CLOUD BASED SECURE INFRASTRUCTURE FOR IOT DEVICES

By

Iqra Jadoon

00000206305

Supervisor

Dr. Abdul Ghafoor Abbasi

Department of Computer Science

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Security (MS IS)

In

School of Electrical Engineering and Computer Science,

National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(June, 2019)

Approval

It is certified that the contents and form of the thesis entitled "**Cloud based Secure Infrastructure for IoT Devices**" submitted by Iqra Jadoon have been found satisfactory for the requirement of the degree.

Advisor: Dr. Abdul Ghafoor Abbasi

Signature: ____________________

Date: ____________________

Committee Member 1: Dr. Hassan Tahir

Signature: ____________________

Date: ____________________

Committee Member 2: Ms. Hirra Anwar

Signature: ____________________

Date: ____________________

Committee Member 3: Dr. Mehdi Hussain

Signature: ____________________

Date: ____________________

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by Ms **Iqra Jadoon**, (Registration No **206305**), of School **of Electrical Engineering and Computer Science** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: ______________________________

Name of Supervisor: _____________________

Date: _________________________________

Signature (HOD): ________________________

Date: _________________________________

Signature (Dean/Principal): ________________

Date: _________________________________

Dedication

Dedicated to my beloved parents, adored siblings and teachers who have helped me thoroughly and gave me the opportunity to learn

Certificate of Originality

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: Iqra Jadoon

Signature: ________________

Acknowledgment

I am grateful to Allah Almighty for guidance and blessings.

Iqra Jadoon

Table of Contents

List of Tables

List of Figures

Abstract

The proliferation of IoT technology has transformed various businesses but at the same time, it has provided access to a huge number of physical devices deployed in the network. The IoT devices are susceptible to multiple security threats and challenges, device authentication, and verification being one of the foremost. Research work in this dimension has been carried out and multiple solutions have been provided however an end-to-end security solution is required which encompasses the IoT devices, Fog layer, and Cloud computing paradigms. This paper presents a secure and trusted framework for anonymous authentication and data integrity while protecting the system against unauthorized access, impersonation and repudiation attacks in the IoT environment. To achieve our objectives, in this paper IoT devices are integrated with blockchain to create, publish and manage their identities anonymously which will be verifiable without consulting a centralized third party to authenticate the IoT devices. The designed protocol is verified using formal verification tool '*Scyther'* and it satisfied various security attributes mandatory for authentication and data integrity protocols.

Chapter 1

Introduction

Internet of Things (IoT) is the combination of smart devices like actuators, sensors that are embedded in physical entities (e.g. smart mobiles, smart homes, and smart vehicles), which are connected by both wireless and wired communication mediums. As the advancement in smart technologies, the usage of IoT devices is increased on a daily basis in various aspects of our life. The importance of IoT devices is comprehended by business and scientific communities and they started to emerge for improving the usage of IoT devices [1]. The statistics of existing literature shows that the annual usage and growth of IoT devices from 2015 to 2017, which is 4.94 billion. The expected ratio of growth of IoT devices is 75.44 billion by 2025 [2].

The IoT devices provide a major technology revolution in smart industries such as smart homes, smart cities, smart healthcare systems, smart traffic management systems, smart grid systems and smart airport management systems that updated the entire infrastructure of the internet. As a concept of a connected world, these smart devices are connected to each other through more advanced computing network and provide different services according to their unique characteristics [3]. By the use of continuously updating and emerging technologies, smart devices (IoT) collects some important data by using some new and already existing communication mechanisms on the basis of automatically configured actions [4].

Those millions of connected IoT devices collect and stored a huge amount of data by using secured mechanisms which provides some important security features such as authentication, confidentiality of data, etc. for their communication with connected servers (e.g. cloud servers) that are explained in *figure 1*. The security and privacy of generated data are very important for IoT devices while data send and retrieve to/from cloud servers. The generated data must be secure at the local site of the IoT devices as-well-as to another end of the internet site to avoid any data altering and destruction from intruders [1], [5]. There are many attacks that may occur while communication between IoT and cloud server if the communication is not secure, these attacks are: IP spoofing, sniffing attack, man-in-the-middle attack, password-based attack and DDOS/DOS attack, etc. that are used to intrude the data while communication. These type of attacks may influence the efficient and effective usage of IoT devices and also may cause some big problems in data critical IoT devices.

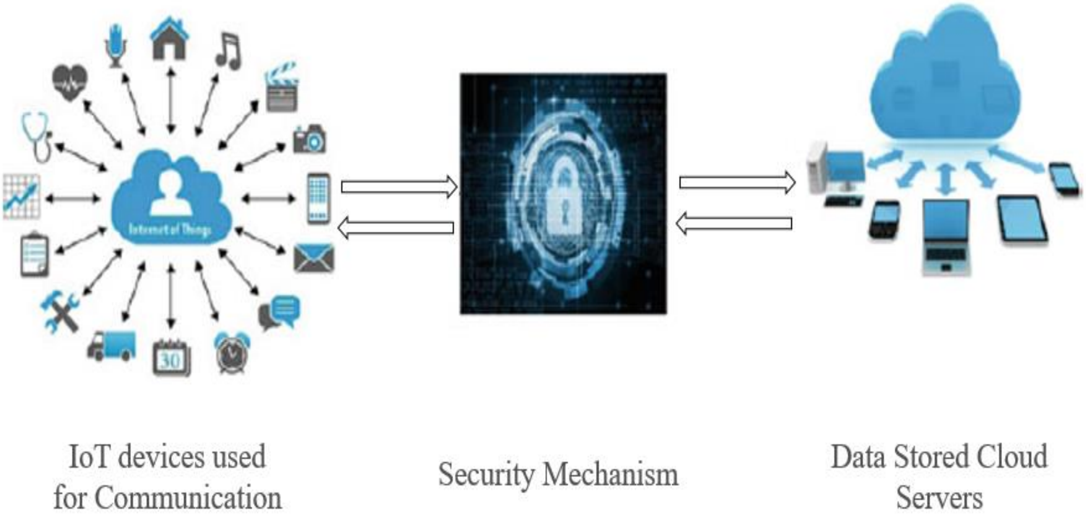


Fig 1: IoT communication with Cloud [68]

The Internet-of-Things (IoT) consists of different elements and contain various characteristics, the main and basic elements of IoT devices are [5]:

a) **IoT devices connectivity:**
The network of IoT devices, in which IoT devices are connected through a communication medium and also depend on the source code like sensors and objects. IoT network is connected in every dimension to present the effective connectivity of IoT devices.

b) **IoT communication:**
The most important use of IoT devices is the collection of data, so the communication of IoT devices with each other and with cloud servers may need some insights or actions.

c) **IoT action and intelligence:**
By solving the smart usage of data and information challenges, using connected IoT devices capacity of action and analysis of data through intelligent networking/communication technologies.

d) **IoT automation:**
The word automation plays a vital role in every field, in which IoT devices that consist of different software's perform their actions without any human's interaction.

IoT devices provide a great potential of flexibility for computing technologies and provide the assurance of a great future to the technological world. But IoT devices faces some security and privacy related disasters too. Its rapid growth and wide adaption increases some security and privacy concerns. The existing security and privacy mechanisms are unable to provide better services in an advanced technological world, so there is a need to design and build proper mechanisms for such security and privacy threats. IoT devices can be exploited by the intruders if they are easily accessible to them [6]. In Today's world, IoT devices have a direct impact on the people lives' that used those devices. The concerns of network security and privacy must be on high priorities. Therefore, there is a need to establish well-defined network security and privacy infrastructures to reduce the network security threats of IoT devices [7]. There are various examples where the vulnerabilities in the IoT network have been exploited which leads to serious consequences. A systemic and cognitive approach is required which must consider People, Process, Intelligent Objects and Technological Environment [8].

IoT devices generate huge amounts of data that needs to be processed, analyzed, stored, and presented into a meaningful manner. There are two types of IoT devices: resourceful IoT devices (e.g. smart mobiles, smart watches, smart grid systems, etc.) and resource constraints IoT devices (e.g. sensors, actuators networks, etc.). Both IoT devices need to store their data on different servers (e.g. local and cloud servers). So, network security and privacy in both cases are very important. The cloud server also called cloud computing, provides a vital role to the growth of IoT devices because cloud computing provides on-demand network access to cloud-based IoT infrastructures in terms of network security and privacy [9].

Cloud computing consists of different models that have been used for an effective and efficient way to process, analyze and store data because they provide on-demand storage and computation capabilities. The cloud computing models are based on centralized computing and most of their computations such as storage, processing, and analysis of data is handled in cloud (e.g. centralized location). In which all the requests that are generated by IoT devices need to be transmitted to that cloud. In which all the data that are generated from IoT devices are directly uploaded to cloud servers for processing and storage. For this purpose, massive measurements are needed on the cloud side for analyzing received data (e.g. which data are important or which are not) [10].

By using cloud on-demand model, data processing, analyzing and storing speed has not a big deal to handle millions of IoT devices, but the network bandwidth that is used by IoT devices to send this data to cloud servers is not increased according. The result of continuously transmitting data that is generated by various types of IoT devices to cloud computing servers is becoming the bottleneck for this network that may cause long latency problem for connected cloud-based IoT devices. Some IoT devices have latency-sensitive characteristics, which have very short time response and mobility support such as healthcare IoT devices, smart traffic management systems for transportation, emergency response systems, and smart grid systems, etc. [11]. This type of delay in response may cause some serious problems in terms of user's lives and cost. So, all the challenges faced during the advancements and rapid growth of IoT devices such as latency in response, network bandwidth, location awareness, mobility in data transfer, security and privacy of IoT devices data, can't be addressed only by using cloud computing [12].

To overcome these issues, fog computing has been introduced. Fog computing consists edge of the network and provides efficient resources such as computation, data access, storage, and networking. It provides a new breed to the Internet of Things (IoT) by providing a wide variety of services and applications at the edge of the network. It acts as a bridge between cloud computing and Internet of Things (IoT). It is considered to be a new paradigm/extension of cloud computing [13]. Fog computing paradigm and its architecture is shown in *figure 2*.

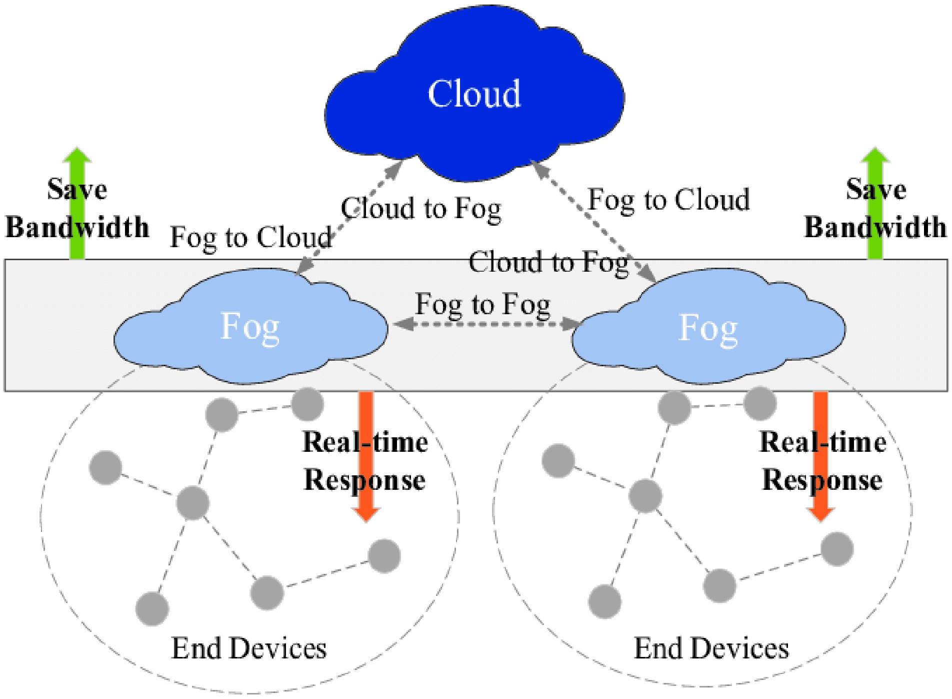


Fig 2: Fog computing enabled IoT system architecture [69]

Fog computing provides unique as well as cloud-related services to the Internet of Things (IoT). It provides data processing, analyzing and storage services to IoT devices at the edge of the network. By providing service at the edge of the network, fog computing faced some security and privacy issues. The existing measurements of cloud computing related to privacy and security cannot be applied to fog computing due to its unique characteristics. For getting an efficient and effective performance from fog computing, there is a much need to address all of the above-mentioned security and privacy concerns. The fact about fog computing paradigm needs to be cleared that it is just an extension of cloud computing and act as a bridge between cloud computing and cloud-based IoT devices. Fog computing nodes just analyze, process, and store some important data that is received from various connected IoT devices for some specified time period. After that, this important data and information is transmitted to the cloud computing servers for further processing, analyzing and storage [14].

1.1 Motivation

The integration of the technologies including IoT network, fog and cloud computing have posed new security risks and challenges [64] as witnessed through recent attacks such as target corporation IoT breach that exposed more than 40 million credit cards and debit card numbers, another breach is Mirai botnet in which the distributed denial of service attack was launched [3]. Attacks on marketing and data aggregation firm Exactis have left about 340 million records exposed on the publicly accessible server due to the database misconfiguration and consequences of the implementation of simple authentication protocol to access stored data. In order to gain the full confidence and trust of the users on IoT devices and their data collection and processing methods, various security problems need to be solved [65-66]. Most of the existing solutions have used cloud and fog computing and some researchers have provided the solution by integrating blockchain technology, however, an end-to-end security solution is required which encompasses the IoT devices, Fog layer, and Cloud computing paradigms.

