Homeowner defines both of these policies in the Policy Header of his local blockchain. The cloud storage groups users data in identical blocks associated with a unique block-number which is used together with the hash for authentication of the data stored by the user. In order to ensure that only the authentic key owner knows the specific block number, after storing the data using a shared key derived from generalized Diffie-Hellman algorithm the new block-number is encrypted. Collision-resistant hashes are used to ensure that only the authentic owner have information about the specific block-number, hence, it can be said that no other person other than the authentic owner can retrieve her data, also fresh data are chained to an existing record. It is important to note that for each device of the user, different record of data can be created in storage or a single common ledger for all of its devices. If the user wishes to provide access to all data of a particular device to a service provider, the former is particularly useful for that.

4.5 Transaction handling

After understanding the Blockchain and IoT convergence general topology, and also its security and privacy architecture. We will look into how transactions are being handled on the network.

As discussed earlier, we have three types of transactions, namely, storing, accessing and monitoring.

4.5.1 Storing

As explained in the architecture earlier, each device in the smart home can either store data locally or store it on the cloud. For instance, let’s assume our smart homeowner already created a cloud storage facility and have set up the device to upload data to this facility. The

device data will be sent to the miner, permission and authentication will be checked by extracting the previous block details and then create a random ID which is attached to the data to be stored.

The storage in turn also validates the transaction with the ID as no two nodes can have the same ID, and check for the cloud storage space availability first. If space is sufficient, the hash of the received data packet is being calculated and compared with the hash received, in a case where they match, it stores the data on the cloud storage and returns an encrypted new block encrypted with the shared key to the miner.

To ensure that and alteration or modification of the user data is visible to all, the cloud signs the hash and send it to the overlay network for processing. But in a case where data are stored locally, the ID is not needed as all transactions are being carried out within the smart home.

When more than one home is been owned or controlled by an individual, each of the home has its own miners and storage. The device in the same home with the miner will experience no change but the device at the other home communicates through a Virtual Private Network (VPN) between internet connectivity in each home and miners of the shared overlay that routes the packets to and from the shared miner.

4.5.2 Accessing

The stored data stored on the cloud will need to be made available to the service provider in order to provide certain service. To access such data, a transaction is created which will need to be authorised by the service provider, then also the home based miner to be validated by the cluster head which checks if the public key exists both in the requester and the requestee, if it does, the transaction will be broadcasted to its own cluster, otherwise it will be sent to another cluster head and the public key be put in a forward list.

When an access request is sent to the miner, it will, first of all, check its local blockchain to see if the user has pre-granted such requested data to the service provider. After sending the requested data to the service provider, the local blockchain records the transaction and also

random cluster heads will be stored in the overlay network to serve as an evidence that the requested data was sent by the user home miner.

This can also be used to notify other nodes in case of a policy breach. All participating nodes or cluster head in a transaction record their activity.

All nodes want to know is the metadata of the system : what has been read, the units used, the corresponding machine, etc. This can be stored and managed separately from the readings as seen in Figure 4.5 .


```
{
    "device": "63722f53-c0dd-4e17-bc14-a22aa49315a2",
    "event_time": "2017-07-12T12:16:47.000Z",
    "source": "oberwil-26",
    "Datetime": "2017-07-12T14:16:47",
    "Status": "mpp-track",
    "DC Voltage 1": 474.8,
    "DC Current 1": 14.87,
    "DC Power 1": 7064,
    "DC Voltage 2": 499.4,
    "DC Current 2": 15.29,
    "DC Power 2": 7641,
    "DC Voltage 3": 511.1,
    "DC Current 3": 10.76,
    "DC Power 3": 5500,
    "AC Voltage 1": 236.1,
    "AC Current 1": 27.04,
    "AC Voltage 2": 236.1,
    "AC Current 2": 27.32,
    "AC Voltage 3": 236,
    "AC Current 3": 27.17,
    "DC Power": 20207,
    "AC Power": 19951,
    "Cos Phi": "0.993i",
    "Temperature": 46,
    "Daily Energy": 63565
},
```


Figure 4.5: A sample meta data and its content

4.5.3 Monitoring

Smart home devices cannot be said to be secured if the homeowner cannot monitor the activities at the real time. The monitoring transaction allows the miner to request data either on interval on continuously as preferred by the user e.g. camera feed, motion detector, fire alarm etc

4.6 Security evaluation

Confidentiality, Integrity, and Availability are the major requirements needed to be addressed by any security design, to ensure that only authorized user to have access to data, to ensure transfer and delivery of data when needed without it being altered.

This approach effectively secures the devices in the smart home by ensuring that they cannot be reached directly but rather, all transactions have to pass through a third party device called miner which authorize all transaction before forwarding them to the devices.

Although there is an increase in transaction delay compared to the existing smart home gateway products, these delays occur as a result of authenticating the user, generating a shared key, matching of keys etc. but this delay doesn't have a negative impact on the availability of the device.

The table below shows how this research achieves the aforementioned security requirements.

Table 4.1: Security Requirements Evaluation

Requirements	**Actions**
Confidentiality	Achieved by using symmetric encryption.
Integrity	Hashing the shared keys is used to achieve integrity.
Availability	Limiting the number of transaction accepted by the devices and the miner will help in achieving this.
User Control	Accomplished by saving datas in the blockchain.
Authorization	The usage of policy header and shared keys.

Two dangerous security attacks that are common to smart homes were analyzed, the Distributed Denial of Service Attack (DDOS), the form of attack where hackers make use of an infected IoT device to hijack a particular targeted node and Man-in-the-middle attack in which an attacker hijack the ledgers that have the same public key and use it to get the identity of user.

