Title: Defending IoT against escalating cyber threats like botnet attacks, data privacy issues and inadequate patch management capabilities

MSc Research Project
MSc in Cybersecurity

Nagraj Merala
Student ID: x20180985

School of Computing
National College of Ireland

Supervisor: Rohit Verma

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	……NAGRAJ MERALA………………………………………………………………………………
Student ID:	……x20180985…………………………………………………………………………………..……
Programme:	……MSc. Cybersecurity…………………………… **Year:** …2021-22…..
Module:	……MSc Research Project…………………………………………………………….………
Supervisor:	……Rohit Verma…………………………………………………………………………….………
Submission Due Date:	……19th September 2022………………………………………………………….………
Project Title:	Defending IoT against escalating cyber threats like botnet attacks, data privacy issues and inadequate patch management capabilities
Word Count:	……**6127**………………………… **Page Count**………**21**…………………………….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……NAGRAJ MERALA……………………………………………………………………

Date: ……19th September 2022……………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Title: Defending IoT against escalating cyber threats like botnet attacks, data privacy issues and inadequate patch management capabilities

Nagraj Merala
Student ID: x20180985

Table of Content

Abstract

Internet of Things (IoT) usage is rising along with wireless technology advancements and causing a swift growth in adaptation of IoT. IoT is a rapidly growing field with many positive innovations that are being adopted by a variety of industries. However, because of the nature of the devices, and in some cases vendor security negligence result in lack of timely updates along with exposure to Cyberthreats due to the mode of connectivity using traditional networks which are usually not secure, adequate or scalable. IoT devices and networks are at an increased risk of Cyberattacks like Botnets, data privacy concerns, and exploitation of lack of updates, always carrying security risks. Unpatched devices in an unsecure environment are an easy target for these hostile actors, who are always searching for vulnerabilities. The research that follows has been developed using Software Defined Networking (SDN), Blockchain (BC) technologies and Intrusion Detection Systems (IDS) based solutions to address these issues. Throughout the course of this research, each of these solutions will be thoroughly studied and examined. Each of these solutions has a distinct feature set that has the potential to improve IoT security.

Keywords: IoT (Internet of Things), patch management, Cyber-attacks, Botnet, DoS, DDoS, SDN (Software Defined Networking), Blockchain (BC), Data privacy, IDS (Intrusion Detection System).

1 Introduction

Internet of Things (IoT) can be described as anything that is connected to the internet, connects and exchanges data. If we look around, we can probably find a device that can connect to the internet, it might be our phone, a laptop or a TV. IoT is the general term used to describe the collection of all those gadgets, which can include laptops, smart TVs, and even refrigerators. This has reached millions of users worldwide and growing further making life amazing with its utility and benefits. The application of IoT is far greater today, it has reached beyond the smart devices used at homes, IoT is being adapted and used extensively in many sectors including Healthcare and Industries as well. In the industrial sectors, IoT has gained a lot of traction and is now widely used to increase productivity, dependability, and monitoring, where it is becoming a driving force in the industry 4.0 (Boyes et al., 2018) which is an industrial revolution. In Healthcare particularly (Farahani et al., 2020), IoT has been incorporated in several medical devices and is being used to monitor critical healthcare and life saving equipment's and proving quite useful. IoT is being used for development of autonomous cars (Baliyan et al., 2022) and are projected to be in a widescale operations soon, because of all this, we could say that we are now living in a future that was thought to be decades away just a few decades ago. IoT could be thought of as a fresh revolution, it is the convergence of physical and informational systems. The IoT's potential appears to be limitless, for example, our refrigerators might remind us of the groceries we still need to buy (Rajeswari et al., 2022), doctors will be able to check on patients from anywhere in the globe (Farahani et al., 2020), and cities are expected to have the ability to monitor anything from buses to garbage cans.

Given the exponential expansion in IoT devices as a result of the swift development of internet and wireless technologies, there are concerns about the potential of the IoT as well as the security implications for society, as there are with any technology. According to a recent prediction by Ericsson (Collela, n.d.), there will be 18 billion IoT devices estimated to be online by the end of 2022, an increase of over 100% from 2020, and this number will keep growing everyday due to the several advantages of IoT.