1.2 Problem statement

A well-defined security protocol is needed to ensure end-to-end security of data generated by the IoT devices, the origin of data must be verified, and the data must be submitted by an authenticated device.

1.3 Objectives and Research Goals

The goal of this thesis is to propose a novel network security IoT framework that ensures the authentication, identification of IoT devices that wants to communicate with fog computing layer, the integrity of data that is transmitted during communication between both ends, and to address the non-repudiation network security feature.

1.4 Thesis Organization

The presented thesis has been organized into different chapters in which each chapter gives certain aspects of our research, depicted in figure 3. Following is the brief description of all the thesis chapters.

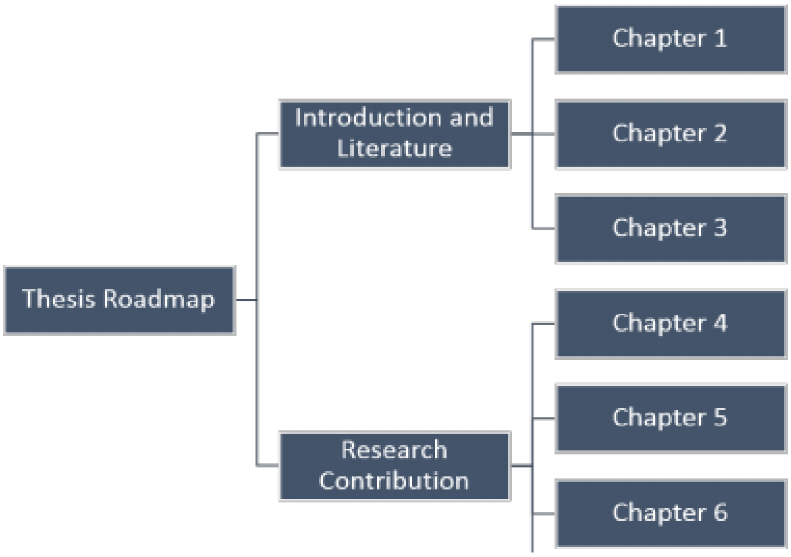


Fig 3: Thesis Organization

- Chapter 1 entitled “Introduction” elaborates the main concepts, problem statement, and motivation behind the thesis
- Chapter 2 entitled “Background” gives detailed background .information of the IoT, Fog Cloud, blockchain and smart contracts.
- Chapter 3 entitled “Literature Review” gives details of the literature survey which has been conducted throughout the research phase.
- Chapter 4 entitled” Secure and trusted IoT framework” explains the proposed framework, components of the framework, and end-to-end security protocols.
- Chapter 5 entitled” Formal verification of protocol using *Scyther* ” explains the analysis and results of the proposed protocol
- Chapter 6 entitled “conclusion” concludes the thesis.

Chapter 2

Background

The background section of this document gives an opportunity to its readers in understanding, which terminologies are used such as Internet of Things (IoT), Cloud computing, Fog computing, and Blockchain, etc.

2.1 Internet of Things (IoT)

Internet devices play an important role in our everyday life. They are made up of different physical objects, digital and mechanical devices. These devices are equipped with storage, communication, processing and computing capabilities, such as mobile phones, oven, sensors, car, refrigerator, laptops, operator, etc. Each object has specific features built into its computer system that interacts with the current Internet infrastructure. These Internet devices are increasing every-day to meet all the needs of our daily lives. According to Cisco's statistical report, the proportion of Internet devices in 2030 will be 125 billion out of 8 billion population [15]. All devices are capable of connecting to the Internet for data exchange. Internet access lets you control your Internet devices remotely from anywhere, anytime. This connection and automation of Internet objects open up new research areas in this domain.

Internet of Things (IoT) combines multiple application areas from private and home perspective fields [16]. In this context, there are many Internet applications that improve the quality of our lives: while traveling, communicating, at home, in industries, etc. or professional life. Many Internet devices collect local data on the everyday life of humans for operational and processing purposes. These devices have become a major source of generating a large amount of information flowing from a various number of interrelated nodes, which must be processed, analyzed, stored, and delivered in an efficient and easy-to-interpret manner [17].

2.1.1 Internet of Things (IoT) Applications

In the advancement of the technology sector, Internet of things (IoT) support various types of applications and they allow developers to develop applications in multiple domains, a large number of applications are available for IoT devices. There are many areas and environments in which Internet applications work. These things improve the quality of our lives, in terms of travel, communication, healthcare, data processing and storage, and so forth. This section explains many internet of things (IoT) domains [18], [19].

a) **Transportation and logistics** (e.g. Advanced trains, cars, traffic lights, buses as well as bicycles instrumented with sensors share some important information to connected servers through real-time processing and analyzing technology using RFID and NFC, etc.)
b) **Smart Environment** (e.g. Smart environment contains the things that make easiness of our routine life things such as comfortable offices, homes, museum, and gym, etc.)
c) **Personal and Social** (The applications of this domain are used to provide services to people to interact with other people for maintaining and developing their social relationships).
d) **Healthcare** (In this domain, there are many applications that provide very important and critical services to its users in the healthcare domain. These types of applications are used to collect data from patients and staff or automatic collection of data through different sensors from various healthcare instruments, etc.**)**
e) **Futuristic** (In this futuristic domain, there are some applications that are used for communication, industrial processes and sensing some important information, etc.). These applications are based on some realistic data type applications, which are already discussed in the above sections.

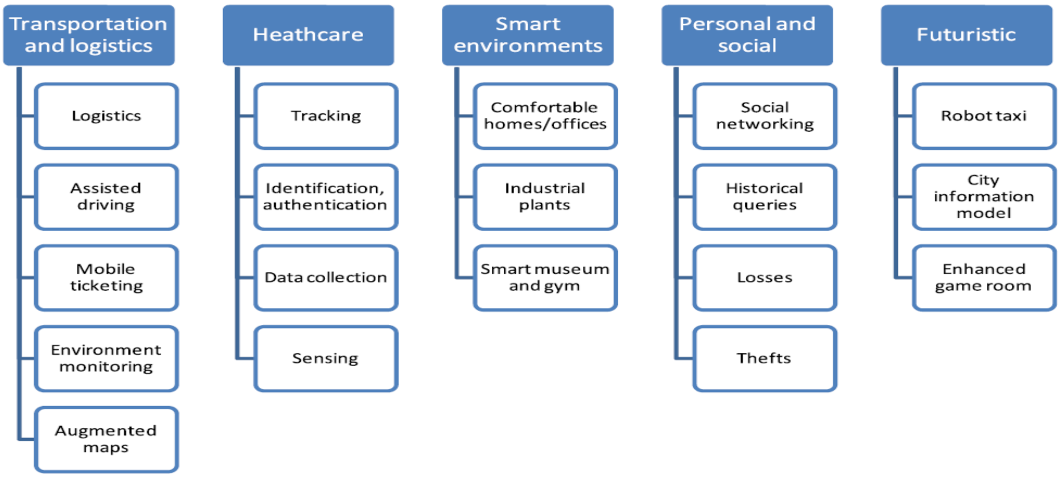


Fig 4: Applications domains and relevant major scenarios [70].

2.2 Cloud Computing

Cloud computing is considered to be data invocation paradigm that empowers the access of shared and private resources. It is the widest representation of the internet. Cloud computing is an advanced technology that is used for business purposes. It provides the facility to its users to store and retrieve data over the internet. It contains high computational powers for providing efficient services to processing and storing data. It increases the capabilities of dynamically adding new resources [20]. Cloud computing acts as a model that offers on-demand service to its users for different cloud-based applications. It’s a combination of distributed and parallel systems. various range of Internet of Things (IoT) used cloud computing for processing, analyzing and storing their data.

National Institute of Standard and Technology (NIST) define cloud computing: “*A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*” [21].

Cloud computing consists of two-tier architecture, in which the first tier represents cloud computing infrastructure which contains servers, storage, and network devices that are shown in *figure 1*. The second one represents different IoT devices such as smart homes, smart grid systems, smart healthcare systems, etc [22]. Various type of benefits are provided by the cloud computing to its users such as: pay-per-use (Compute the resources that are measured at granular level, and allow its users to pay only for the workload and resources they used), workload resilience (By ensuring resilience storage and maintaining users workload, service providers implement redundant resources) and migration flexibility (Firms and organizations can move their resources and workloads to/from the cloud) etc. By providing these service to its consumer's cloud computing reveals a remarkable potential in a cost-effective way.

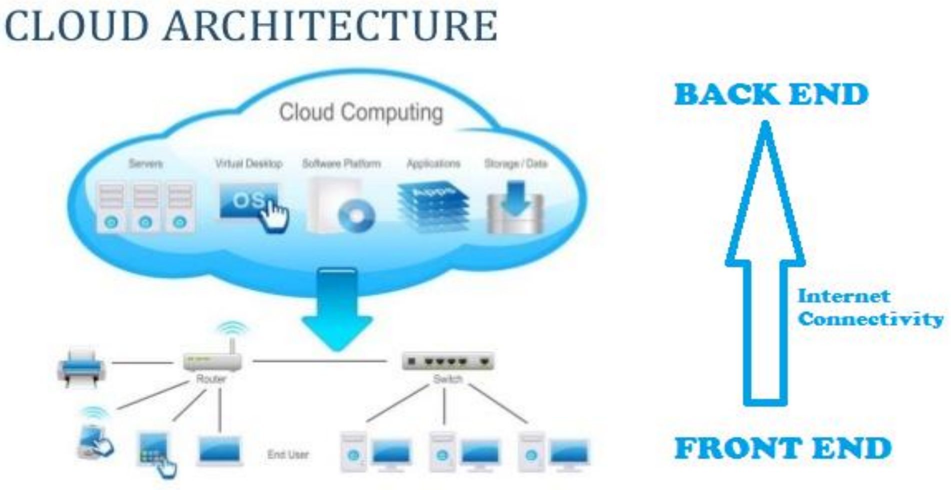


Fig 5: Cloud computing architecture [71].

2.2.1 Cloud Computing Models

Cloud computing is divided into three deployment models such as: public cloud model, private cloud model, and hybrid cloud model. These models have different characteristics.

a) Public cloud computing model

In this model a third-party service provider's makes computational and storage resources available to the general public over the internet. Due to the access of this model to the general public, it provides less security of data.

Fig 6: Public cloud [72]

b) Private cloud computing model

The private cloud model provides accessibility of their systems and services inside an organization. It is considered to be more secure as compared to the public cloud model, due to its private nature. This cloud model is only accessible to limited and authenticated users. The general public is unable to access its systems and services.

Fig 7: Private cloud [72]

c) Hybrid cloud computing model

The hybrid cloud computing model is a combination of private and public cloud computing models. The performance of this cloud model is divided into critical and non-critical ways. Critical performance of this model is handled using a private cloud computing model and non-critical performance is handled using public cloud computing model.

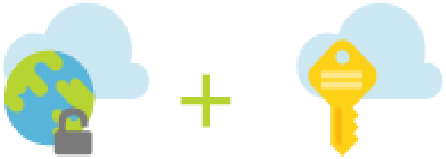


Fig 8: Hybrid cloud [72]

2.2.2 Cloud computing services

Cloud computing provides various type of services to its users, which are: Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS).

a) Infrastructure-as-a-Service (IaaS)

In this service, cloud service providers provide physical, virtual, additional storage and networking devices to their users, in which cloud service users are responsible for installing and maintaining operating systems on provided virtual devices and software applications. IaaS is an instant computing infrastructure that is used and managed over the internet. IaaS also used a pay-per-use model, in which users are allowed to increase and decrease resources/infrastructure according to their requirements [23]. Users only pay for those service components that they used. By using IaaS users reduce their infrastructure cost in terms of purchasing and managing hardware resources etc. It allows users to install their own operating systems and software applications.

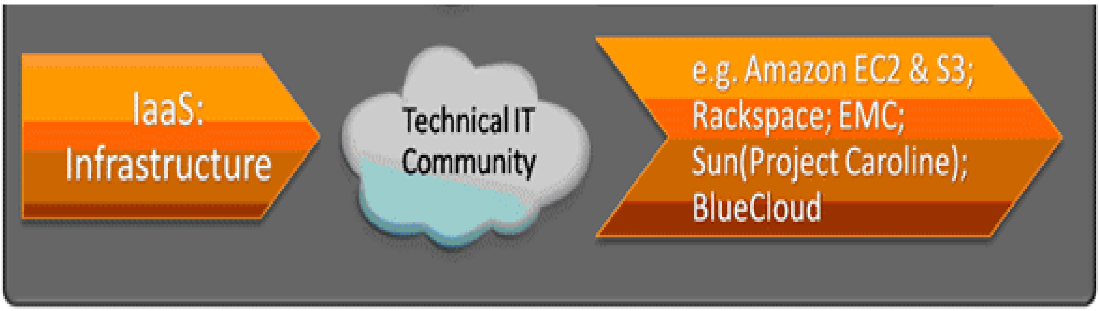


Fig 9: Infrastructure-as-a-Service (IaaS) [73]

b) Platform-as-a-Service (PaaS)

This cloud service utilizes the software's or platforms provided by cloud service providers. In this service, service providers provide a complete development environment, in which users will be able to develop and deploy their software's. For development and deployment of software's applications, this service provides all required resources to their users. For this purpose users just need to purchase their required resources form service providers using the on-demand model. PaaS supports the complete life cycle (e.g. development, testing, deployment, managing, and updating) of the web-applications. By using this cloud service, user's will not need to purchase new software tools and their licenses [24]. In PaaS you just need to manage your applications and services that you have developed, other typical things are managed by the PaaS service providers.