4.6.1 Distributed Denial of Service Attack (DDOS)

A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or another network resource, and cause a denial of service for users of the targeted resource(David and Ruby, 2001).

Our approach have multiplelayers of defense, the first makes it difficult for a hacker to install a malware directly on devices since it can't be accessed directly as all transaction has to pass through the miner.

Another layer of defense is for instance if the attacker breaks the first and managed to infect the devices. All outgoing traffic will need to be examined by the policy header for authorization and since the DDOS attack request will not be authorized by the miner, their would be no exit on the network.

Man-in-the-middle attack

The man-in-the-middle concept is where an attacker interrupts and breach communications between two separate systems as the name implies by hijacking communications from the middle before it gets to the intended destination (Meyer & Wetzel, 2004).

This attack endangers privacy. It can be a dangerous attack because when the attacker secretly intercepts data ledgers with the same public keys, they are made to believe that the communication is going on directly between devices whereas, the attacker is already compromising by revealing the ID of the user.

To curtail this type of attack, a unique key is used to store each data, the miner generates a unique ledger of data for each of the device and stored on the cloud using the different public key. A unique key is used by a miner for each transaction.

4.7 Evaluating performance

There will be a slight increase in the data and computational overhead on the smart home devices and miner according to this approach as a tradeoff for improved security and privacy (Dorri et al, 2017).

The data overhead will increases a result of the encryption and hashing mechanism involved, but these have a minimal effect on the device performance as against the existing system which only requires username and password just to the dashboard.

Transaction process time increases too as more time will be required in order for data to undergo encryption, hashing and storing to the blockchain operations because several encryption will be done as against single encryption done in existing system.

Also, energy consumption increases as the miner are the major consumer of more energy due to the task is done by this device.

CHAPTER 5

PROPOSED DECENTRALISED MODEL

Asymmetric **keys**, also known as public/private key pairs, are used for asymmetric encryption. Asymmetric encryption is used mainly to encrypt and decrypt session keys and digital signatures.

In this chapter, a prototype of how the SHA256 is used in generating a private key and public key which will be used in signing a transaction.

5.1 Public / Private key pairs

The private key is known only to the smart home owner while the public key is the one displayed. These transactions are verified by the miner after it has been signed, in order to verify if the private key in the blockchain correspond with the public key and the signed transaction.

The diagram below shows how public and private keys are been generated using SHA256.

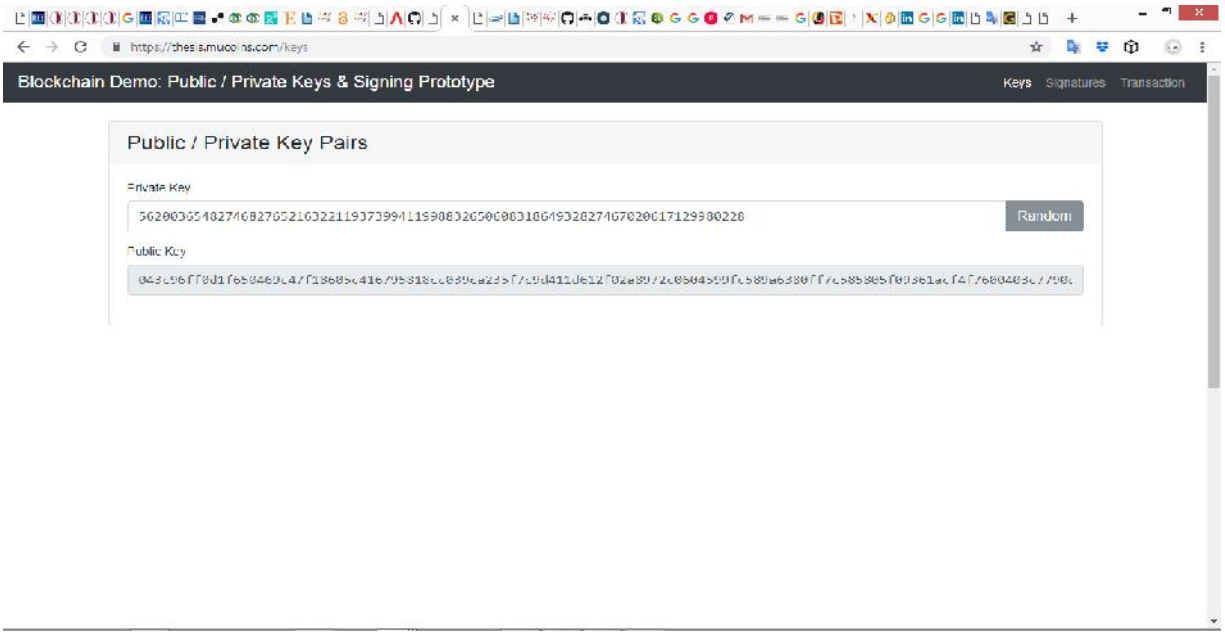


Figure 5.1 Public / Private Key Signing.

Also, the diagram below displays how the generated private key and public are used in signing transactions.

5.2 Signature

All transactions in the blockchain network are signed by the home owner using the private key generated. If there is any slightest change in the coded message or any part of the transaction, the transaction will be nullified. In Figure 5.2 below, the signing of transactions is being displayed.