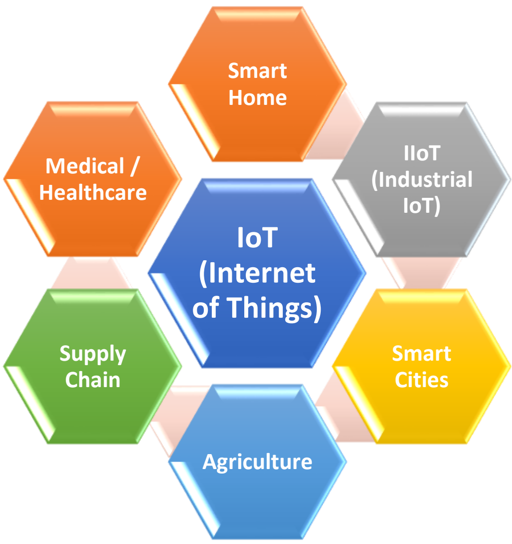


Figure 1: Examples of applications of IoT (Internet of Things).

IoT has a variety of applications, as shown in Fig. 1, and is swiftly gaining popularity in other industries due to its advantages, simplicity, and usability. The healthcare sector (Farahani et al., 2020) is one of the areas that is benefiting from the Internet of Things (IoT). IoT is cutting expenses and removing geographical boundaries by enabling video doctor consultations, reducing paperwork, and assisting in the early diagnosis of chronic diseases through the use of big data analytics created by medical sensors and alarm-based medical IoT devices.

The industrial sector, which is projected to be essential to Industry 4.0 (Boyes et al., 2018), is already experiencing similar benefits.

IoT security concerns: The increase of botnet attacks, data privacy concerns, use of weak passwords, a lack of secure update mechanisms, a lack of secure storage, and inadequate testing are just a few of the security challenges brought on by IoT. Although the Internet of Things offers the medical sector numerous benefits, we must exercise caution because these incredible new biological discoveries may also pose problems. We also need to consider the fact that computing devices have the ability to run code, which can then be misused to run harmful programmes. Because they are regularly networked, modern medical devices are vulnerable to hacking. Owing to the speed at which IOT is expanding and how quickly they are coming up with new ideas, Businesses typically can forget or ignore to incorporate data security and privacy into new products, cost is a big factor as well. Release of a technology into the world that you are unable to fully safeguard and that has a long shelf life is exceedingly dangerous. Our digital selves have evolved into extensions of our real-life selves. We communicate with our friends on social media. These days, we can use our phones to control our homes. If you keep your front door unlocked at home, it's unlikely that someone will come to check on you, but in the online world, many people are constantly checking every door and opportunity. Using a botnet, an attacker could look for vulnerabilities in them, then infect cameras and DVRs if they were discovered to be freely accessible. Since end users frequently lack the necessary skills, many devices come pre-configured with default usernames and passwords, which can lead to hundreds of thousands or even millions of people having their accounts hijacked. We haven't even touched on weak passwords yet. This leads to other flaws that attackers may exploit, such as a lack of secure update procedures and device management. One instance of how botnets can wreak havoc by utilising vulnerable IoT devices is the Mirai botnet attack, where hackers used a malware to target IoT devices and smart home devices to create a zombie network managed by them to target attacks towards other organisations and networks by creating a massive DDoS kind of attacks (Borys et al., 2022).

IoT is crucial for many businesses today and has huge potential to help people live and work more intelligently. IoT can flourish more and realise its full potential sooner than anticipated if security is improved. To prevent end users from being harmed and to protect security of their data, threats concerning IoT must be addressed.

The following Thesis report includes sections like Research Question, Literature review, Research methodology, Design specification, Implementation, Evaluation and Conclusion. I will articulate the detailed study and analysis conducted throughout this academic research report.

2 Research Question, Motivation and Objectives

Research Question:
What are the possibilities of reducing the risk of improper patch management, botnet attacks and data privacy issues in IoT by using Blockchain solutions, IDS (Intrusion Detection System), SDN (Software Defined Networking) solutions and how much risk can be reduced by these solutions? Is it possible to patch IoT devices in a timely, proactive and secure manner using Blockchain solutions, IDS and SDN solutions?