PaaS: Platform
Technical IT Community
e.g. Google app Engine; Force.com; Azure

Fig 10: Platform-as-a-Service (PaaS) [73]

c) Software-as-a-Service (SaaS)

SaaS avoids the maintenance and support of software's/applications. It allows its users to use software's and applications (e.g. emails, office tools, operating systems, etc.) over the internet. In SaaS service infrastructure various software's and applications have been installed already, and the user is able to use this software and applications. It provides various software's and applications that users can purchase by using a pay-on-demand model from SaaS service providers. SaaS service providers maintain hardware and software resources, they also provides security of your data. Cloud user access this SaaS by using their browsing applications (e.g. web browser) [23], [24].

SaaS: App/ Service
Business User/Consumer
e.g. Salesforce; NetSuite; Zoho;Zimbra; Office Live; Concur; Taleo

Fig 11: Software-as-a-Service (SaaS) [73]

2.2.3 Security Issues In Cloud Computing

Cloud computing provides various benefits and advantageous characteristics to their users. Even though cloud computing is more flexible, reliable and cost-effective due to lack of privacy and security concerns, it contains remarkable security issues that are needed to be solved. These security issues in cloud computing are given below:

- Data Integrity
- Data Location
- Data Segregation
- Network Security
- Data Privacy
- Data Security
- Data Availability
- Management of patch
- Security Compliance and policy
- Access to Servers & Applications

2.3 Fog Computing

Fog computing technology is used as a bridge between cloud computing and Internet of Things (IoT). It is considered to be a new paradigm/extension of cloud computing. Fog computing consists edge of the network and provides efficient resources such as: computation, data access, storage, and networking. It provides a new breed to the Internet of Things (IoT) by providing a wide verity of services and applications at the edge of the network. Fog computing contains different characteristics as compared to cloud computing, but it also supports multiple concerns such as: location awareness, mobility, large scalability, heterogeneity, low latency and geo-distribution [25]. In other words, fog computing is used to decrease the latency, reduce the data traffic to cloud servers, and also improve the quality of service. Fog computing was introduced by CISCO as an extension of cloud computing. Fog computing provides unique as well as cloud-related services to the Internet of Things (IoT). It provides data processing, analyzing and storage services to IoT devices at the edge of the network. By providing service at the edge of the network, fog computing faced some security and privacy issues [26]. The existing measurements of cloud computing related to privacy and security cannot be applied to fog computing due to its unique characteristics. Due to the limited resources of IoT devices, they are unable to execute all crypto graphic operations for secure communication, there fog computing layer act as a proxy to overcome these issues. For getting efficient and effective performance from fog computing, it is therefore much needed to address all security and privacy concerns [27].

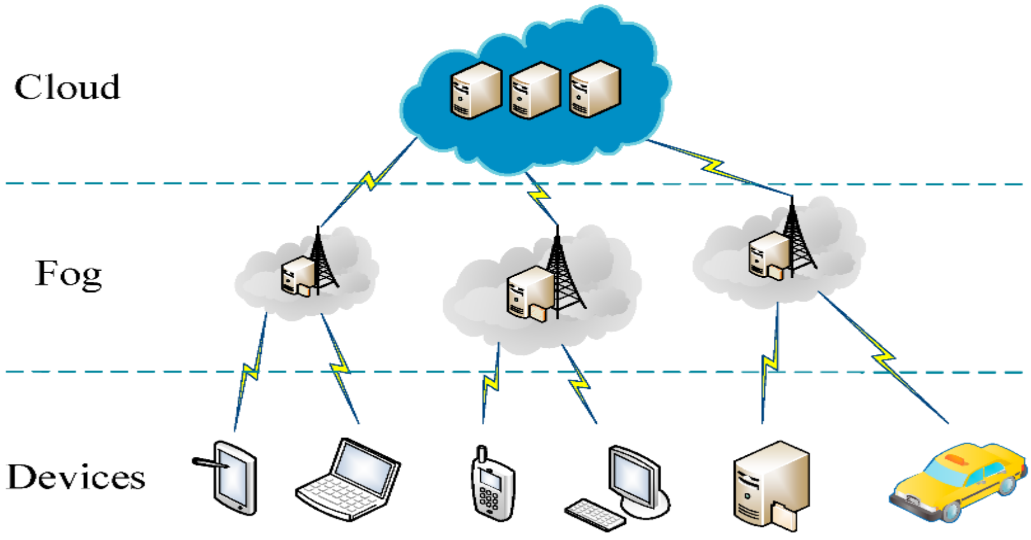


Fig 12: System model in fog-cloud computing environment [74]

2.3.1 Security Requirements in Fog Computing

Cloud computing act as a centralized framework that provides computational and storage of data services to its users. The centralized behavior of cloud computing is considered to be vulnerable and hacked by external intruders. On the other side, fog computing provides a decentralized framework and is considered to be an extension of cloud computing at the edge of the network. In decentralized computing infrastructure, fog computing act as a bridge between cloud computing and the internet of things (IoT). In this infrastructure, it is capable to utilize various type of IoT devices. It helps to perform a significant amount of computation, communication, storage, management and control on data that are generated by a various number of connected IoT devices [28]. Fog computing with decentralized infrastructure can efficiently and effectively address the challenges faced in cloud computing. It meets the demands of real-time and time-sensitive applications and reduce the bottlenecks issues of the network by being proximity to IoT devices. The integration of cloud-based IoT devices into fog computing faced new security and privacy-related issues. Although, there are many security measures that exist to provide effective and efficient services to cloud computing while communicating with IoT devices [29]. These existing cloud computing security measures are not suitable for fog computing due to its decentralized infrastructure and unique characteristics. Some security features such as: Authentication of IoT devices, Confidentiality and integrity of data, and non-repudiation of communication bodies are very important to be an effective and efficient use of fog computing. Internet of things (IoT) have become a major source of generating a huge amount of data, this generated data are called streamed information that needs to be processed, analyzed and stored [30]. There are some fog security requirements that are given below:

a) Authentication

Authentication is an essential security requirement of fog computing for cloud-based IoT devices. It is the process to identify the IoT devices that are trying to communicate with fog computing. In this process, multiple authentication schemes are used to identify IoT devices such as: token and smart card based authentication, etc. It is very important for fog computing to prevent the entries of unauthorized IoT devices while communicating with them.

b) Confidentiality

Confidentiality means to protect something from unauthorized bodies. In a fog computing environment, confidentiality refers to protecting streamed information and data that are generated by authorized connected IoT devices from unauthorized external intruders or IoT devices. It is considered to be an important part of fog computing while providing services to the heterogeneous IoT devices. For making secure end-to-end communication between fog and IoT devices, confidentiality is very important. [31].

(c) Integrity

It is the process of ensuring the authenticity of data and streamed information that is generated from various IoT devices. The main goal of integrity is to protect data from external intruders from any modifications. It maintains the trustworthiness of streamed information, consistency, and accuracy. In this process, it prevents external intruders from any type of modification in the streamed information [32].

(d) Availability

Availability of data is very important for the effective and efficient use of fog computing layer for heterogeneous IoT devices. It ensures that data is always available for authorized IoT devices and they don’t not faced any type of delays in retrieving and sending data/streamed information. Availability of data is considered to be a very important factor for the success of fog computing [14].

(e) Non-repudiation

It is the process to ensure the identity of source and recipient, which share some data with one another. It refers to ensure that source and receiver cannot deny something, it means the source is unable to disown from the information that the receiver received. In this process, through non-repudiation, source and receiver know one another while communicating. Non-repudiation can be addressed by digital signatures. Digital signatures are the electronic signatures that are used to describe someone identity [8]. By addressing non-repudiation in fog and IoT devices communication we can improve the usability of fog computing at local level and increase the utilization of various types of IoT devices [33].

Table 1: Fog computing security features and threats

No	Security Requirement	Security Threats	Description
1	Authentication	Brute Force	Brute force attack is a type of authentication security related attack in which external/internal intruders hack person's password's, secret keys that are used for encryption and description of important data, person's usernames, and might be credit card numbers by guessing and using automated tools. In these automated tools, attackers used millions of combinations of words, numbers, and symbols repeatedly until it matches with original targeted data.
		Insufficient Authentication	It is another type of authentication security attack, in which external/internal intruders access the website and other links which contain some sensitive information of users, through this information they may guess their passwords, usernames, credit card passwords, etc.
		Week Password Recovery System	Week Password Recovery System is another type of authentication-related attack, in which some websites don't use well-organized password recovery mechanisms, this type of loose password recovery mechanisms generates some vulnerabilities. Attackers attack those mechanisms to change the user's password and get the complete access of user's data.
2	Confidentiality	Packet Capturing/Sniffing	Packet sniffing/capturing is confidentiality related network security attack. In this attack, internal/external intruders capture the packets/frames of data from the transmission medium and read sensitive information from those captured packets/frames such as: person's username, passwords, credit card numbers, etc. This type of attack

			occurred if network traffic is not encrypted or encrypted with weak encrypted mechanisms.
		Password Based Attack	Password related attack is a type of confidentiality of data, in which external/internal intruders gain access to the target device. This type of attack is used to get access to a user's sensitive information or to harm someone. Password-based-attack consists of two types, first one is dictionary-based-attack (attackers used millions of commonly used password to match with target user's password), and the second one is brute-force attack that is already discussed in the authentication section.
		Port Scanning and Ping Sweeps	Port Scanning and Ping Sweeps is another type of confidentiality of data related network security attack. In this attack, external/internal intruders scan target users/system TCP/UDP ports to discover the running services and software of the target system.
3	Integrity	Tempering Attack	Tempering attack is a type of integrity related network security attack. In which invaders maliciously modify, delay or drop the transmitting frames/packets of target users data to disrupt and degrade the performance and services of fog computing. This type of network security attack is considered to be difficult to detect due to its tempering behavior. The results of this attack, mobility, and performance of used communication medium may delay and failure in transmission of data.
		Forgery Attack	Forgery attack means to forge the identities and profiles related information of target users. Through this attack, invaders also mislead other users by using some wrong information. This type of attack is used to make delays and failures of fog computing services by

			using their resources such as: storage, data analyzing and processing, through faked data generated by malicious invaders.
4	Availability	Denial of Service Attack	In denial of service (DoS) attack, attackers usually block the accessibility of services that are provide by fog computing to the authenticated users. This type of attack consumed a large amount of fog computing resources, this may cause to prohibit the fog computing services from authenticated users.
		Jamming Service Attack	This type of attack is used to jam the service of fog computing by generating large amount of bogus data for consuming resources to prohibit the authenticated users. For the result of this attack, fog computing may unable to provide services to authenticated users.
5	Non-repudiation	Collision Based Attack	Collision-based-attack is a type of non-repudiation related network security attack. In which external/internal invaders collude together to deceive of mislead legitimate users.

2.4 Blockchain Technology

These days digital currency has turned into a trendy expression in both industry and academia. As a standout amongst the best cryptographic money, Bitcoin has appreciated a gigantic accomplishment with it's capital showcase achieving 10 billion dollars in 2016. With a uniquely planned information stockpiling structure, exchanges in Bitcoin system could occur with no outsider and the center innovation to assemble Bitcoin is blockchain, which was first proposed in 2008 and actualized in 2009 [34]. Blockchain could be viewed as an open record and all dedicated exchanges are put away in a rundown of blocks. This chain develops as new blocks are affixed to it constantly. Awry cryptography and appropriated agreement calculations have been actualized for client security and record consistency [35].

Blockchain is a distributed ledger which eliminates the need of trusted third party and can be used for identity authentication and security protection of IoT devices. The blockchain is a sequence of data represented by blocks, where each block is linked with the previous one. Each block consists of two parts; block header and block body. The block header includes the block version, Merkle root, timestamp, and nonce, etc., whereas the block body includes transactions(Zheng, Xie and Dai, 2018). Each transaction is initiated by the user and is signed by his private key, whereas the public keys are used as an address (Narayanan *et al.*, 2016).[36] Each block contains the hash of the previous block The following three properties are provided simultaneously by the blockchain: (i) trusted (ii) permissionless (iii) censorship resistant(Id and Tapas, 2018) [37]. There are special nodes in the network that are called miners, which verify the transactions occurring in the network. Miners solve a mathematical puzzle called as proof of work and generate a block and propagate those blocks in the network(Dorri *et al.*, 2017).[38]

The blockchain innovation for the most part has key attributes of decentralization, persistency, secrecy, and audibility. With these qualities, blockchain can significantly spare the expense and improve its effectiveness. Blockchain is a circulated record innovation developed from Bitcoin and other digital forms of money. The blockchain is fundamentally a changeless, decentralized furthermore, open accessible shared database. In the blockchain, all exchanges are recorded and anybody in the framework is permitted to get to, send and check these exchanges. Applying block-chain innovation to keen urban areas can bring numerous great highlights, for example, without trust, straightforwardness, pseudonymity, computerization, decentralization, and security [39]. Trust free implies that the blockchain framework can run typically in a shared way without a dependable outsider. Blockchain innovation empowers everybody to get to all exchange records, which makes it straightforward. The pseudonymity can be figured it out by chronicle exchanges utilizing open pseudonymous locations, what's more, keeping hubs' true personalities covered up. In the blockchain framework, choices are made by all hubs in a peer-to-peer way, which makes it decentralized [40]. Smart contracts on the block-chain can perform exchange age, basic leadership and information stockpiling naturally. The decentralization of the blockchain framework makes it fundamental to guarantee consistency by running accord calculations among decentralized hubs. Security in the blockchain framework is identified with respectability, privacy and approval [41].