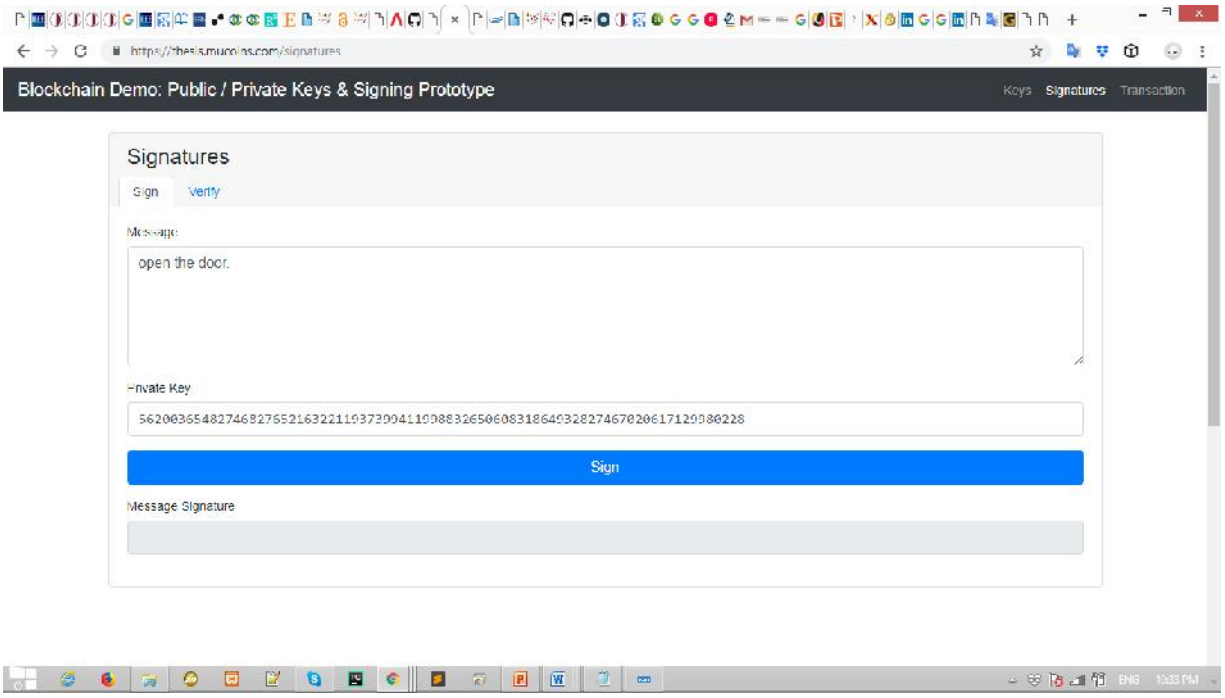


Figure 5.3 Signature Signing

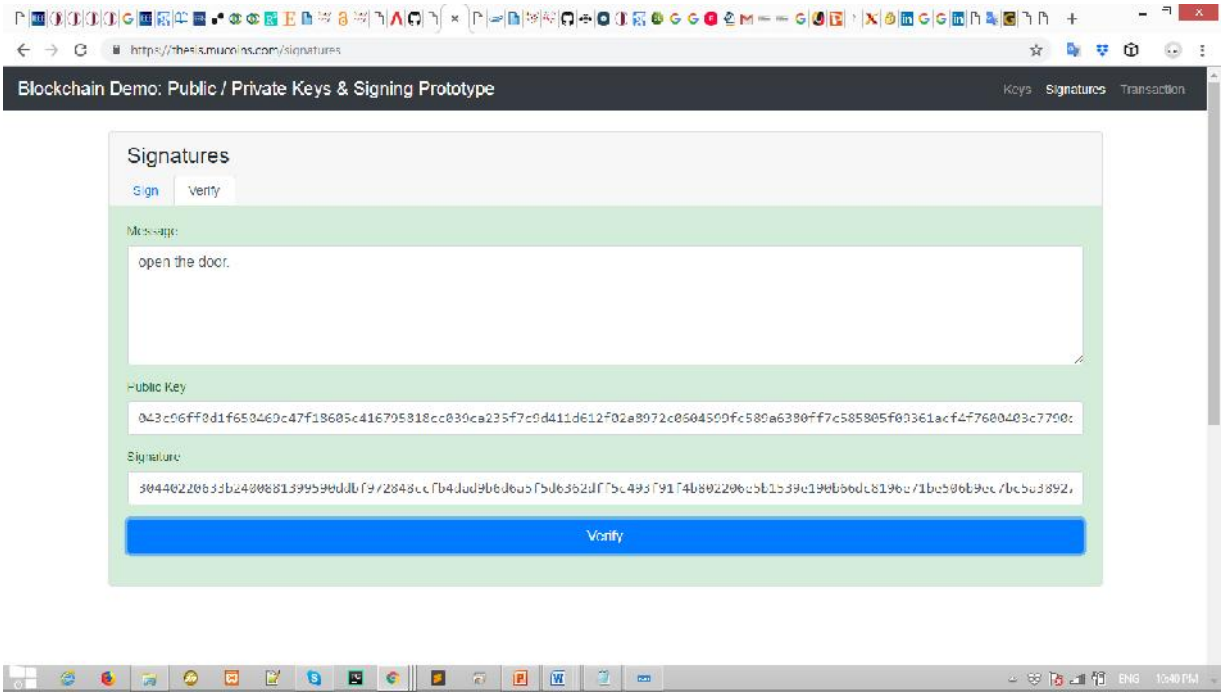


Figure 5.4 Signature Verification

In the above diagram, the background shows green when the verification is successful while it shows red when verification fails.

5.3 Transaction

This displays how this prototype combines the public key / private key generated to the transaction signing and verification as shown below.