2.1 Motivation and justification:

The enormous growth of IoT devices and their positive effects on daily life served as the motivation and driving force behind this research project. Our reliance on IoT will only grow as more devices connect to the Internet. A lot of useful benefits are provided by utilising IoT across a variety of industries, including production, dependability, and monitoring. However, it also poses security risks. The fact that many IoT devices are used by non-IT (information technology) users who are not familiar with IT security threats and cyber security best practises is one of the disadvantages of the IoT. This could be as simple as adjusting the IoT device's default settings or more complicated privacy and security settings. Regular software patches and firmware updates are crucial for IoT devices to stay current. Unpatched devices in an environment devoid of security are easy targets for attackers, who are continuously looking for weak areas. The possibility of Zero Day vulnerabilities is the next risk, which necessitates quick manufacturer action but is found to be lacking in a range of IoT devices for a variety of reasons. Given the IoT's rise and its future importance, notably in Industry 4.0 (Boyes et al., 2018), Regular danger assessments and staying on top of emerging detection and prevention techniques are essential. IOT devices are fast expanding and evolving in a variety of societal areas, including the healthcare industry, aside from home appliances (Djenna and Eddine Saidouni, 2018) and the industrial sector (IIoT) (Boyes et al., 2018). The security concerns related to IoT must be solved in order to make sure that the progress of IoT technologies and their use is not hampered. There is a lot of space for improvement in this area, according to numerous studies on the subject of patch management on IoT devices. The decentralised nature of IoT device connectivity and the customary cheap cost of goods pose some of the biggest issues, as they do not encourage manufacturers to prioritise security.

2.2 Research Objectives:

Objective of this research is to defend and secure IoT devices and networks, I have discovered that the issues described in the research question can be innovatively solved using SDN (Software Defined Networking), IDS (Intrusion Detection System), and Blockchain-based solutions. It also appears feasible to create a suitable solution to reduce the threats and vulnerabilities found.

SDN: The openness and programmability of the network is the primary objective of SDN. An organization can create or install an application to accomplish its goals if it needs a specific kind of network activity. To better comprehend SDN, it may be helpful to use an already well-known analogy—in this case, the operating system of a typical desktop computer. A desktop operating system can be divided into three fundamental layers at a high level. First, there is the operating system itself, which serves as a middleman, controlling how applications can access the hardware below. The OS also includes basic services to help with this process. The operating system is also in charge of system management. The ability to create, add, or move applications makes a system flexible, allowing it to be tailored to your unique needs. Hardware on the lower level, such as CPUs, storage, memory, and network interfaces, can also be described as being to the south of the OS above the operating system or on the north side. Whether it be for engineering or game design. The middle layer for SDN is the network operating system, which is also known as an SDN controller. The network operating system will typically have core services to help it in its job of interacting with network nodes and for providing a programmable interface to the network applications on the south side instead of hardware. The SDN model will look quite similar to the operating system model just discussed. Sending packets out of a single port or out of numerous ports are examples of actions, as well as merely deleting the packet and changing the packet headers. Hardware switches are frequently anticipated to support superior performance, whereas software switches like the one used in SDN provide more adaptability for novel behaviors. Instructions for packet handling, notifications of packet arrivals on network nodes, alarms of connection status changes, and statistics data like flow counters are a few examples of the data that must be sent to network forwarding devices via the southbound interface of the SDN controller. Everything happens over the southbound interface. The SDN protocol on the southbound interface with the greatest discussion is open flow for packet handling instructions.

IDS – Snort: Snort, a well-known free and open-source IDS (intrusion detection system) / IPS (intrusion prevention system) system, can be utilised to do a traffic or protocol analysis, content matching, and to identify and prevent various attacks based on specified rules. In order to stay up with the most recent attacks and incursions, snort has been actively developed with the help of thousands of users and contributors. It has the capability to log traffic at the most fundamental level, or to alert administrators or security analysts to specific traffic and vulnerability alerts. One of the best features of snort rules is the capability to perform signature matching, which enables it to identify a signature from the content of a packet and use that signature to detect intrusions or attacks.

Blockchain: Blockchain has been proposed as a solution for some of the security issues observed and provide an end-to-end security and accountability for transactions such as Patch downloads and data transfers. We will discuss in detail about blockchain, its working methodology and possible solutions applicable. A blockchain is, as its name suggests, a chain of information-containing blocks. Each block includes some data as well as its own hash and the hash of the block before it. Depending on the type of blockchain, different types of data are kept inside blocks. For instance, the sender, receiver, and total quantity of bitcoin for a transaction are all stored in the Bitcoin blockchain. A block has a hash as well. A hash is comparable to a fingerprint. Similar to a fingerprint, it uniquely identifies a block and all of its contents and is constantly different. A block's hash is determined once it is produced. The hash will alter if anything inside the block is modified. Blockchains safeguard themselves in another way as well, and that is by being distributed.