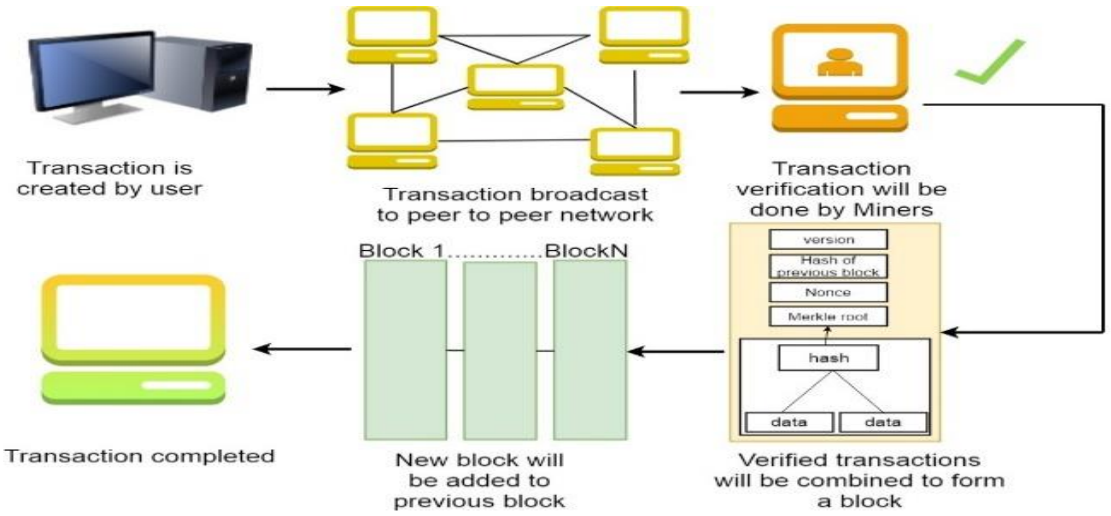

Transaction is created by user
Transaction broadcast to peer to peer network
Transaction verification will be done by Miners
version
Hash of previous block
Nonce
Merkle root
hash
data
data
Block 1............BlockN
Transaction completed
New block will be added to previous block
Verified transactions will be combined to form a block

Fig 13: Sequence and steps required to complete transactions in the blockchain network

2.4.1 Smart Contracts

Smart contracts are digital contracts those are executable code and maintain private storage to manage blockchain data. The code is written on the blockchain and it cannot be changed once deployed to make them immutable. There is a unique 20 bytes address that has been assigned to a smart contract (Alharby and Moorsel, 2017).[42] The main features of Ethereum blockchain are Smart Contracts that are written in Solidity language, Serpent and Low-level Lisp-like Language (LLL) but solidity language is mostly used by the developers. In order to prevent the contract tempering, they are copied to each node (Cheng *et al.*, 2018) [43].

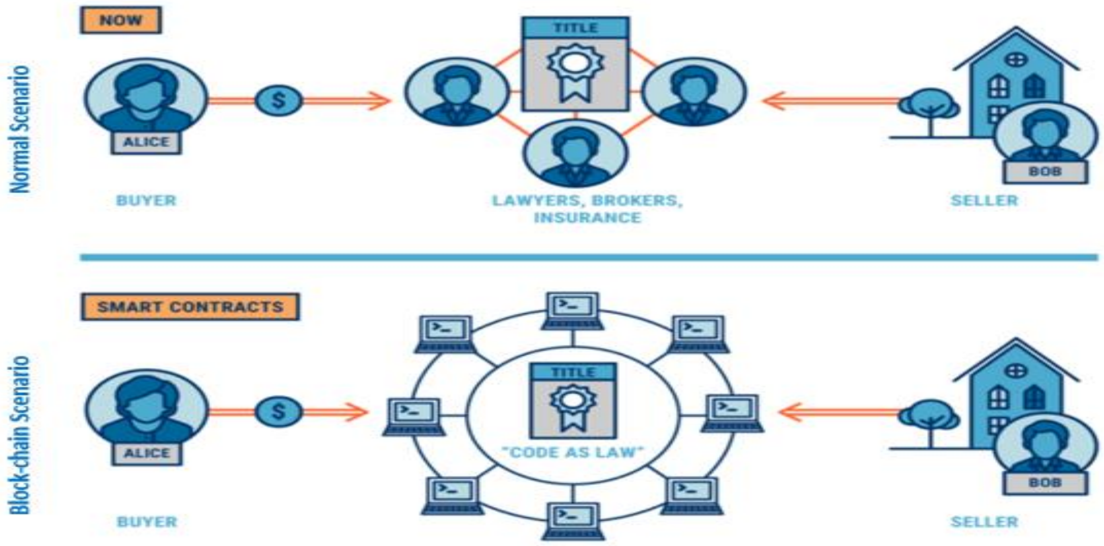


Fig 14: Bloch-chain with Smart Contract [75]

Chapter 3

Literature Review

This section highlights in detail state of the art research that has been carried out in the areas of IoT security, Fog computing, and Blockchain, specifically focusing on the security aspects.

(Salman *et al.*, 2016)[44] have proposed an identity-based authentication scheme for the heterogeneous IoT devices in a network. In the proposed scheme the authors have used Software Defined Networks (SDN) for identification and authentication of IoT devices. There are three main components in the scheme, IoT devices, Gateway, and Controller. In the first phase, the Gateway will authenticate himself to Controller. In the second phase, IoT devices will register themselves with the Controller. In the last phase, the authentication will begin in which IoT devices will authenticate themselves. Testing was also done by using a tool called SPAN/AVISPA. Attacks that have been considered in this scheme are masquerading attack, man-in-the-middle attack, and replay attack. The scheme is well designed in terms of managing security data and storage overhead has been decreased by transferring powerful work to gateway and controller, however, IoT devices faces some challenges in terms of computation.

The authors in (Abdo, 2017)[45] have proposed an authentication mechanism on transport/application layer. They have proposed a cloud service known as Authentication proxy as a service. When the user accesses the service they have to face a lot of delay due to many reasons, even after authentication device has to perform some operations. In the proposed authentication scheme the password will be saved on the remote cloud. When the user wants to access the service or website the request is passed to cloud. All the key agreement and session establishment is done by a remote cloud. The user device has to perform fewer operations. The authentication of the user is done without manual interference. For measuring the performance multithread C# simulator is developed. The results show that the proposed APaaS is 2.6 times faster and it is more secure than other legacy systems.

(Mahmoud *et al.*, 2015)[46] presents the survey and analysis on the current status and concerns of the IoT security. IoT architecture has been explained which consist of three layers perception layer, network layer, and application layer. IoT security issues are also explained like confidentiality, integrity, availability, and authentication of data. The author also explains the security challenges faced in each layer and state-of-art security measures. Current mechanisms of data protection are only limited to authentication, identity establishment, and access control. Along with that future research, directions have also been proposed by the author.

Since IoT devices are resource constrained and have limited processing capabilities, so they utilize cloud computing for data storage and processing, however, the cloud paradigm has also some bottlenecks such as latency issue, bandwidth, etc (Guan *et al.*, 2018). [47] To overcome these problems, fog computing paradigm has been introduced which adds an extra layer between cloud and IoT devices to meet the challenges of lower latency, high performance, mobility, reliability, and security (Atlam, Walters and Wills, 2018).[48] In this regard, many researchers have provided the solution to enhance IoT security by using fog computing.

(Alharbi, Rodriguez and Maharaja, 2017) [49] have proposed a mechanism to secure the internet of things with the help of challenge-response protocol. The proposed system is called (FOCUS). The system consists of two main components VPN server and Challenge response. With the help of decision tree classification, malicious traffic sources can be detected. If the traffic comes from a trusted source then it will be allowed to access the VPN server, else challenge is sent to the IoT device. The device responds to the challenge, and if the response is correct then the source is considered as trusted otherwise not. The performance of the system is also checked by generating DDOS attacks. The results show that the proposed system effectively filter out the DDOS attacks and also has low response latency.

Alrawais et al. (2017) [50] have proposed a survey on the security and privacy issues in Fog computing. In this paper, the author discussed how fog computing can be used to distribute the certificate revocation information. There are four main entities IoT, Fog, Cloud, and Certification authority. The CA sends the updated list to the cloud that will further transfer it to fog nodes. The fog nodes use the bloom filter. The filter reduces the revocation list size. The integrity is preserved because of fog signatures. When the IoT device wants to communicate with each other the IoT device will check the device certificate status in the bloom filter. Analysis of the proposed scheme is also provided. The results have shown that the proposed mechanism provides an efficient distribution of certificate revocation information. However, maintaining and updating of certificate list file at the fog is a limitation in this solution.

(Mukherjee et al., 2017)[51] have discussed about the security concerns and issues present in Fog computing. Some of the issues that have been addressed are Trust which played two main roles: Firstly, if the IoT devices request the service, then the fog should be able to validate that the IoT devices are genuine and secondly that the fog nodes are secure. The author has also pointed out the question that how trust in fog service can be measured and what attributes define it,., Other issues included authentication, end-user privacy, and the establishment of secure communication between IoT devices and fog nodes, and from fog nodes to various other fog nodes. The author has also discussed the fog computing existing research and what are the open challenges that need to be solved further. Summary of the current work. The authors have concluded that trust, privacy, and authentication are a few of the major open challenges in the fog paradigm.

(Aazam, Zeadally and Harras, 2018) [52] have discussed the cloud-IoT integration issues and compared the fog and cloud performance using performance metrics. The performance is measured in terms of processing delay, processing cost, processing Capability, and task length. The performance was conducted by using toolkit called Cloudsim. In each simulation test, 200 runs were used. User can request the execution for each simulation run ranging from 10 BI to 30,000. The results show that fog computing reduces the processing delay but in terms of its efficiency there is a limit and it depends on the task length. If the length is greater than the processing difference between cloud and fog will be reduced. At the end the author also discusses the future research directions.

(Lu, Member and Heung, 2017) [53] presents a lightweight privacy scheme for fog computing enhanced IoT. The main objective focuses on privacy, security, efficiency and fault tolerance. The proposed Scheme uses hash functions, pillar holomorphic encryption, and Chinese Remainder Theorem. In the proposed, scheme trusted authority (TA) is responsible for bootstrapping the whole system. TA chooses the parameter and assigns to all entities. The IoT device at every time slot Ts will report its sensing data. After receiving the data in timeslot T the fog computing will check its validity. The control center after receiving data will perform some calculations to check the validity. The analysis shows that the proposed scheme easily detect the false data injection because of the hash function and there is less computation and communication overhead, it also identifies false data injection due to the one-way hash function.

The authors in (Ni et al. 2017) [54] have discussed the security issues of IoT with respect to fog computing. The author has initially discussed the fog computing and its architecture. Many real-time applications require billions of IoT devices to communicate with each other and share a huge amount of data however some of the features are unsupported such as location awareness, low latency which can cause serious concerns. Fog computing has played its role to solve some of these issues and provide the resources to the edge of the network however that are some security and privacy challenges. Several security threats have been identified and some solutions are proposed to address those concerns.

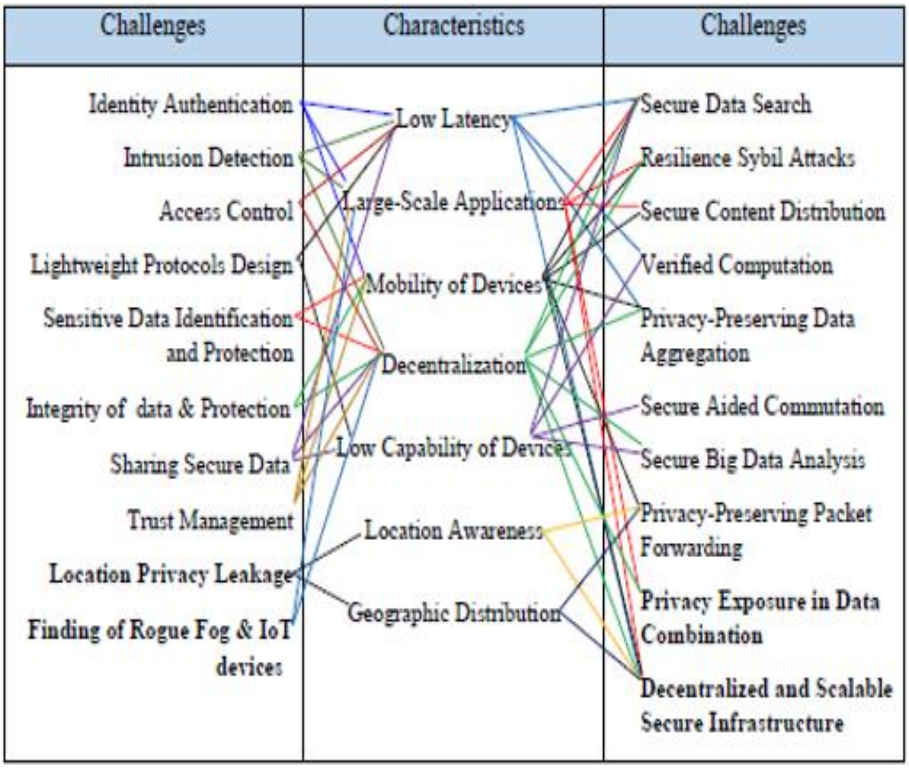


Table 2: Shows Relationship between security issues and Features in Fog comp proposed in (Ni et al. 2017)

The authors (AlNuaim and Ahmed, 2018) [55] have proposed an approach that provides security to cloud computing. In the proposed approach the client based authentication methodology was used at the fog layer. The IoT device will communicate with the cloud using the fog layer. In the proposed mechanism IoT device will send the unique number to fog which will send that number to the cloud. The cloud will generate the password against that number and send to the client using SMS. If the IoT device wants to access the service at cloud next time, it will send that password to fog which will further send that to the cloud. The cloud will match them if both of them matches then IoT device will be authenticated. The attacks that have been addressed in this paper is man-in-the-middle attack. The SMS based approach will prevent this attack.

(Abbasi and Shah, 2017) [56] have presented fog architecture critical analysis with respect to security. The authors have provided a critical analysis of work done since 2012. Authors have discussed that most of the techniques discussed in the papers do not provide simulation results and are limited to a few security features and none of the security systems provides the full security features.