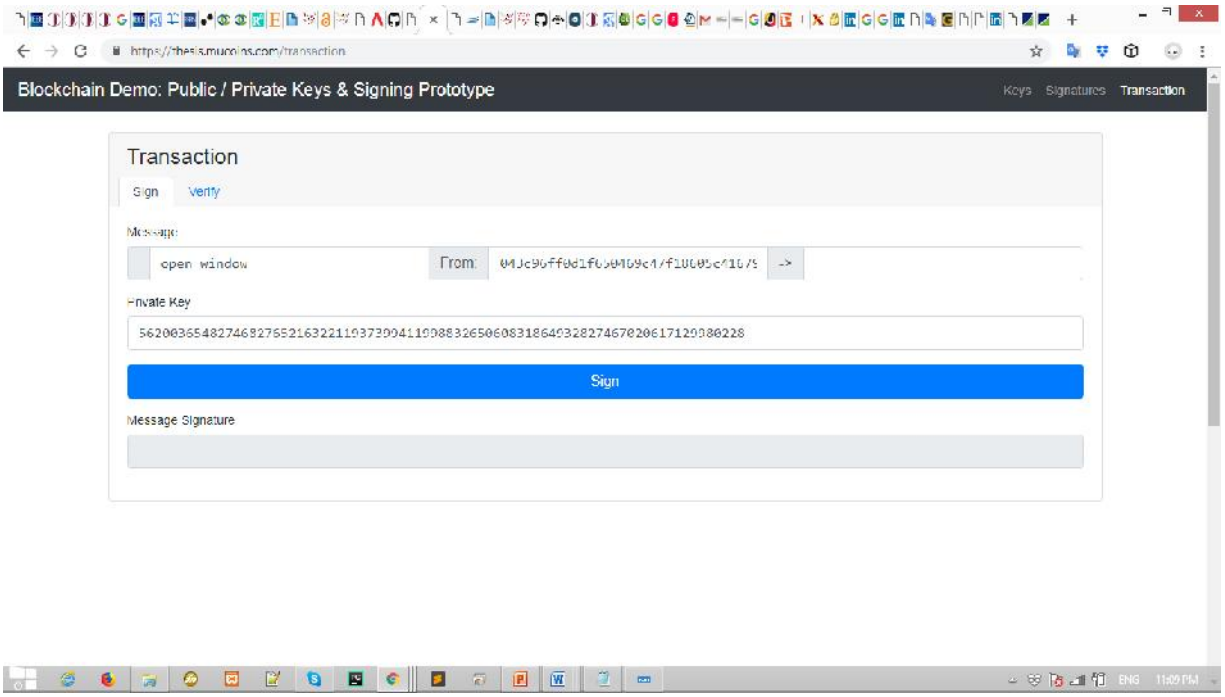


Figure 5.4 TransactionSigning

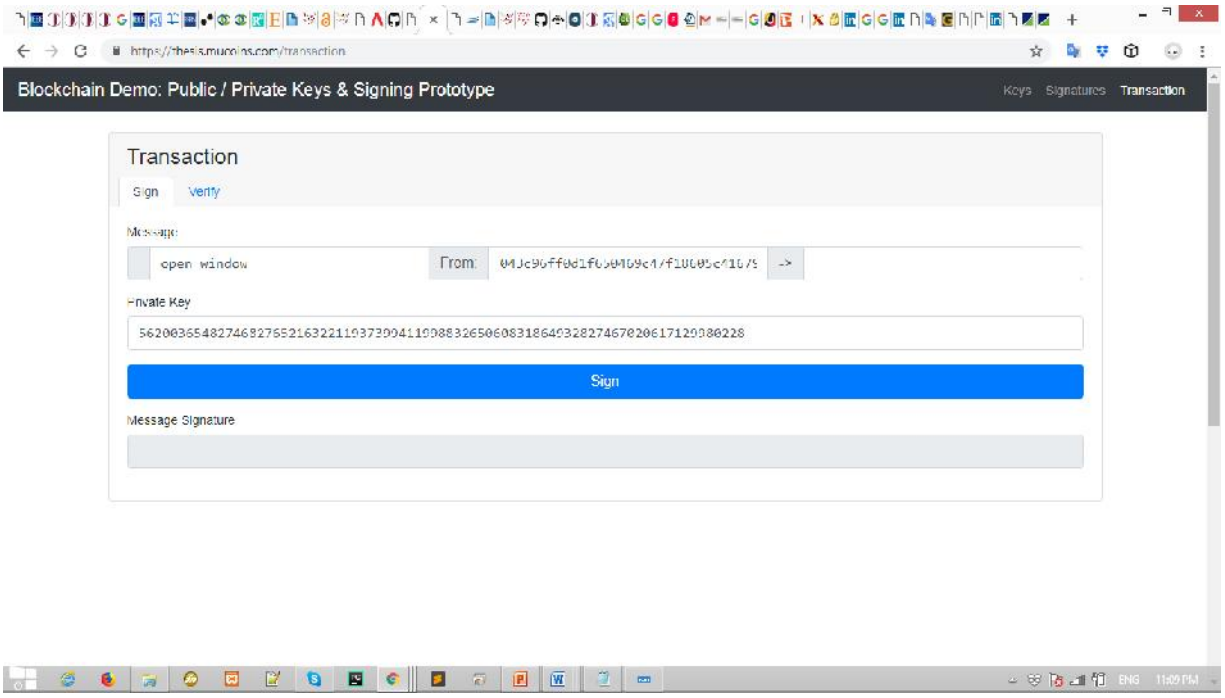


Figure 5.5 Transaction Verification

The miner authenticates each transaction to ensure the integrity and make sure the transaction is from an authorized owner, which is the major aim of making use of blockchain.

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

Due to its decentralised nature, blockchain integrity have been tested and implemented upon bitcoin and its gaining fast reputation in the IoT ecosystem. blockchain major building block is its distributed ledger and public key encryption which is promising in the IoT sector for data monitoring.

IoT underlaying architecture was discussed, its growth and impact on the society, damages that could be caused when not appropriately used, the need to improve its security, and investment of different sectors into iot security was also looked in.