Smart contracts: Blockchains are likewise undergoing constant change. The development of smart contracts is one of the more recent innovations. These contracts, which are straightforward scripts stored on the blockchain, can be used to automatically trade money in accordance with specific criteria. Smart contracts are essentially the same as contracts in the real world—you know, the paper agreements where you sign—except that they're digital. Being digital means that smart contracts are stored inside a blockchain, giving them all of the advantages of the blockchain and making them publicly accessible. Everyone who wants to can view the contract, which also implies that everyone may interact with it, run it, and check its terms, and there is agreement on how the smart contract will turn out. Therefore, if I build a smart contract that computes one plus one, then everyone on the network will concur that one plus one equals two. If someone then says, "Yeah, but in my case, my computer said one plus one equals four," then the others will respond, "Yeah, but we verified ourselves so one plus one is still two." The smart contract can give and receive currencies and communicate with other smart contracts, but what more can it do? They are stored on the blockchain and are immutable exactly like a blockchain. In other words, once you've added a smart contract to it, it can't be changed any longer. Because it's distributed and there is consensus regarding it, no one can force your contract and claim that you agreed to different terms or that the contract's outcome is now different. As a result, no one can manipulate the system because everyone knows what the contract is and what the outcome is.

3 Related Work

I have researched a lot about the Internet of Things and read about its possible uses, security concerns, mitigation options and future applications. I have thought about its benefits and important limitations, as well as some potential solutions to some of its security concerns. IoT provides a lot of benefits, but due to its extensive connectivity, it is also open to cyberattacks. Some of the most important security concerns with IoT are shown in Figure 2 below.

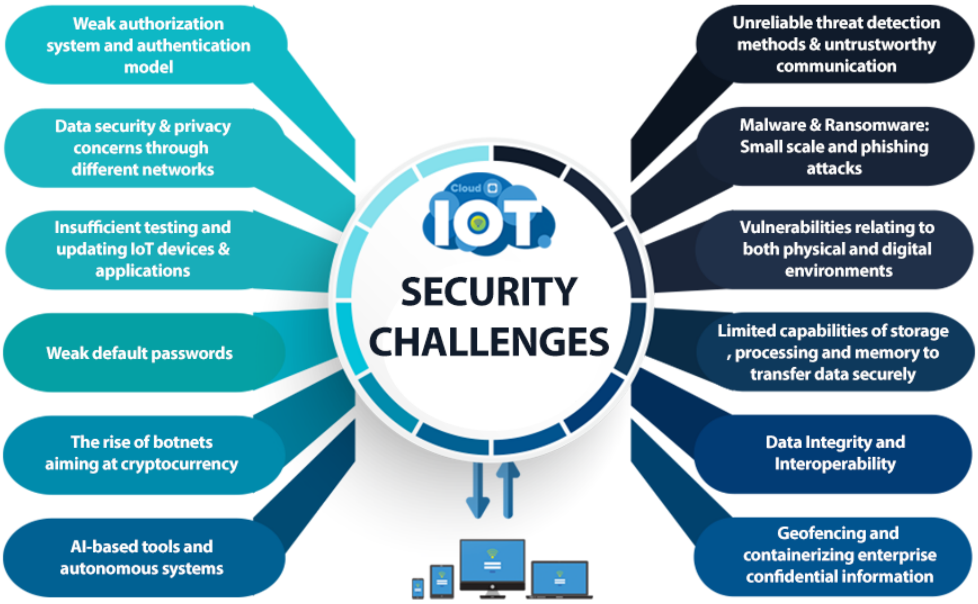


Figure 2: Examples of security challenges in IoT (MediaDSCI, n.d.).

3.1 Subsection 1 – Challenges in IoT – Related research:

The Internet of Things (IoT) is a system with an ever-growing complexity; it is the next breakthrough that will give everything we use a human face, as well as the next stage of automation. IoT is bringing more and more objects online on a daily basis, which will probably cause it to become a multi-trillion-dollar industry soon. Check the number of recent conferences, papers, and research about the internet of things (IoT) to get a sense of how popular it is. However, as the IoT industry is developing further, there will be significant challenges, chief among them the urgent need for a secure IoT model to carry out typical tasks like sensing, processing, storing, and communicating. This is because the IoT market has grown quickly, leading to an increase in the number and wide range of IoT solutions. By no means will it be simple to develop such model; there are numerous obstacles and difficulties that must be overcome before a true safe IoT model can be developed. One of the security issues with IoT is that because of their current computing limitations, the devices cannot use tools like host-based firewalls. Considering that IoT involves many devices that communicate with one another, there is a large attack surface, and given that IoT is growing into sectors like healthcare, finance, and transportation, security is becoming increasingly crucial. Appropriate standardization has not been developed.