(Stolfo, Salem and Keromytis, 2012) [57] have discussed that since the data stored in the cloud is transparent so malicious insider attack could occur. Existing mechanism has failed to protect against such attacks, hence author in this paper has proposed a new mechanism to mitigate insider data theft attack in the cloud. The proposed mechanism is a combination of two techniques. User behavior profiling technique and decoy technique. The data accessed in the cloud is being monitored to detect abnormal patterns. When unauthorized access is suspected then it is verified using the challenge question. Upon verification, disinformation attack is launched by using decoy technique. Experiments have also been conducted in local file settings. The experiment results show that this technique achieves equal or better results than search profiling approach alone. Simulation results are also provided. The overhead in the scheme is to maintain the bogus information that will be caused in case of uncertain behavior. The technique is also unable to detect that if the unexpected behavior is from the intended user or not, and will send the bogus information in both the cases.

IoT security can be increased by using blockchain technology. Blockchain is a decentralized ledger in which all the transactions are signed by using the private key. All the blocks contain the hash of the previous block making it tamper evident. As IoT devices generate a huge amount of data hence it is necessary that the data must be secured. Blockchain can provide the solution as there is no centralized entity involved also due to the decentralized nature there is no single point of failure Device identity validity can also be verified and as the transactions are signed by the private key hence it ensures that only the sender has sent it. (Kshetri 2017) [58]

(Qian *et al.*, 2018) [59] have discussed the different layers of IoT devices such as application layer, network layer, perception layer, and their corresponding security problems. As the IoT devices are increasing day by day hence in order to achieve identity authentication the traditional method requires trusted third party but with the incorporation of blockchain technology trusted third party can be eliminated also there is need to secure the transmitted data integrity. The blockchain technology when combined can help us to secure the IoT data Fig 15. Shows how blockchain technology can strength the IoT devices. It shows the IoT devices threat traceability includingthe interaction between IoT devices and network and IoT devices and cloud.

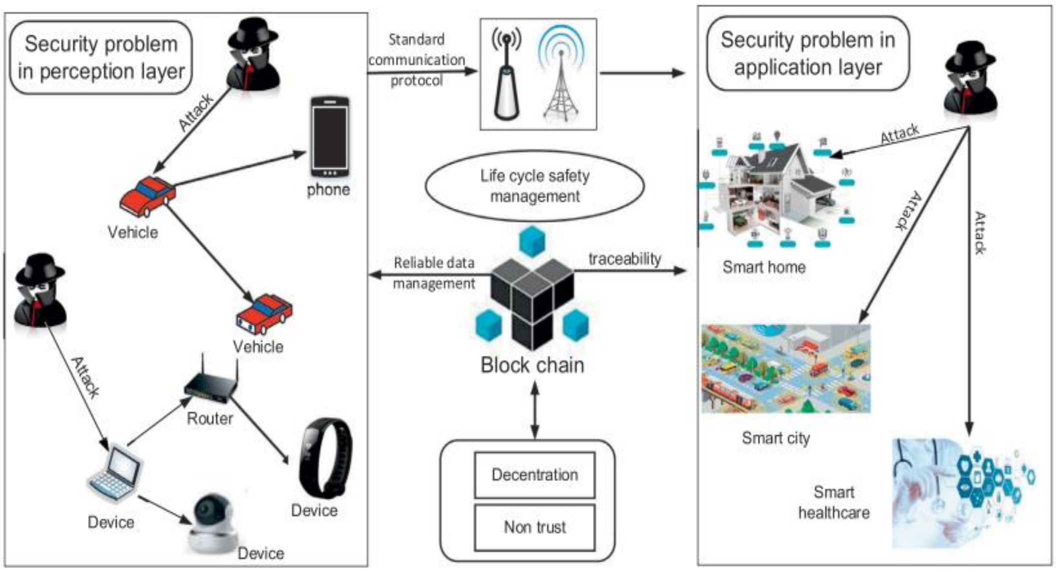


Fig 15: Blockchain enhanced IoT Security architecture. Ref. image from (Qian *et al.*, 2018)

(Li *et al.*, 2018) [60] have proposed a blockchain mechanism for authentication of IoT devices. The author has explained that the existing authentication mechanisms depend upon the CA which can suffer from a single point of failure hence blockchain based decentralized method has been proposed. In the proposed method IoT device will register its credentials on the blockchain so that without the third party they can be authenticated. The authentication of the IoT device is done using the verification of registration information published in the blockchain. In order to preserve the data integrity, the hash of the data is also uploaded into the blockchain. The proposed system verification is also done by implementing a prototype based on the Hyperledger Fabric. The blockchain has been deployed on the raspberry pi. Consensus algorithm that has been used is PBFT. The proposed system can prevent malicious nodes from intruding. If some of the nodes suffer from a DDOS attack, the system will still work due to the decentralized ledger.

The authors (Lee and Kim, 2018) [61] have proposed an authentication mechanism through zero-knowledge proof to authenticate the IoT devices because when device information is put on to the blockchain personal information can be leaked through proof of work. The author has first explained the device authentication and sequence diagram. In the proposed system if the verifier knows the address, personal information can be leaked. To mitigate that author has proposed zero-knowledge protocol in which public key is stored on the blockchain while the original data is stored on the database also privacy is been protected because original data is not published on the blockchain. Implementation has also been done which shows that if the data has been tempered it will be detected.

(Huh, Cho and Kim, 2017) [62] have proposed a mechanism in which the IoT devices are managed by using the blockchain technology. In the proposed approach smartphone along with three raspberry pi has been used to keep the track of electricity used, air conditioner and light bulb. With the help of smart contract, the user has set up the policy, as data is stored on distributed ledger so it can't tamper easily. Three Smart contracts have been written. For the validation of the account signature, the public key has also been added to smart contracts. All the values coming from the devices are checked through the signature. Simulation and experimental results have also been discussed. At the end of the paper, some weakness has also been discussed during development for which there is a need to investigate further and to find the solutions.

(Samaniego and Deters, 2017) [63] evaluates the use of cloud computing and fog computing as a hosting platform for the blockchain. The main key challenge is where it should be deployed since fog is an extension of cloud computing but has limited resources. On the other hand, cloud has unlimited resources but there are some issues such as latency, real-time monitoring. So to evaluate the use of both, set of experiments were performed. The result of the experiment shows that although cloud has unlimited resources fog outperforms the cloud due to the latency factor hence it is more feasible to host blockchain on fog computing.

Table 3: Comparative analysis of literature review papers

Authors	Title of Paper	Features Addressed	Proposed Scheme	Limitations
Alrawais et al. (2017)	Security and Privacy Issues for the Internet of Things in Fog Computing	Non-repudiation	Bloom filter	Maintaining and updating of list at the fog layer
(Luo *et al.*, 2016)	Fog computing with the face identification and resolution framework	Integrity Availability Confidentiality	Authentication and session key agreement	Increases computation and communication overhead
(Lu, Member and Heung, 2017)	A Lightweight Privacy-Preserving Scheme for Fog Computing-Enhanced IoT	Integrity Privacy	Homomorphic Paillier encryption Hash function	Traceability has not been considered
(Stolfo, Salem and Keromytis, 2012)	Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud	Control data access	User behavior profiling Decoy Technique	Maintaining bogus information
(Science *et al.*, 2018)	An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology	Authentication Authorization	Out of band channel for secondary authentication Supported by blockchain technology	Increases communication overhead.
(Basudan, Lin and Sankaranarayanan, 2017)	Vehicular crowdsensing using fog computing	Integrity Confidentiality Authenticity	Certificateless Aggregate signcryption	Location privacy has not been considered.

Chapter 4

Secure and Trusted Framework for IoT

4.1 Framework

This section presents a secure and trusted framework for the IoT network based on blockchain technology. Blockchain is a distributed ledger which eliminates the need of trusted third party and can be used for identity authentication and security protection of IoT devices. A typical IoT network comprises of sensors that sense the real-time data from the environment and transfers that data to the fog layer that is an intermediary layer between IoT device and cloud layer. The data is analyzed and processed at the fog layer and consequently, the filtered data is sent to the cloud layer through a secure communication channel. A secure framework and secure communication protocol is proposed that ensures the following security requirements (a) Authentication: The data must be submitted by an authentic IoT device, (b) Integrity: The data transmitted by the IoT device should not be altered, (c) Non-Repudiation: The IoT device should not deny the fact that it has generated the data. The abstract level architecture of the proposed secure and trusted IoT framework is illustrated in Fig.16

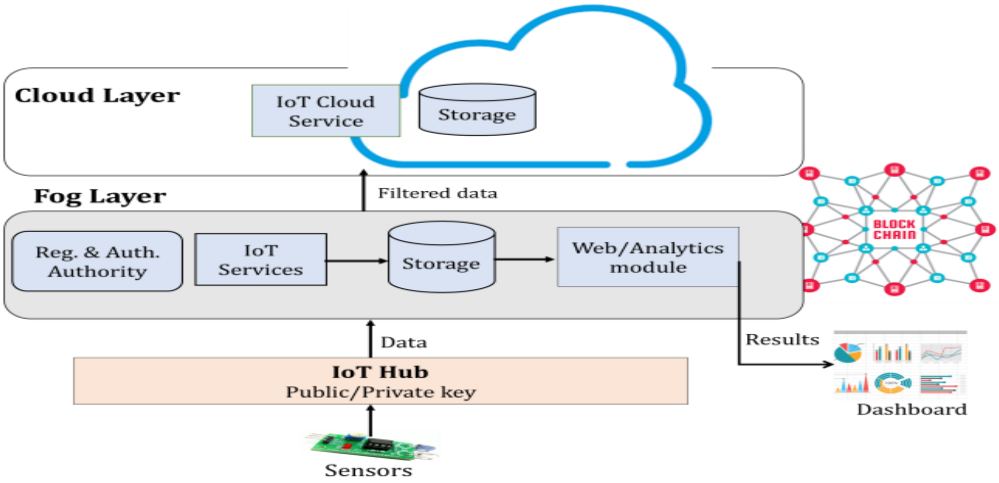


Fig 16: Secure and trusted abstract level IoT framework

The framework comprises of three layers including the IoT layer, the fog layer, and the cloud layer. The IoT layer consists of sensors that sense the real-time data from the environment but as these sensors are resource constrained and have limited processing capabilities, therefore, these sensors are connected to the sensor hub. A sensor hub is basically a point of connection for multiple sensors. Some of the workload has been shared by the sensor hub. In order to ensure the integrity and non-repudiation of data generated by the sensor, the sensor hub signs the data with the private key corresponding to that sensor and transmits the data to the middle layer known as fog layer. Fog layer provides services to the IoT devices at the edge of the network. Fog layer also includes registration authority and storage server. For creating the trusted and decentralized environment blockchain technology is also deployed at the fog layer. Verifiable identities are also managed by using the blockchain technology at the fog layer. The IoT devices are only allowed to access the service at the fog layer once they are authenticated and verified. After receiving the data from the authentic IoT device, the fog layer performs some analysis and filtering over the data. The web module at the fog layer is connected to the decision panel that shows the analysis performed over the data. The useful data is then sent to the cloud for permanent storage. In order to do that the fog layer authenticates itself to the cloud layer. The authentication of the fog layer with the cloud layer is done in the same manner as the IoT device authenticates itself to the fog layer. After successfully authenticating itself with the cloud layer, the fog layer sends only the useful data along with the digital signature and block id to the cloud layer. The integrity of data sent by the fog layer can be checked easily since the block id contains the corresponding filtered data hash.

4.1.1 Components of the Framework

The framework comprises of three layers including the IoT layer, the fog layer, and the cloud layer. Each layer consists of different components such as the IoT layer consist of sensors that are connected to the IoT hub, the fog layer consists of registration and authentication authority, Storage, web/analytics module, blockchain, and the cloud layer consist of storage component. The description of each of the component is given below.

a) IoT Hub

This component is present at the IoT layer that consists of sensors but as these sensors are resource constrained and have limited processing capabilities, therefore, these sensors are connected to the sensor hub. A sensor hub is basically a point of connection for multiple sensors. Some of the workload has been shared by the sensor hub. In order to ensure the integrity and non-repudiation of data generated by the sensor, the sensor hub signs the data with the private key corresponding to that sensor and transmits the data to the middle layer known as fog layer.

b) Registration and Authentication Authority

This component is deployed at the fog layer that is an intermediate layer between the IoT device and cloud layer and provides services to the IoT device at the edge of the network. This component is responsible for registering the IoT devices. The registration information is stored in the local registration repository. After the successful registration, the IoT hub performs basic authentication with this component using basic credentials. Upon successful authentication, this component creates a verifiable identity by digitally signing it and sends it to the IoT hub.

c) Storage

This component is responsible for storing the data and is present at the fog layer. When the IoT hub sends the data to the fog layer, fog layer stores that data in the local database server.

d) Web/Analytics Module

This component is present at the fog layer and is connected to the dashboard. When the fog layer receives the data from the authentic IoT hub, it performs some analysis and filtering over the data. The purpose of this component is to show the analysis performed over the data.

e) Blockchain

Blockchain is a circulated record innovation developed from Bitcoin and other digital forms of money. The blockchain is fundamentally a changeless, decentralized furthermore, open accessible shared database. In the blockchain, all exchanges are recorded and anybody in the framework is permitted to get to, send and check these exchanges.

For creating the trusted and decentralized environment blockchain technology is deployed at the fog layer. It is a decentralized ledger that eliminates the need for trusted third party. The purpose of this component is to manage the verifiable identities uploaded by the IoT hub.