It is concluded that blockchain due to its integrity and its incorruptible ledger mechanism will adequately ensure safety against attack on IoT systems. The hashing algorithm used by current system for encrypting passwords isn't efficient enough to mitigate modern attacks, as not only user authentication should be required to have access, control data and transaction involved in the interoperability of various connected devices but also the transactions should be assigned a public key that will be signed and authorized with a secret key known only to the user and get verified before access and control will be granted.

6.2 Recommendations

These research contribution can be summarized by mentioning that the adoption of IoT increases daily and its growth among sectors is also growing steadily, with this comes a need for effective security to prevent data leakage and hijack, by making use of a distributed network such as blockchain will improve the security of IoT devices by effectively using miner to hash and encrypt all outgoing and incoming transactions.

By scrutinizing all transaction and rejecting the rogue connection, attacks such as (DDoS) Attack and other data and access breach attack can be mitigated and hence IoT users can worry less about data leak, device hijack and other forms of attack.

Also, it can be said that the savings factor of IoT devices surveyed in this thesis is centered on the security feature provided by the miner and the blockchain, however, it will be beneficial to look into the details of the hashing algorithm used by the miner which is based on double-hashing SHA256 and how effective SHA256 is. But due to time constraint, this thesis is more of a theoretical approach towards studying and review of how blockchain can be implemented for effective security of smart devices.

Future research work will be suggested to research into the working algorithm of SHA256 used by the miner to encrypt data and transactions and also optimization of this algorithm to produce exact or higher computational hashing while reducing the time spent and power consumption.

REFERENCES

Ashton K. (2009). That 'Internet of Things' Thing. RFID Journal. (Vol 22, pp. 97-114).

Boosting security with blockchain and IoT,Retrieved October 11, 2018 from https://eastwestpr.com/boosting-security-with-blockchain-and-iot/

Chakravorty A, Wlodarczyk T, and Rong C,(2013). "Privacy-preserving data analytics for smart homes," in Security and Privacy Workshops (SPW), IEEE,(pp. 23–27).

David K, Ruby L, (2001) "Remote Denial of Service Attacks and Countermeasures," Princeton UniversityDepartment of Electrical EngineeringTechnicalReport CE-L2001002.

Decker C, Wattenhofer R (2013) Information propagationin the bitcoin network. In: 13th IEEE internationalconference on peer-to-peer computing (P2P), Trento.

Deloitte. (2017). AI and you Perceptions of Artificial Intelligence from the EMEA financial services industry.Retrieved October 11, 2018from https://www2.deloitte.com/it/it/pages/financial-services/articles/ai-and-you---deloitte italy---financial-services.html.

Douglas R. (2006). Cryptography, Theory and Practice, Thirdedition.Ed. by Kenneth H.Rosen. 3rd ed. Chapman & Hall/CRC,

Dorri A, Kanhere S, and Jurdak R, (2016)"Blockchain in internet of things:Challenges and solutions," arXiv preprint arXiv:1608.05187,.

Distributed denial of service (DDoS) attack, Retrieved October 18, 2018 from https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

Gartner. (2014). 4.9 Billion Connected" Things" Will Be in Use in 2015. Retrieved 18th October, 2018 fromhttps://www.gartner.com/newsroom/id/2905717

King S, "Primecoin: Cryptocurrency with prime number proof-of-work," Retrieved July 7th, 2013 from http://primecoin.io/bin/primecoin-paper.pdf .

Kitchenham B, Charters S.(2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering.

Kolias, C.; Kambourakis, G.; Stavrou, A.(2017).; Voas, J. DDoS in the IoT: Mirai and other botnets Computer malware. v50, pp 80–84.

Legg, S; Hutter, M. (2007). A Collection of Definitions of Intelligence. arXiv:0706.3639 .157, pp 17-24.

Meyer, U., & Wetzel, S. (2004). A man-in-the-middle attack on UMTS. In Proceedings of the 3rd ACM workshop on Wireless security(pp. 90-97). ACM .

M.Fernández-Caramés T, Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access, 6*, 32979-33001.

Nakamoto S,(2008) "Bitcoin: A peer-to-peer electronic cash system," SSRN Electronic Journal.doi: 10.2139/ssrn.3065723

Narayanan A, Bonneau J, Felten E, Miller A, and Goldfeder S (2016), Bitcoin and cryptocurrency technologies. Princeton University Press.

Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal, 5*, 1184-1195.

Petersen K, Feldt R, Mujtaba S, Mattsson M.(2008). Systematic Mapping Studies in SoftwareEngineering. In: Proceedings of the 12th International Conference on Evaluation andAssessment in Software Engineering. EASE'08. Swinton, UK: British Computer Society;. p. 68–77. Retrieved on 27th December from: http://dl.acm.org/citation.cfm?id=2227115.2227123.

Presser, M., Gluhak, A., (2009). The Internet of Things: Connecting the Real World with the digital World, EURESCOM mess@ge – The Magazine for Telecom Insiders 2.

Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M.(2018) On blockchain and its integration with IoT Challenges and opportunities. Future Generation Computer Systems, 88, 173–190.

Reshmi.S, Kannan Balakrishnan. (2018) Empowering chatbots with business intelligence by big data integration.

Roman R, Zhou J, and Lopez L, (2013)"On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279.

Samaniego, M.; Deters, R.(2016) Blockchain as a Service for IoT. In Proceedings of the 9th IEEE International Conference on Internet of Things, Chengdu, China, 15–18; pp. 433–436

Sicari S, Rizzardi A, Grieco L.A,and Coen-Porisini A,(2015) "Security, privacy and trust in the internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164.

Sun, J.; Yan, J.; Zhang, K, (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities.