Data Privacy: In this paper the authors have highlighted the challenges and concerns related to privacy in IoT, they have proposed a solution accordingly (Solangi et al., 2018). This paper (Boeckl et al., 2019) has been published with an aim to help organisations and federal agencies to better understand the cybersecurity threat risks and Related to security challenges, considerations for managing risks related to Cybersecurity and Privacy in IoT. The authors have observed that the organisations are usually not aware of the scale of IoT deployment in their infrastructure and discuss extensively on the related risks and need to address these (Boeckl et al., 2019).

Inadequate patch management: The authors have conducted a detailed research and survey on various security challenges and aspects covering IoT, including inadequate patching capabilities, IoT vulnerabilities, encryption concerns, access control and authentication issues. The authors have stressed on the fact that these concerns needs to be addressed appropriately with future work scopes (Neshenko et al., 2019).

Botnet: This paper talks about the impacts of Botnet attacks on IoT Network and potential escalation of threat emerging from compromise of IoT devices in a large scale. The authors have studied two Botnets (Mirai and Hajime Botnets) in particular, the authors have stressed on the need for patching the devices adequately and to take necessary actions for security (Herwig et al., 2019). Another paper (Kolias et al., 2017) has conducted a detailed study on the impact of Mirai botnet and DDoS attacks which affected IoT and should serve as a wakeup call for taking necessary precautions and protecting the IoT assets.

3.2 Subsection 2 – Solutions – related research:

Over the past few months, I have conducted extensive study to determine whether SDN, IDS, and Blockchain (BC) technologies combined can secure and defend IoT devices.

SDN solutions related research: I have researched and reviewed several papers related to IoT and SDN, several researches have contributed to this area and have provided their observations and sometimes solutions on how SDN has been effective at supporting and enhancing IoT Networks, further scope and possibilities along with few short comings which can be mitigated in future. Overall SDN seems to be able to provide the required flexibility and scalability along with security aspects related to IoT. The summary of few of the reviewed papers are as following:

SDN based architecture with Security enhancement for IoT: In this paper the authors have discussed about the opportunities being introduced by SDN for IoT along with scalable option and have conducted their research to establish a secured architecture for IoT (Flauzac et al., 2015).

SDN-based management of heterogeneous home networks: The authors have demonstrated how the Home networks can benefit from the SDN architecture, where differentiating the control plane from the data plane is a crucial component of SDN. This allows other network devices to now function only as data forwarders and do not require any intelligence thanks to the introduction of an SDN controller administering the control plane of the network (Soetens et al., 2015).

Combining Software-Defined Networking with Internet of Things: This paper talks about the traditional network connectivity for IoT, its limitations, advantages and disadvantages, have demonstrated and conclude how it is difficult to manage IoT using traditional networking. The authors have proposed a SDN based solution to make IoT networks flexible and scalable along with enhancing its security with help of enhanced monitoring and security analysis possibilities (Yassein et al., 2017)

Benefits of SDN in IoT: In this paper the authors have conducted a thorough research and presented their inputs on the possible benefits of SDN in IoT to overcome some of the security challenges, the paper also talks about the limitations of SDN and future scope (Farris et al., 2019). This paper talks about how IoT has been evolving rapidly and the compound increase in data traffic related to IoT, the authors have researched and discussed how SDN can complement the growing demands of IoT (Rafique et al., 2020)

IDS related research: Detection of Botnet attacks using IDS: The authors talks about the research conducted on IDS related tools to detect Botnet attacks on IoT, this paper was able to successfully deploy IDS rules to detect Botnet attacks with a Novel approach hence proving the utility of IDS to provide a security aspect to IoT. (Al-Kasassbeh et al., 2020).

In this paper the authors have discussed about the potential cyberattacks on IoT and have proposed a secured and efficient IDS solution to defend IoT, overall IDS seems to be providing an adequate security benefit in detecting alerts of potential vulnerability and attacks in IoT (Javaid and Bandekar, 2017).