4.1.2 Initial Setup

a) Registration

The owner of the IoT device registers himself to the registration authority which is deployed at the fog layer in our architecture. For successful registration, the owner provides basic credentials such as id, name, password, email, etc. After that, the IoT hub performs basic authentication with registration authority using basic credentials provided by the owner of the IoT device in the form of configuration. Upon successful authentication, the registration authority creates a verifiable identity which is digitally signed by it and sends back to the IoT hub.

b) Key Generation

Each layer (IoT, Fog, and Cloud) will generate public/ private key pairs from their corresponding security module. The public key is used for encryption process and it is known to everyone, whereas the private key is used for decryption and it is kept secret. The same key pair may be used for digital signature generation.

c) Credentials Management

The registration credentials e.g. id, password, email, resource name, etc. of IoT devices are managed at the fog layer by the registration authority in the local registration repository. These credentials are stored in encrypted form, similarly, when the fog device registers itself with the cloud layer, the registration credentials of fog device is stored in the cloud in an encrypted form. In addition to that, each layer stores the private key locally whereas the public key is shared globally with other partners.

Chapter 5

Security Protocols for IoT

The protocol provides an end-to-end sure communication and transmission of data generate from IoT devices to the Fog layer and the Cloud layer satisfying the following security requirements (i) Authentication: The data should be uploaded by an authentic IoT device (ii) Integrity: The data transmitted by the device should not be changed (iii) Non-Repudiation: The device should not deny the fact that it has generated the data. The complete communication process including the exchange of secure messages between various entities of the secure and trusted framework including the IoT devices, Fog layer that includes Registration authority, IoT service, blockchain verification service, and Cloud layer has been illustrated in Fig. 17.

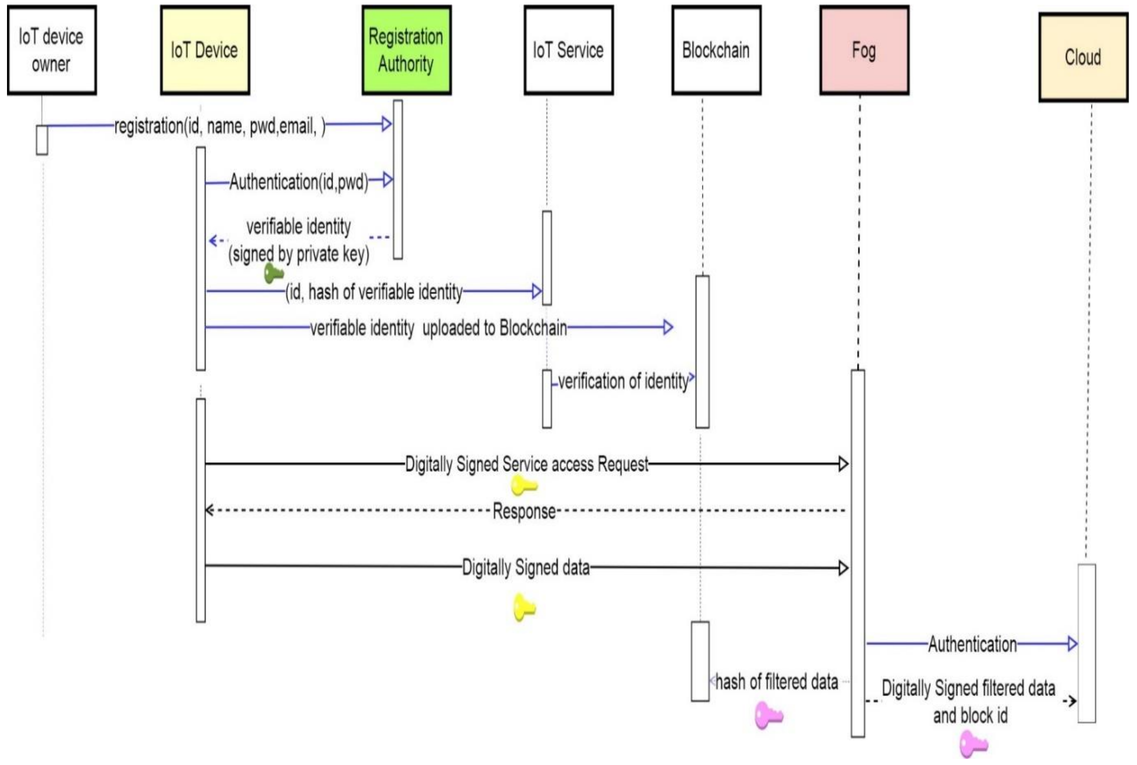

IoT device owner
IoT Device
Registration Authority
IoT Service
Blockchain
Fog
Cloud
registration(id, name, pwd,email,)
Authentication(id,pwd)
verifiable identity (signed by private key)
(id, hash of verifiable identity
verifiable identity uploaded to Blockchain
verification of identity
Digitally Signed Service access Request
Response
Digitally Signed data
Authentication
hash of filtered data
Digitally Signed filtered data and block id

Fig 17: Secure and trusted communication protocol for IoT network

The complete process of the communication and description of each of the entity involved in the Communication process of the secure and trusted framework is given in the section below.

1. Protocol 1: Registration and Basic Authentication

In the first phase of the protocol, the IoT device owner registers itself to the registration authority, deployed at the fog layer. In this phase, the owner provides basic credentials for the registration such as id (this id is device id), name, password, email, etc. After the successful registration, the registration authority sends the response to the IoT device owner. The owner then configures the IoT hub with id, password. After successful configuration IoT hub sends the basic credentials for the authentication to the registration authority. It also sends nonce to protect from replay attack and timestamp for the synchronization. The registration authority verifies those credentials e.g. id, password from local registration repository. If both of them matches it means that IoT hub has successfully authenticated itself. The registration authority then sends the response to the IoT hub. Steps required for registration and basic authentication is shown in Fig.18

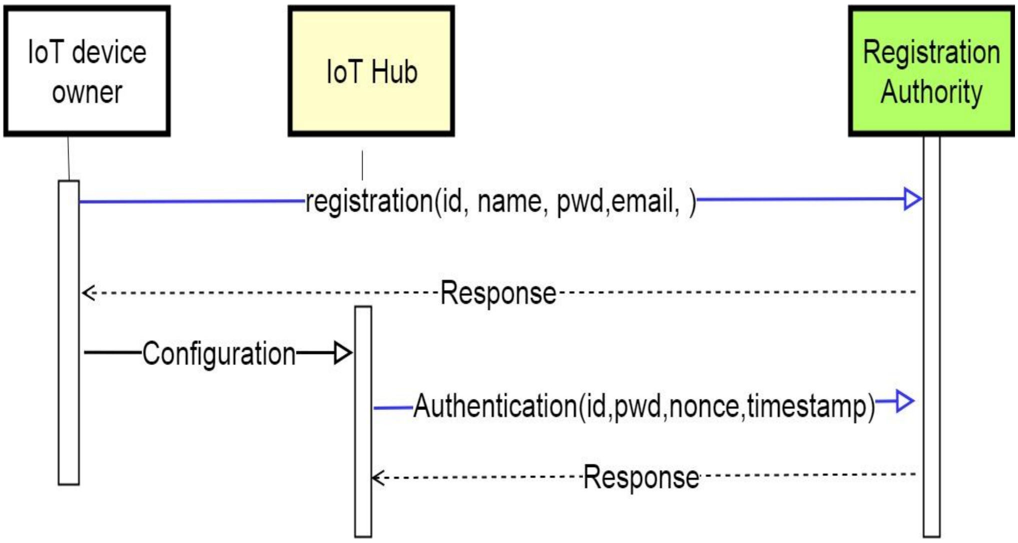


Fig 18: Protocol for registration and basic authentication

2. Protocol 2: Verifiable Identity-based Authentication

After successful basic authentication, the registration authority creates a verifiable identity by digitally signing it and sends it to the IoT hub. To protect from the replay attack and for the synchronization it also sends nonce and timestamp to the IoT hub. The IoT hub receives verifiable identity and then publishes it in the blockchain. It also sends the hash of verifiable identity along with its anonymous id to the Rest based service for onward authentication. In order to verify identity, the service will match the identity in the blockchain with the ones that is previously uploaded by the IoT hub. Complete steps for verifiable identity-based authentication is shown in Fig 19.

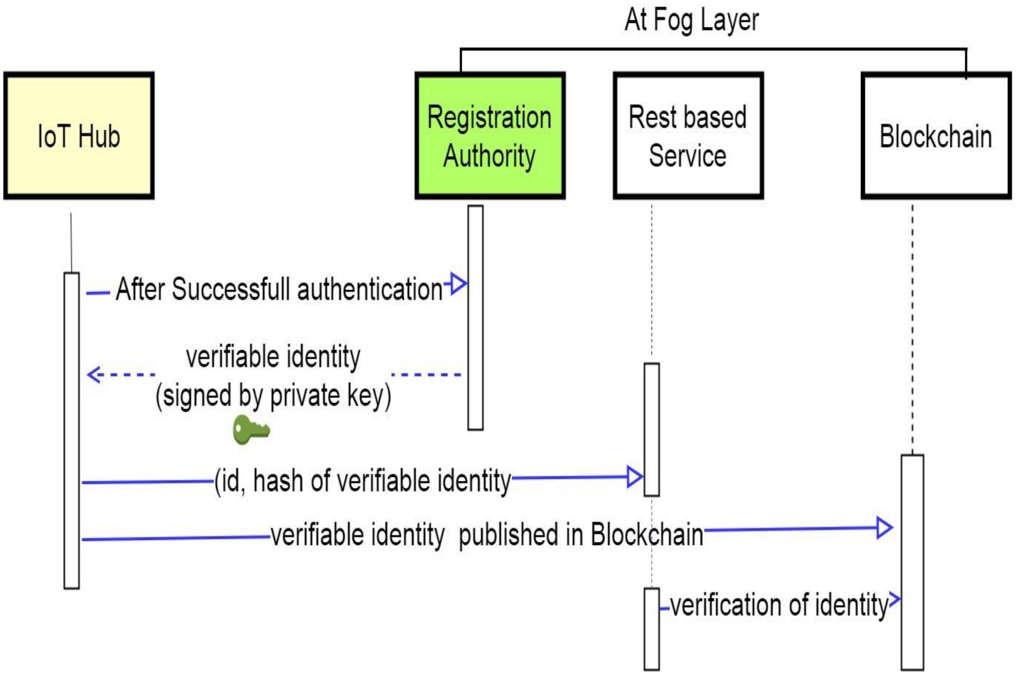

At Fog Layer
IoT Hub
Registration Authority
Rest based Service
Blockchain
After Successfull authentication
verifiable identity (signed by private key)
(id, hash of verifiable identity
verifiable identity published in Blockchain
verification of identity

Fig 19: Verifiable identity-based authentication

3. Protocol 3: IoT Device Signature Verification

The IoT hub sends a service request, digitally signed to the fog layer. This service request includes demand for storage, filtering or analysis of data. The fog layer verifies the signature of the IoT hub by taking the public key from that verifiable identity that is present in the blockchain. After verifying the signature of the IoT hub fog layer sends the response. Protocol for the signature verification is illustrated in Fig 20.

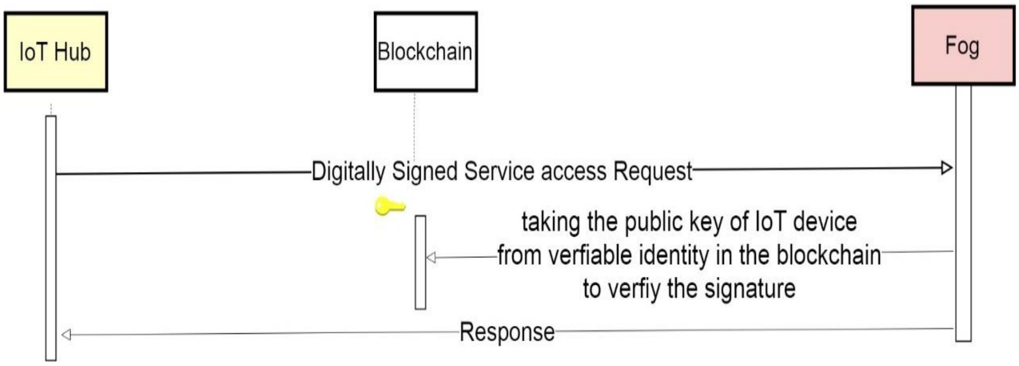

IoT Hub
Blockchain
Fog
Digitally Signed Service access Request
taking the public key of IoT device from verfiable identity in the blockchain to verfiy the signature
Response

Fig 20: IoT device signature verification protocol

4. Protocol 4: Data Uploading on Fog Layer

After successfully authenticating itself, the IoT hub is allowed to access the service at the fog layer. The IoT hub sends the digitally signed data to the fog layer. The fog layer analyzes that data and performs some filtering over the data. In order to protect the privacy, original data is not stored on the blockchain it is stored on the local database server. For data integrity, the corresponding filter data hash is uploaded to the blockchain as illustrated in Fig 21.