The Convergence of Blockchain and IoT: Opportunities, Challenges and Solutions, Retrieved on 28th December 2018 from http://ieee-iotj.org/wp content/uploads/2018/03/CFP_SI_IOTJ_BlockChain.pdf

Tor Project. [Online]. Available: https://www.torproject.org/.

Understanding IoT Security – Part 2 of 3: IoT Cyber Security for Cloud and Lifecycle Management,Accessed on 18th December 2018 from https://iotanalytics.com/understanding-iot-cyber-security-part-2/.

United Nations, World Urbanization Prospects: The 2014 Revision, Highlights (ST/ESA/SER.A/352), Dept. of Economic and Social Affairs, ISBN: 978-92-11515176, pp. 1–32, 2014.

Yiyun Z, Meng H, Liyuan L, Yan W, Yi L, Ling T. (2018).Improving IoT Service In The Smart Home Using Blockchain Smart Contract.In Proceedings of the 11th IEEE International Conference on Internet of Things (iThings 2018), Halifax, Canada.DOI: 10.1109/Cybermatics_2018.2018.00047

Zibin Z, Shaoan X, Hongning D, Xiangping C, and Huaimin W. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.

APPENDIX

SOURCE CODE

Blockchain.js source code

```
var difficulty = 4;        // number of zeros required at front of hash
var maximumNonce = 500000; // limit the nonce to this so we don't mine too long

// NOTE: Because there are 16 possible characters in a hex value, each time you increment
// the difficulty by one you make the puzzle 16 times harder. In my testing, a difficulty
// of 6 requires a maximumNonce well over 500,000,000.

//////////////////////////
// global variable setup
//////////////////////////
var pattern = '';
for (var x=0; x<difficulty; x++) {
  pattern += '0';
}

//////////////////////////
// functions
//////////////////////////
function sha256(block, chain) {
  // calculate a SHA256 hash of the contents of the block
  return CryptoJS.SHA256(getText(block, chain));
```

```
}

function updateState(block, chain) {
  // set the card background red or green for this block
  if ($('#block'+block+'chain'+chain+'hash').val().substr(0, difficulty) === pattern) {
    $('#block'+block+'chain'+chain+'card').removeClass('card-error').addClass('card-success');
  }
  else {
    $('#block'+block+'chain'+chain+'card').removeClass('card-success').addClass('card-error');
  }
}

function updateHash(block, chain) {
  // update the SHA256 hash value for this block
  $('#block'+block+'chain'+chain+'hash').val(sha256(block, chain));
  updateState(block, chain);
}

function updateChain(block, chain, txCount) {
  // update all blocks walking the chain from this block to the end
  for (var x = block; x <= 5; x++) {
    if (x > 1) {
      $('#block'+x+'chain'+chain+'previous').val($('#block'+(x-
1).toString()+'chain'+chain+'hash').val());
```

```
    }
    updateHash(x, chain);
    if (txCount)
      for (var y=0; y<txCount; y++)
        verifySignature(block, chain, y);
  }
}

function mine(block, chain, isChain) {
  for (var x = 0; x <= maximumNonce; x++) {
    $('#block'+block+'chain'+chain+'nonce').val(x);
    $('#block'+block+'chain'+chain+'hash').val(sha256(block, chain));
    if ($('#block'+block+'chain'+chain+'hash').val().substr(0, difficulty) === pattern) {
      if (isChain) {
        updateChain(block, chain);
      }
      else {
        updateState(block, chain);
      }
      break;
    }
  }
}
```

Index.pug source code

```
extends layout


block content
  .container
    br
    br
    br
    br
    h1 BLOCKCHAIN APPLICATION TO IOT: A SECURITY SURVEY
    .h1 Public / Private Keys &amp;amp; Signing Prototype
    br
    p.pull-right by
      a(href='http://abc.com/') Sodruldeen Mustapha
      | Submitted to the Department of Software Engineering in Partial fulfillment of the Requirements for the Degree of Master of Science in Software Engineering.
```