Blockchain related research: A Distributed Secure Blockchain Based SDN-IoT Architecture: The authors have introduced SDN and Blockchain in IoT in a secure manner and argue that SDN setup is reliable overall while there could be few concerns which needs to be addressed in future (Rahman et al., 2019)

Benefits of Blockchain in IoT: In this paper the authors have described the benefits of using Blockchain in IoT and demonstrated with certain examples by proposing an optimised Blockchain and light weight setup excluding mining process to speed up, conducted few tests to demonstrate the robustness of the proposed setup and articulated the scope for future work (Dorri et al., 2017)

Blockchains and Smart Contracts in IoT: This paper tries to examine blockchains utility in IoT to see if it can be a good choice overall, hypothesis is that this Blockchain and IoT combination can be a good solution for several use cases. Authors have seen successful to an extent to demonstrate the power of their proposed solution, where Blockchain provides enough resilience to the IoT setup and they encourage its future use (Christidis and Devetsikiotis, 2016)

Can Blockchain Strengthen the IoT? – The authors have articulated that IoT security can be improved by utilising identity and access management systems built on blockchain technology. They have provided the identified challenges and potential solutions along with appropriate solutions (Kshetri, 2017)

File sharing & Data management related: Authors have proposed a blockchain based solution with an aim of distributed data management for IoT, this is still work in progress as per authors and have faced few overheads while the initial results and performance are promising.(Shafagh et al., 2017)

Patching – Blockchain ledger usage: The authors have researched and presented their view of the benefits of Blockchain in securing Patching of devices, using Blockchain distributed ledger for security of complex software processes (Mylrea and Gourisetti, 2018)

IPFS (InterPlanetary File System): This paper discusses the proposed solution of integrating IPFS Technology and solution with Blockchain to implement a secured platform for data sharing (Jianjun et al., 2020).

3.3 Timeline of papers researched

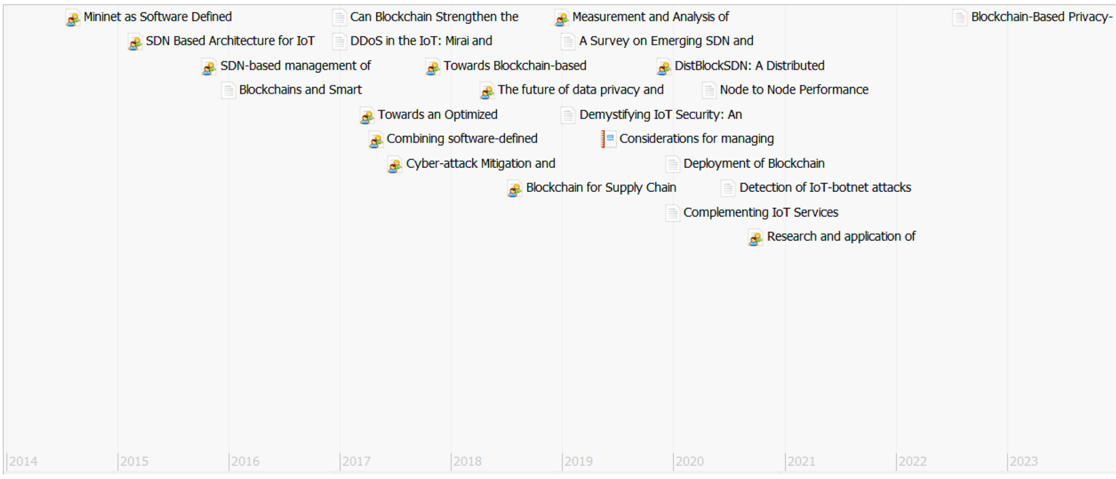


Figure 3: Timeline based report of papers used in this research project.

4 Research Methodology & Design specification

There is a huge potential of combining SDN, Blockchain and IDS solutions to secure IoT devices and Network. SDN & IDS combined provides flexibility and a secured layer of Protection, one of the other areas of focus was blockchain, which apart from being a tradable currency or digital asset, actually serves as a platform or network for the development of decentralised apps.

In my research, my objective was to utilise SDN & IDS from Network Layer security perspective and utilise Blockchain technology to secure File transfer, including relevant transactions.

SDN (Software Defined Networking): Based on the research carried out, it is evident that SDN functionality is a good addition to any IoT based Network for introducing flexibility, scalability and security. I have leveraged several tools to achieve this objective, notable Mininet and RYU Controller to achieve the SDN functionality simulation, will discuss further on these tools and their functionalities.

Mininet: Mininet can be described as an Emulator which can be used to deploy massive networks including a basic single computer or virtual machine. Mininet was developed to facilitate research in OpenFlow and Software Defined Networking (SDN). On a basic PC, the Mininet emulator enables interactive execution of unmodified code on virtual hardware. Mininet is an open source tool which is freely available and supports in emulating an SDN prototype Network setup (Kaur et al., 2014). I have used Mininet tool combined with RYU controller to simulate SDN based setup in my research project.