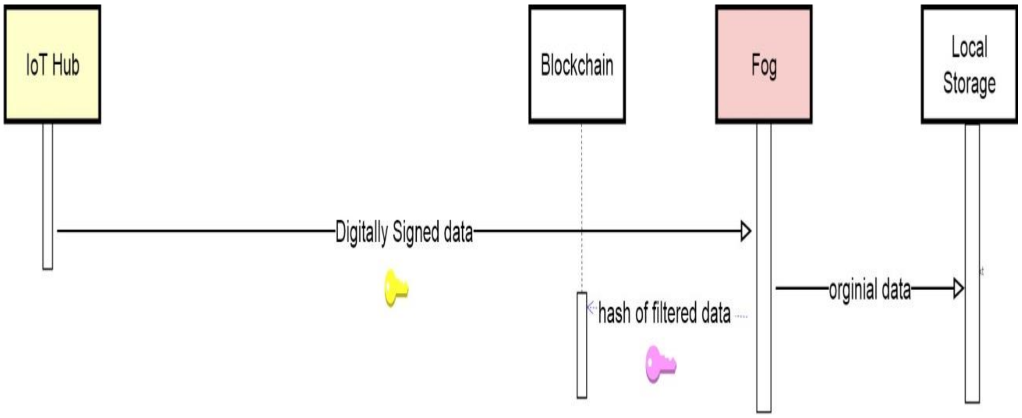


Fig 21: Data uploading on Fog layer protocol

5. Protocol 5: Data Uploading to Cloud Layer

For sending the filtered data to the cloud layer the fog layer first authenticates itself to the cloud layer in the same manner as IoT device does to fog. After successfully authenticating itself with the cloud layer the fog layer is now allowed to send the important data to the cloud. The fog layer sends the filtered digitally signed data and block id to the cloud layer as illustrated in fig 22. The integrity of data send by fog can be checked easily since the block id contains the corresponding hash of the useful data in the blockchain as no one can change it because it is a temper proof ledger

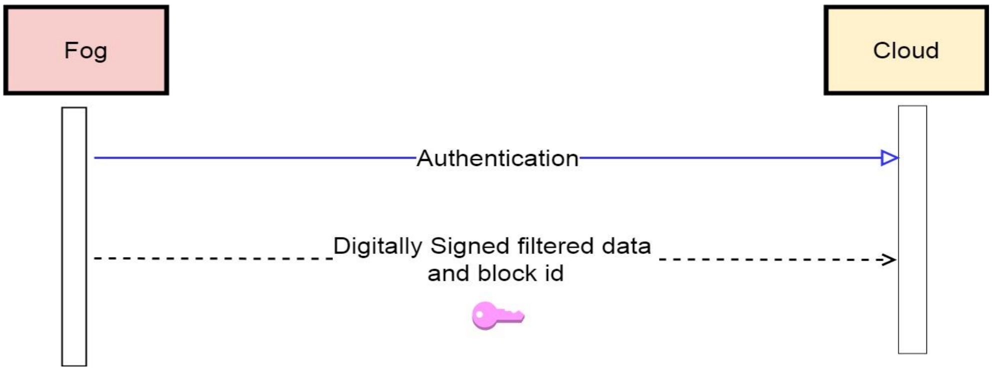


Fig 22: Data uploading on Cloud layer protocol

Chapter 6

Formal Verification of Security Protocol

The proposed secure and trusted protocol for IoT devices is verified using an automated security verification tool called *Scyther*. The tool is primarily based on a sample refinement algorithm

that permits unbounded verification, falsification, and characterization. A lot of new features are provided, that are not offered by the other tools. Security protocols can be verified in two different ways. First Scyther scripts can be executed through the command-line interface in which an output file is provided that contains the result of protocol verification. The second option is to use a Graphical User Interface in which the panel is provided for both verification results and attacks that are found if any.

6.1 Scyther Specification Language

Scyther uses its own specification language that resembles most of the popular languages such as C, C++, or JAVA. Its main purpose is to describe the protocols that are defined by a set of roles which in turn are defined by the sequence of events. The input language of the Scyther is case sensitive.

6.1.1. Roles

In the proposed End-to-End Secure and Trusted Protocol for the IoT devices we have defined six roles that are as follows:

1. IoT device

2. Registration authority

3. IoT Service

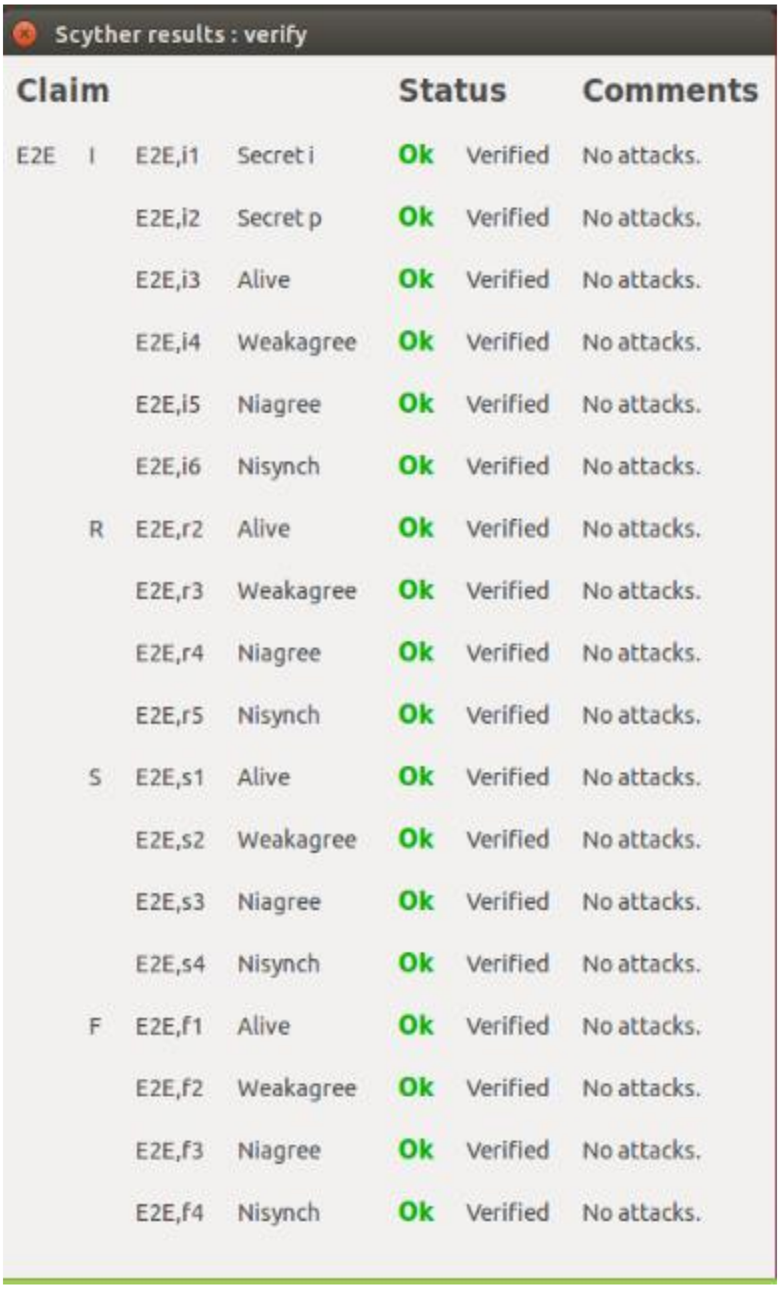
4. Blockchain

5. Fog

6. Cloud

For each of the different roles in the protocol, behavior can be added as a sequence of send and receive events, as well as variable declarations, constants, and claims.

6.2 Results



Scyther results : verify

Claim				Status		Comments
E2E	I	E2E,i1	Secret i	Ok	Verified	No attacks.
		E2E,i2	Secret p	Ok	Verified	No attacks.
		E2E,i3	Alive	Ok	Verified	No attacks.
		E2E,i4	Weakagree	Ok	Verified	No attacks.
		E2E,i5	Niagree	Ok	Verified	No attacks.
		E2E,i6	Nisynch	Ok	Verified	No attacks.
	R	E2E,r2	Alive	Ok	Verified	No attacks.
		E2E,r3	Weakagree	Ok	Verified	No attacks.
		E2E,r4	Niagree	Ok	Verified	No attacks.
		E2E,r5	Nisynch	Ok	Verified	No attacks.
	S	E2E,s1	Alive	Ok	Verified	No attacks.
		E2E,s2	Weakagree	Ok	Verified	No attacks.
		E2E,s3	Niagree	Ok	Verified	No attacks.
		E2E,s4	Nisynch	Ok	Verified	No attacks.
	F	E2E,f1	Alive	Ok	Verified	No attacks.
		E2E,f2	Weakagree	Ok	Verified	No attacks.
		E2E,f3	Niagree	Ok	Verified	No attacks.
		E2E,f4	Nisynch	Ok	Verified	No attacks.

Fig23: Protocol verification results

6. 3. Analysis of Protocol

Scyther. Since the protocol is based on multi-party communication, therefore, we created various roles in the protocol as shown in Appendix A. In this code:

- I represents IoT Device
- R represents Registration Authority
- S represents REST based services which communicates with Blockchain network for performing transactions to store IoT device's credentials
- B represents Blockchain network
- F represents Fog Computing Layer
- C represents Cloud Computing Layer

In order to test the various objectives defined in this paper for authentication and non-repudiation, various claims are made in this verification code which is tested by the Scyther: The protocol is verified according to the following Scyther attributes: Secrecy, Aliveness, Weak agreement, Non-injective Agreement, Non-injective Synchronization

Secrecy:

It is the most trivial security claim as it states that the property must be kept hidden from the adversary. When the IoT device authenticates itself using the credentials e.g. id, password it is important that those credentials are not revealed to an intruder because if the intruder stole those credentials then he can launch an impersonation attack. Since in the proposed "secure and trusted protocol for IoT devices", the data is encrypted hence both id, and password is confidential, and the results show that no attacks are found against this claim.

Aliveness:

Aliveness is considered to be the weakest form of authentication. This claim guarantees to the initiator (talking agent) about the aliveness of responder (communicating party) which means that if whenever the initiator completes the protocol with the responder then the responder has previously executed the protocol. However, this doesn't mean that the responder knew that he was running the protocol with the initiator also the protocol may have not been run recently by the responder. The proposed protocol fulfills the aliveness claim against different roles as shown in fig 23. and the results show that no attack was found against this claim.

Weak agreement:

Since the authentication form introduced as aliveness is considered to be the weakest form hence it is strengthened by the weak agreement which states that if the initiator completes the protocol with the responder then the responder has previously executed the protocol and it also guarantees that the responder knew that he was running the protocol with the initiator. Such a claim would prevent an adversary from acting as a responder by running another run of the protocol in parallel with an initiator and conducting a man-in-the-middle-attack. The proposed protocol also fulfills the weak agreement claim against different roles because the messages are digitally signed and encrypted and no attack was found against this claim also.

Nisynch

It is used to ensure that the communication between sender and receiver is synched and sent by the sender. As shown in figure 23, the designed protocol fulfills this property since the protocol uses the timestamps.

Niagree

This claim ensures that the non-injective property is achieved to protect the protocol from replay attack. The verification results show that the designed protocol is protected against the replay attacks since the protocol uses nonce (random number used once).

Chapter 7

Conclusion and Future Work

Today, IoT devices play a significant role in industries, automated solutions, businesses and almost every aspect of a person's life. These devices are the main source of generating a huge amount of data, which needs to be processed, stored in a secure manner and presented in an interpretable form. Since IoT devices are resource constrained and have limited processing capabilities, so they utilize cloud computing for data storage and processing, however, the cloud paradigm has also some bottlenecks such as latency issue, bandwidth, etc. To overcome these problems, fog computing paradigm has been introduced which adds an extra layer between cloud and IoT devices to meet the challenges of lower latency, high performance, mobility, reliability, and security. However, the integration of the aforementioned technologies including IoT network, fog and cloud computing have posed new security risks and challenges. Authentication and source verification being some of the foremost.

So in this regard, we have proposed a secure and trusted framework for the IoT network that satisfies the multiple security requirements such as authentication, integrity, non-repudiation. The components of the framework and communication between them have also been discussed in detail. In order to create a trusted decentralized environment to strength the IoT security, the blockchain technology is also deployed at the fog layer. After designing the protocol we have verified it using the security verification tool Scyther. The results show that the protocol provides security against multiple attacks. For building trust between the components and verification it still needs public key infrastructure which is the limitation of this solution. In future our objective is to extend this solution to introduce VeidBlock for the authorization services.

References

[1] S. Karthikeyan, R. Patan, and B. Balamurugan, *Recent Trends in Communication, Computing, and Electronics*, vol. 524. Springer Singapore, 2019.

[2] and X. C. 2017. "Fog C. for the I. of T. S. and P. I. . I. I. C. 21 (2):34–42. https://doi. org/10. 1109/MIC. 2017. 37. Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, "No Title."

[3] no. M. https://doi. org/10. 1109/W.-I. 2014. 6803174. Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. 2014. "A Survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services." 2014 IEEE World Forum on Internet of Things, WF-IoT 2014, "No Title."

[4] "No Title," *Yi, Shanhe, Cheng Li, Qun Li. 2015. "A Surv. Fog Comput. Proc. 2015 Work. Mob. Big Data - Mobidata '15, no. June 201537–42. https//doi.org/10.1145/2757384.2757397.*

[5] P. Singhal, P. Sharma, and B. Hazela, *International Conference on Innovative Computing and Communications*, vol. 55. Springer Singapore, 2019.

[6] 1–5. https://doi.org/10.1109/CCNC.2018.8319238. Alharbi, Salem, Peter Rodriguez, Rajaputhri Maharaja, Prashant Iyer, Nivethitha Bose, and Zilong Ye. 2018. "FOCUS: A Fog Computing-Based Security System for the Internet of Things." 2018 15th IEEE Annual Consumer Communications & Networking Conference (CC, "No Title."

[7] and A. . I. I. of T. J. 4 (5):1125–42. https://doi. org/10. 1109/JIOT. 2017. 2683200. Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. 2017. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, "No Title."

[8] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal And Zied Chtourou, "*A Roadmap For Security* 632 *Challenges In Internet Of Things*", Digital Communications And Networks, Volume 4, Issue 2, pages 633 118-137, April 2018.

[9] and Y. L. 2017. "Cost-E. S. for R. R. S. in M. S. N. . I. T. on V. T. 66 (3):2789–2800. https://doi. org/10. 1109/TVT. 2016. 2585591. He, Zaobo, Zhipeng Cai, Jiguo Yu, Xiaoming Wang, Yunchuan Sun, "No Title."

[10] "No Title," *Dastbaz, Mohammad, Hamid Arab. Babak Ahgkar. 2017. "Technology Smart Futur. Technol. Smart Futur. 1–363. https//doi.org/10.1007/978-3-319-60137-3.*

[11] and P. S. 2015. "Stream P. of H. S. D. S. U. T. to I. C. from a B. D. P. . P. C. S. 52 (1):1004–9. https://doi. org/10. 1016/j. procs. 2015. 05. 093. Cortés, Rudyar, Xavier Bonnaire, Olivier Marin, "No Title."