Transaction.pug

```
extends layout


block content
  .container
    .card
```

```
.card-header

  h4 Transaction

  ul.nav.nav-tabs.card-header-tabs#myTab(role='tablist')

    li.nav-item

      a.nav-link.active#sign-tab(data-toggle='tab', href='#sign', role='tab', aria-controls='sign', aria-selected='true') Sign

    li.nav-item

      a.nav-link#verify-tab(data-toggle='tab', href='#verify', role='tab', aria-controls='verify', aria-selected='false') Verify

.card-body#card

  .tab-content#myTabContent

    .tab-pane.show.active#sign(role='tabpanel', aria-labelledby='sign-tab')

      form.form-horizontal

        .form-group

          label.control-label(for='data') Message

          .input-group

            .input-group-addon

            input.form-control#sign-amount(value='input message here')

            .input-group-addon From:

            input.form-control#sign-from

            .input-group-addon -&gt;

            input.form-control#sign-to(value='04cc955bf8e359cc7ebbb66f4c2dc616a93e8ba08e93d27996e20299ba92cba9cbd73c2ff46ed27a3727ba09486ba32b5ac35dd20c0adec020536996ca4d9f3d74')

        .form-group

          label.control-label(for='data') Private Key
```

```
            input#privateKey(type='number').form-control
          .form-group
            button#sign-button.btn.btn-block.btn-primary(type='button') Sign
          .form-group
            label.control-label(for='data') Message Signature
            input#sign-signature.form-control(disabled)
        .tab-pane#verify(role='tabpanel', aria-labelledby='verify-tab')
          form.form-horizontal
          .form-group
            label.control-label(for='data') Message
            .input-group
              .input-group-addon
              input.form-control#verify-amount(value='20.00')
              .input-group-addon From:
              input.form-control.border-primary#verify-from
              .input-group-addon -&gt;
              input.form-control#verify-
to(value='04cc955bf8e359cc7ebbb66f4c2dc616a93e8ba08e93d27996e20299ba92cba9cbd73c
2ff46ed27a3727ba09486ba32b5ac35dd20c0adec020536996ca4d9f3d74')
          .form-group
            label.control-label(for='data') Signature
            input#verify-signature.form-control
          .form-group
            button#verify-button.btn.btn-block.btn-primary(type='button') Verify
```

```
script.
  var EC = elliptic.elliptic().ec;
  var ec = new EC('secp256k1');

  var keypair = ec.genKeyPair();
  if (Cookies.get('privateKey')) {
    keypair = ec.keyFromPrivate(Cookies.get('privateKey'));
  }

  function update() {
    var prv = keypair.getPrivate('hex');
    var pub = keypair.getPublic('hex');
    $('#privateKey').val(bigInt(prv, 16).toString());
    $('#sign-from').val(pub);
    $('#verify-from').val(pub);
    Cookies.set('privateKey', prv.toString());
    Cookies.set('publicKey', pub);
  }

  function resetVerifier() {
    $('#card').removeClass('alert-success');
    $('#card').removeClass('alert-danger');
  }
```

```
  $(function() {
    $('#sign-button').click(function() {
      var message = $('#sign-amount').val() + $('#sign-from').val() + $('#sign-to').val();
      var binaryMessage =
buffer.Buffer.from(CryptoJS.SHA256(message).toString(CryptoJS.enc.Hex));
      var hexSignature =
buffer.Buffer.from(keypair.sign(binaryMessage).toDER()).toString('hex');
      $('#sign-signature').val(hexSignature);
      $('#verify-signature').val(hexSignature);
      update();
      resetVerifier();
    });
    $('#verify-button').click(function() {
      // verify by using only the public key
      $('#verify-from').val($('#verify-from').val().replace(/[^0-9a-fA-F]/g, ''));
      var tmpKey;
      try {
        tmpKey = ec.keyFromPublic($('#verify-from').val(), 'hex');
        var message = $('#verify-amount').val() + $('#verify-from').val() + $('#verify-to').val();
        var binaryMessage =
buffer.Buffer.from(CryptoJS.SHA256(message).toString(CryptoJS.enc.Hex));
        if (tmpKey.verify(binaryMessage, $('#verify-signature').val())) {
          $('#card').addClass('alert-success');
        }
        else {
```

```
      $('#card').addClass('alert-danger');
    }
  }
  catch(e) {
    $('#card').addClass('alert-danger');
  }
});
$('#sign-signature').bind('keyup', function() {
  resetVerifier();
});
$('#sign-amount').bind('keyup', function() {
  resetVerifier();
});
$('#sign-from').bind('keyup', function() {
  resetVerifier();
});
$('#sign-to').bind('keyup', function() {
  resetVerifier();
});
$('#verify-signature').bind('keyup', function() {
  resetVerifier();
});
$('#verify-amount').bind('keyup', function() {
  resetVerifier();
```

```
});
$('#verify-from').bind('keyup', function() {
  resetVerifier();
});
$('#verify-to').bind('keyup', function() {
  resetVerifier();
});
$('#publicKey').bind('keyup', function() {
  resetVerifier();
});
$('#privateKey').bind('keyup', function() {
  $('#privateKey').val($('#privateKey').val().replace(/\D/g, ''));
  keypair = ec.keyFromPrivate(bigInt($('#privateKey').val()).toString(16));
  resetVerifier();
  update();
});
if (Cookies.get('amount')) {
  $('#sign-amount').val(Cookies.get('amount'));
  $('#verify-amount').val(Cookies.get('amount'));
}
if (Cookies.get('amount')) {
  $('#sign-from').val(Cookies.get('from'));
  $('#verify-from').val(Cookies.get('from'));
}
```

```
if (Cookies.get('amount')) {
  $('#sign-to').val(Cookies.get('to'));
  $('#verify-to').val(Cookies.get('to'));
}
$('#sign-amount').bind('keyup', function() {
  Cookies.set('amount', $('#sign-amount').val());
  $('#verify-amount').val($('#sign-amount').val());
});
$('#sign-from').bind('keyup', function() {
  Cookies.set('from', $('#sign-from').val());
  $('#verify-from').val($('#sign-from').val());
});
$('#sign-to').bind('keyup', function() {
  Cookies.set('to', $('#sign-to').val());
  $('#verify-to').val($('#sign-to').val());
});
$('#verify-amount').bind('keyup', function() {
  Cookies.set('amount', $('#verify-amount').val());
  $('#sign-amount').val($('#verify-amount').val());
});
$('#verify-from').bind('keyup', function() {
  Cookies.set('from', $('#verify-from').val());
  $('#sign-from').val($('#verify-from').val());
});
```

```
    $('#verify-to').bind('keyup', function() {
      Cookies.set('to', $('#verify-to').val());
      $('#sign-to').val($('#verify-to').val());
    });
    $('#myTab').on('shown.bs.tab', function (e) {
      resetVerifier();
    });
    update();
  });
```