RYU: The Ryu Controller is an open-source, software-defined networking (SDN) controller created to improve network agility by simplifying the management and adaptation of traffic management (Islam et al., 2020). I have combined RYU controller along with Mininet, where, RYU forms the control plane and Mininet forms the Data plane of the SDN Prototype network layer for our research.

IDS (Intrusion Detection System): IDS plays a critical role in this research project related setup, where IDS is being deployed to monitor the network events, analyze traffic, detect security incidents and generate relevant alerts. We have used Snort based IDS. Snort is a powerful open-source IDS which helps in monitoring and alerting based on potentially malicious activities. Snort employs a rule-based language that integrates protocol, and signature inspection techniques.

The following Network Architecture Diagram depicts the Integration of SDN and IDS components in forming a secure layer in Defending IoT based network and devices.

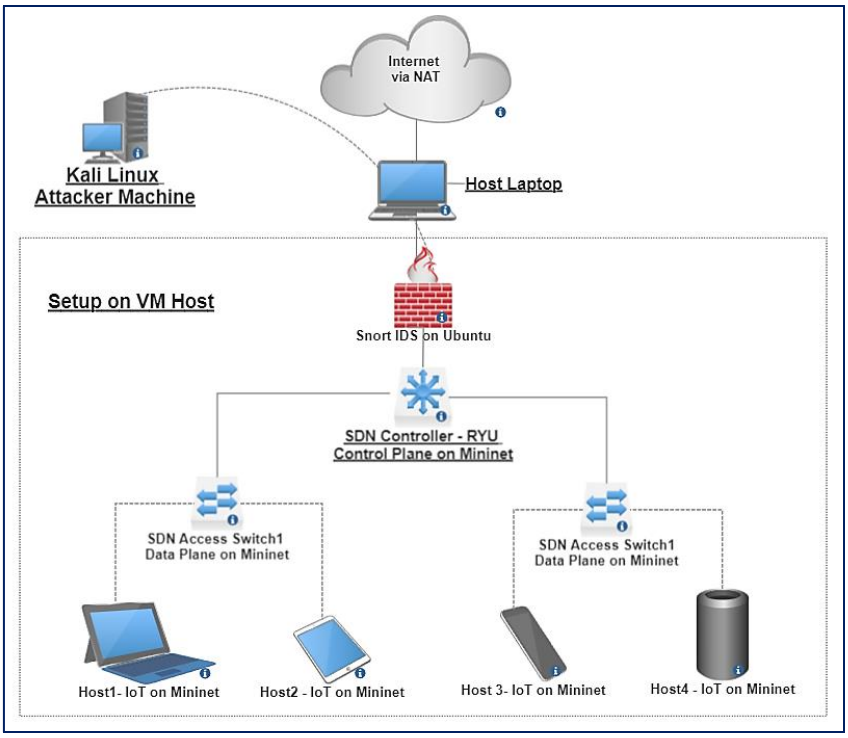


Figure 4: Network architecture diagram – SDN and IDS based setup for IoT.

Blockchain: Blockchain based solution have a huge potential in securing IoT network and devices, related transactions and file transfers. This security feature gets enhanced when we combine it with IDS & SDN Layer as proposed in the Novel approach of my research project. We have used several Blockchain based platforms and tools to perform relevant actions and tests in order to try and achieve the objectives. The Following Network Diagram depicts the Blockchain based solution wherein several Blockchain platforms and tools are integrated to try and achieve the objectives of securing Patch updates and file transfers in an IoT environment.