[12] D. &amp; W. T. 17:849–54. https://doi. org/10. 1007/97.-3-319-75928-9. Ogiela, Marek R, and Lidia Ogiela. 2018. "Advances in Internet, "No Title."

[13] 19293–304. Mukherjee, Mithun, and Rakesh Matam. 2017. "Security and Privacy in Fog Computing : Challenges, "No Title."

[14] and S. A. 2018. "Fog C. A. N. A. to P. S. in C. C. . I. J. of S. and T. 11 (15):1–6. https://doi. org/10. 17485/ijst/2018/v11i15/119540. AlNuaim, Abdullah, "No Title."

[15] HS Technology, "IoT platforms: enabling the Internet of Things," *IHS Technol.*, vol. Whitepaper, no. March, pp. 1–19, 2016.

[16] Z. Alansari, S. Soomro, M. R. Belgaum, and S. Shamshirband, "The Rise of Internet of Things (IoT) in Big Healthcare Data: Review and Open Research Issues View project Annals of Emerging Technologies in Computing (AETiC) View project The Rise of Internet of Things (IoT) in Big Healthcare Data: Review and Open Resear," no. September 2017, 2016.

[17] S. K. Datta, C. Bonnet, and J. Haerri, "Fog Computing architecture to enable consumer centric Internet of Things services," *Proc. Int. Symp. Consum. Electron. ISCE*, vol. 2015-August, pp. 2014–2015, 2015.

[18] C. P. Mayer, "Security and Privacy Challenges in the Internet of Things Security and Privacy Challenges in the Internet of Thing," *Electron. Commun. EASST*, vol. 17, pp. 1–13, 2009.

[19] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) Security : Current Status , Challenges and Prospective Measures," pp. 336–341, 2015.

[20] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," *Futur. Gener. Comput. Syst.*, vol. 56, pp. 684–700, 2016.

[21] NIST, "https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published."

[22] A. A. Lisbon, "A Study on Cloud and Fog Computing Security Issues and Solutions," *Int. J. Innov. Res. Adv. Eng.*, vol. 03, no. 4, pp. 2349–2163, 2017.

[23] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 27–33, 2010.

[24] A. Mohammad *et al.*, "Cloud Computing : Issues and Security Challenges," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 2, pp. 2015–2017, 2017.

[25] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, "Fog Computing: Principles, architectures, and applications," *Internet Things Princ.*

Paradig., pp. 61–75, 2016.

[26] S. Yi and and Q. L. , Zhengrui Qin, "Security and Privacy Issues of Fog Computing: A Survey," *Springer Int. Publ. Switz. 2015*, no. WASA 2015, LNCS 9204, pp. 685–695, 2015.

[27] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," *Proc. 2015 Work. Mob. Big Data - Mobidata '15*, pp. 37–42, 2015.

[28] L. M. Vaquero, L. Rodero-Merino, and L. Rodero-Merino Gradiant Vigo, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, 2014.

[29] S. J. Stolfo, M. Ben Salem, and A. D. Keromytis, "Fog computing: Mitigating insider data theft attacks in the cloud," *Proc. - IEEE CS Secur. Priv. Work. SPW 2012*, pp. 125–128, 2012.

[30] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, 2017.

[31] M. Aazam and E. N. Huh, "Fog computing and smart gateway based communication for cloud of things," *Proc. - 2014 Int. Conf. Futur. Internet Things Cloud, FiCloud 2014*, pp. 464–470, 2014.

[32] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Big Data and Internet of Things: A Roadmap for Smart Environments," vol. 546, pp. 169–186, 2014.

[33] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," *Proc. - 3rd Work. Hot Top. Web Syst. Technol. HotWeb 2015*, pp. 73–78, 2016.

[34] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017.

[35] J. Xie *et al.*, "A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," *IEEE Commun. Surv. Tutorials*, vol. PP, no. c, pp. 1–1, 2019.

[36] Zheng, Z., Xie, S. and Dai, H. (2018) 'Blockchain challenges and opportunities : a survey',
(October). doi: 10.1504/IJWGS.2018.10016848.

[37] Narayanan, A. *et al.* (2016) 'Bitcoin and Cryptocurrency Technologies'.

[38] Id, A. P. and Tapas, N. (2018) *Blockchain and IoT Integration : A Systematic Survey*. doi:
10.3390/s18082575.

[39] Dorri, A. *et al.* (2017) 'Blockchain for IoT Security and Privacy : The Case Study of a Smart Home'.

[40] Alharby, M. and Moorsel, A. Van (2017) ‘B LOCKCHAIN -BASED SMART CONTRACTS : A SYSTEMATIC MAPPING S TUDY’, pp. 125–140.

[41] Cheng, J. *et al.* (2018) ‘Blockchain and Smart Contract for Digital Certificate’, *2018 International Conference on Applied System Invention (ICASI)*. IEEE, pp. 1046–1051.

[42] J. A. Jaoude and R. Saade, “Business Applications of Blockchain Technology -A Systematic Review,” *IEEE Access*, vol. PP, no. c, pp. 1–1, 2019.

[43] R. Jayaraman, K. Saleh, and N. King, “Improving Opportunities in Healthcare Supply Chain Processes via the Internet of Things and Blockchain Technology,” *Int. J. Healthc. Inf. Syst. Informatics*, vol. 14, no. 2, pp. 49–65, 2019.

[44] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, “Identity-based authentication scheme 600 for the Internet of Things,” in *Proceedings - IEEE Symposium on Computers and Communications*, 601 2016, vol. 2016–Augus, pp. 1109–1111

[45] J. B. Abdo, “Authentication proxy as a service,” *2017 2nd Int. Conf. Fog Mob. Edge Comput. FMEC 2017*, pp. 45–49, 2017.

[46] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of Things (IoT) Security : Current Status , Challenges and Prospective Measures,” *Icitst*, 2015.

[47] Y. Guan, J. Shao, G. Wei, and M. Xie, “Data Security and Privacy in Fog Computing,” *IEEE Netw.*, vol. 32, no. 5, pp. 106–111, 2018.

[48] H. Atlam, R. Walters, and G. Wills, “Fog Computing and the Internet of Things: A Review,” *Big Data Cogn. Comput.*, vol. 2, no. 2, p. 10, 2018.

[49] S. Alharbi, P. Rodriguez, and R. Maharaja, “Secure the Internet of Things with Challenge Response Authentication in Fog Computing,” pp. 7–8, 2017.

[50] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, “Fog Computing for the Internet of Things : Security and Privacy Issues,” 2017.

[51] M. Mukherjee *et al.*, “Security and Privacy in Fog Computing: Challenges,” *IEEE Access*, vol. 5, pp. 19293–19304, 2017.

[52] M. Aazam, S. Zeadally, and K. A. Harras, “Fog Computing Architecture , Evaluation , and Future Research Directions,” no. May, pp. 46–52, 2018.

[53] R. Lu, S. Member, and K. Heung, “A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT,” vol. 5, 2017.

[54] J. Ni, S. Member, K. Zhang, X. Lin, and X. S. Shen, “Securing Fog Computing for Internet of Things Applications : Challenges and Solutions,” no. c, 2017.

[55] A. AlNuaim and S. Ahmed, “Fog Computing: A Novel Approach to provide Security in Cloud Computing,” *Indian J. Sci. Technol.*, vol. 11, no. 15, pp. 1–6, 2018.

[56] B. Z. Abbasi and M. A. Shah, "Fog Computing: Security Issues, Solutions and Robust Practices," pp. 7–8, 2017.

[57] S. J. Stolfo, M. Ben Salem, and A. D. Keromytis, "Fog computing: Mitigating insider data theft attacks in the cloud," *Proc. - IEEE CS Secur. Priv. Work. SPW 2012*, pp. 125–128, 2012.

[58] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," no. August, 2017.

[59] Y. Qian *et al.*, "Towards decentralized IoT security enhancement: A blockchain approach," *Comput. Electr. Eng.*, vol. 72, pp. 266–273, 2018.

[60] Li, D. et al. (2018) 'A Blockchain-Based Authentication and Security Mechanism for IoT', 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6. doi: 10.1109/ICCCN.2018.8487449.

[61] C. H. Lee and K. Kim, "Implementation of IoT System using BlockChain with Authentication and Data Protection," pp. 936–940, 2018.

[62] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 464–467, 2017.

[63] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," pp. 433–436, 2016.

[64] L. F. Bittencourt et al., "The Internet of Things, Fog and Cloud Continuum: Integration and 551 Challenges," 2018.

[65] Minhaj Ahmad Khan, Khaled Salah "IoT security: Review, blockchain solutions, and open 635 challenges", Future Generation Computer Systems, vol. 82, page number 395 - 411, May 2018. 636

[66] Mohamed Abomhara, Geir M. Køien. "Cyber Security and the Internet of Things: Vulnerabilities, 637 Threats, Intruders and Attacks" Journal of Cyber Security 2015, Published in 6 2015, Norway. 638

[67] Chan Hyeok Lee ; Ki-Hyung Kim. "Implementation of IoT System using BlockChain with 639 Authentication and Data Protection", published in the proceeding of the 2018 International Conference 640 on Information Networking (ICOIN), pp. 936 – 940, 10-12 Jan. 2018, Chiang Mai, Thailand

[68] S. Karthikeyan, R. Patan, and B. Balamurugan, *Recent Trends in Communication, Computing, and Electronics*, vol. 524. Springer Singapore, 2019

[69] T. Yu, X. Wang, and A. Shami, "A novel fog computing enabled temporal data reduction scheme in iot systems," *2017 IEEE Glob. Commun. Conf. GLOBECOM 2017 - Proc.*, vol. 2018–January, pp. 1–5, 2018.

[70] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[71] https://medium.com/@himanshugupta0007/cloud-computing-working-model-2ab1b6887b4c

[72] https://azure.microsoft.com/en-gb/overview/what-are-private-public-hybrid-clouds/

[73] http://cloudcomputingtechnologybasics.blogspot.com/2011/08/delivery-models-of-

cloud-computing.html

[74] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "A secure and verifiable outsourced access control scheme in fog-cloud computing," *Sensors (Switzerland)*, vol. 17, no. 7, 2017.

[75] https://www.cbinsights.com/research/what-is-ethereum/

Appendix A

Scyther Script for protocol verification

```
/*
 * End to End Secure Communication
 */
// The protocol description
usertype id,pass,verifiableidentity,Message,Data,Filteredata,Blockid;  const Fresh: Function;
protocol E2E(I,R,S,B,F,C)
{
        role I // IoT Device

        {
                fresh i: id;
                fresh p:pass;
                fresh ni:Nonce;
                fresh ti:Timestamp;
                var vi: verifiableidentity;
                var nr:Nonce;
                var tr:Timestamp;
                hashfunction H;
                fresh m: Message;
                fresh d : Data;
                //Authentication phase
                send_1(I,R, (i,p,ni,ti,{H(i,p)}sk(I)));
                recv_2(R,I,(vi,nr,tr,{H(vi)}sk(R)));
                //IoT Service
                send_3(I,S,(i,ni,ti,{H(vi)}sk(I)));
                // Blockchain
                send_4(I,B,(vi));
                //Service message access request
                send_5(I,F,(m,{H(m)}sk(I)));
                //Data send
                send_6(I,F,(d,{H(d)}sk(I)));
                //Security Properties claimed by IoT Device
                claim_i1(I,Secret,i);
                claim_i2(I,Secret,p);
                claim_i3(I,Alive);
                claim_i4(I,Weakagree);
                claim_i5(I,Niagree);
                claim_i6(I,Nisynch);
        }

        role R   // Registration authority

        {
                var i: id;
                var p:pass;
                var ni:Nonce;
                var ti:Timestamp;
                fresh vi: verifiableidentity;
                fresh nr:Nonce;
                fresh tr:Timestamp;
                hashfunction H;
                recv_1(I,R, (i,p,ni,ti,{H(i,p)}sk(I)));
                send_2(R,I,(vi,nr,tr,{H(vi)}sk(R)));
                claim_r2(R,Alive);
                claim_r3(R,Weakagree);
                claim_r4(R,Niagree);
                claim_r5(R,Nisynch);
        }

         role S   //  Rest Service

        {
                var i:id;
                var ni:Nonce;
                var ti: Timestamp;
                hashfunction H;
                var vi:verifiableidentity;
                recv_3(I,S,(i,ni,ti,{H(vi)}sk(I)));
                claim_s1(S,Alive);
                claim_s2(S,Weakagree);
                claim_s3(S,Niagree);
                claim_s4(S,Nisynch);
        }

        role B  // Blockchain

        {
                hashfunction H;
                var fd: Filteredata;
                var vi:verifiableidentity;
                recv_4(I,B,(vi));
```

```
          recv_7(F,B,{H(fd)}sk(F));
}

    role F  // Fog

    {

          fresh fd: Filteredata;
          fresh bid: Blockid;
          fresh n: Nonce;
          fresh t: Timestamp;
          hashfunction  H;
          var m: Message;
          var d : Data;
          recv_5(I,F,(m,{H(m)}sk(I)));
          recv_6(I,F,(d,{H(d)}sk(I)));
          send_7(F,B,{H(fd)}sk(F));
          send_8(F,C,{bid,n,t,fd}sk(F));
          claim_f1(F,Alive);
          claim_f2(F,Weakagree);
          claim_f3(F,Niagree);
           claim_f4(F,Nisynch);


    }

    role C  // cloud

    {
           var fd:Filteredata;
           var bid: Blockid;
            var n: Nonce;
```

```
         var t: Timestamp;
        recv_8(F,C,{bid,n,t,fd}sk(F));
}
}
```