Signature.pug source code

```
extends layout

block content
  .container
    .card
      .card-header
        h4 Signatures
        ul.nav.nav-tabs.card-header-tabs#myTab(role='tablist')
          li.nav-item
            a.nav-link.active#sign-tab(data-toggle='tab', href='#sign', role='tab', aria-controls='sign', aria-selected='true') Sign
          li.nav-item
            a.nav-link#verify-tab(data-toggle='tab', href='#verify', role='tab', aria-controls='verify', aria-selected='false') Verify
```

```
.card-body#card
  .tab-content#myTabContent
    .tab-pane.show.active#sign(role='tabpanel', aria-labelledby='sign-tab')
      form.form-horizontal
        .form-group
          label.control-label(for='data') Message
          textarea.form-control#sign-message('rows=5', aria-label='Message')
        .form-group
          label.control-label(for='data') Private Key
          input#privateKey(type='number').form-control
        .form-group
          button#sign-button.btn.btn-block.btn-primary(type='button') Sign
        .form-group
          label.control-label(for='data') Message Signature
          input#sign-signature.form-control(disabled)
    .tab-pane#verify(role='tabpanel', aria-labelledby='verify-tab')
      form.form-horizontal
        .form-group
          label.control-label(for='data') Message
          textarea.form-control#verify-message('rows=5', aria-label='Message')
        .form-group
          label.control-label(for='data') Public Key
          input#publicKey.form-control
        .form-group
```

```
            label.control-label(for='data') Signature
            input#verify-signature.form-control
          .form-group
            button#verify-button.btn.btn-block.btn-primary(type='button') Verify

script.
  var EC = elliptic.elliptic().ec;
  var ec = new EC('secp256k1');

  var keypair = ec.genKeyPair();
  if (Cookies.get('privateKey')) {
    keypair = ec.keyFromPrivate(Cookies.get('privateKey'));
  }

  function update() {
    var prv = keypair.getPrivate('hex');
    var pub = keypair.getPublic('hex');
    $('#privateKey').val(bigInt(prv, 16).toString());
    $('#publicKey').val(pub);
    Cookies.set('privateKey', prv.toString());
    Cookies.set('publicKey', pub);
  }

  function resetVerifier() {
```

```
    $('#card').removeClass('alert-success');
    $('#card').removeClass('alert-danger');
  }

  $(function() {
    $('#sign-button').click(function() {
      var binaryMessage = buffer.Buffer.from(CryptoJS.SHA256($('#sign-message').val()).toString(CryptoJS.enc.Hex));
      var hexSignature = buffer.Buffer.from(keypair.sign(binaryMessage).toDER()).toString('hex');
      $('#sign-signature').val(hexSignature);
      $('#verify-signature').val(hexSignature);
      update();
      resetVerifier();
    });
    $('#verify-button').click(function() {
      // verify by using only the public key
      $('#publicKey').val($('#publicKey').val().replace(/[^0-9a-fA-F]/g, ''));
      var tmpKey;
      try {
        tmpKey = ec.keyFromPublic($('#publicKey').val(), 'hex');
        var binaryMessage = buffer.Buffer.from(CryptoJS.SHA256($('#verify-message').val()).toString(CryptoJS.enc.Hex));
        if (tmpKey.verify(binaryMessage, $('#verify-signature').val())) {
          $('#card').addClass('alert-success');
```

```
    }
    else {
      $('#card').addClass('alert-danger');
    }
  }
  catch(e) {
    $('#card').addClass('alert-danger');
  }
});
$('#sign-signature').bind('keyup', function() {
  resetVerifier();
});
$('#sign-message').bind('keyup', function() {
  resetVerifier();
});
$('#verify-signature').bind('keyup', function() {
  resetVerifier();
});
$('#verify-message').bind('keyup', function() {
  resetVerifier();
});
$('#publicKey').bind('keyup', function() {
  resetVerifier();
});
```

```
  $('#privateKey').bind('keyup', function() {
    $('#privateKey').val($('#privateKey').val().replace(/\D/g, ''));
    keypair = ec.keyFromPrivate(bigInt($('#privateKey').val()).toString(16));
    resetVerifier();
    update();
  });
  if (Cookies.get('message')) {
    $('#sign-message').val(Cookies.get('message'));
    $('#verify-message').val(Cookies.get('message'));
  }
  $('#sign-message').bind('keyup', function() {
    Cookies.set('message', $('#sign-message').val());
    $('#verify-message').val($('#sign-message').val());
  });
  $('#verify-message').bind('keyup', function() {
    Cookies.set('message', $('#verify-message').val());
    $('#sign-message').val($('#verify-message').val());
  });
  $('#myTab').on('shown.bs.tab', function (e) {
    resetVerifier();
  });
  update();
});
```

Keys.pug source code

```
extends layout

block content
  .container

    .card
      h4.card-header Public / Private Key Pairs
      .card-body
        form.form-horizontal
          .form-group
            label.control-label(for='data') Private Key
            .input-group
              input.form-control#privateKey(aria-label='Private Key', type='number')
              span.input-group-btn
                button.btn.btn-secondary#randomButton(type='button', ) Random
          .form-group
            label.control-label(for='data') Public Key
            input#publicKey.form-control(disabled)

  script.
    var EC = elliptic.elliptic().ec;
    var ec = new EC('secp256k1');
```

```
var keypair = ec.genKeyPair();
if (Cookies.get('privateKey')) {
  keypair = ec.keyFromPrivate(Cookies.get('privateKey'));
}

function update() {
  var prv = keypair.getPrivate('hex');
  var pub = keypair.getPublic('hex');
  $('#privateKey').val(bigInt(prv, 16).toString());
  $('#publicKey').val(pub);
  Cookies.set('privateKey', prv.toString());
  Cookies.set('publicKey', pub.toString());
}

function random() {
  keypair = ec.genKeyPair();
  update();
}

$(function() {
  $('#randomButton').click(random);
  $('#privateKey').bind('keyup', function() {
    $('#privateKey').val($('#privateKey').val().replace(/\D/g, ''));
```

```
    keypair = ec.keyFromPrivate(bigInt($('#privateKey').val()).toString(16));
    update();
  });
  update();
});
```