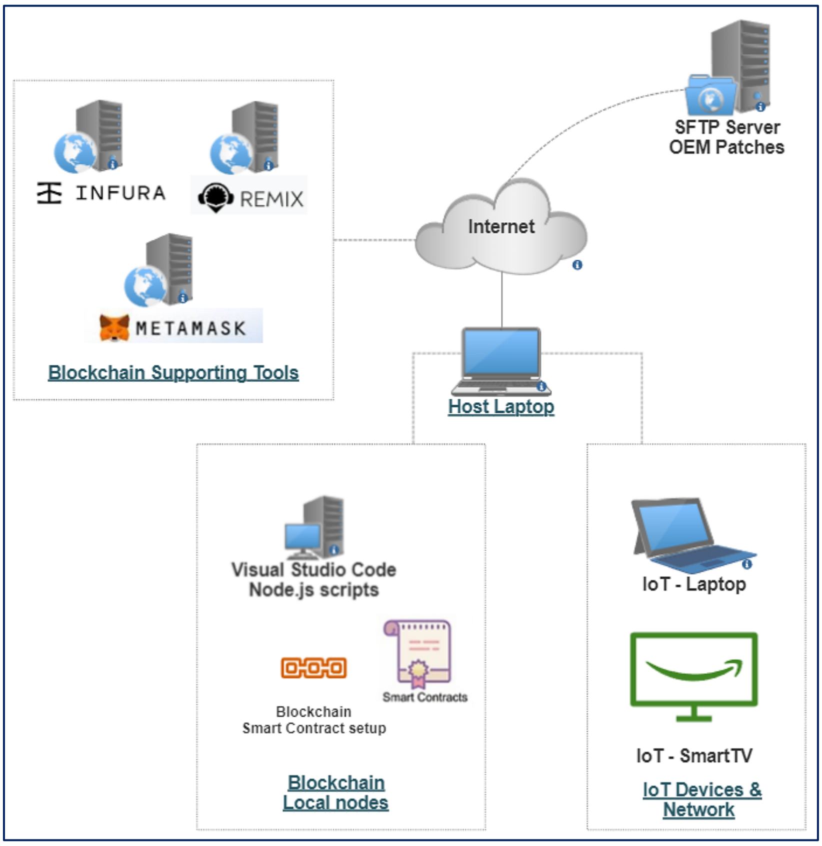


Figure 5: Architecture diagram – Blockchain solution for secured file transfer and patch download in IoT.

5 Implementation

I have created a setup of SDN, IDS and Blockchain to achieve the objectives of my research project. Below are few samples of implementation steps carried out to configure the Network setup and installation of relevant tools to carry out the objectives of this research project. Detailed implementation steps and screenshots are captured in configuration manual being submitted separately.

System Specifications Table:

Hardware - Specifications	
RAM – Host Machine	16 GB
Processor	AMD RYZEN 9 5900HX
Graphics card - GPU	Nvidia GeForce RTX 3050 – 4GB
Storage	1 TB SSD
Software - Specifications	
OS & Critical Software's	Windows 11, Kali Linux, Virtual Box & Ubuntu LTS 22.04

SDN: I have utilised Mininet and RYU Controller for configuration for simulation of SDN Prototype network.

- RYU Installation and activation.

```
Nagraj@Nagraj:~$ pip install ryu
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: ryu in ./.local/lib/python3.10/site-packages (4.
34)
Requirement already satisfied: eventlet!=0.18.3,!=0.20.1,!=0.21.0,!=0.23.0,>=0.
18.2 in ./.local/lib/python3.10/site-packages (from ryu) (0.33.1)
Requirement already satisfied: oslo.config>=2.5.0 in ./.local/lib/python3.10/si
te-packages (from ryu) (9.0.0)
Requirement already satisfied: routes in ./.local/lib/python3.10/site-packages
(from ryu) (2.5.1)
Requirement already satisfied: six>=1.4.0 in /usr/lib/python3/dist-packages (fr
om ryu) (1.16.0)
```

```
Nagraj@Nagraj:~/ryu$ PYTHONPATH=. ./bin/ryu-manager ryu/app/simple_switch_13.py
loading app ryu/app/simple_switch_13.py
loading app ryu.controller.ofp_handler
instantiating app ryu/app/simple_switch_13.py of SimpleSwitch13
instantiating app ryu.controller.ofp_handler of OFPHandler
```

- Mininet Installation and activation:

```
Nagraj@Nagraj:~$ sudo apt-get install mininet
[sudo] password for Nagraj:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mininet is already the newest version (2.3.0-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 3 not up
Nagraj@Nagraj:~$
```

```
Nagraj@Nagraj:~$ sudo mn --topo single,3 --mac --switch ovsk --controller remot
e
[sudo] password for Nagraj:
*** Creating network
*** Adding controller
Connecting to remote controller at 127.0.0.1:6653
*** Adding hosts:
h1 h2 h3
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1) (h3, s1)
*** Configuring hosts
h1 h2 h3
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet> net
h1 h1-eth0:s1-eth1
h2 h2-eth0:s1-eth2
h3 h3-eth0:s1-eth3
s1 lo:  s1-eth1:h1-eth0 s1-eth2:h2-eth0 s1-eth3:h3-eth0
c0
mininet>
```

IDS: Snort has been used to configure IDS functionality for relevant testing.

Snort IDS Installation and sample rule creation:

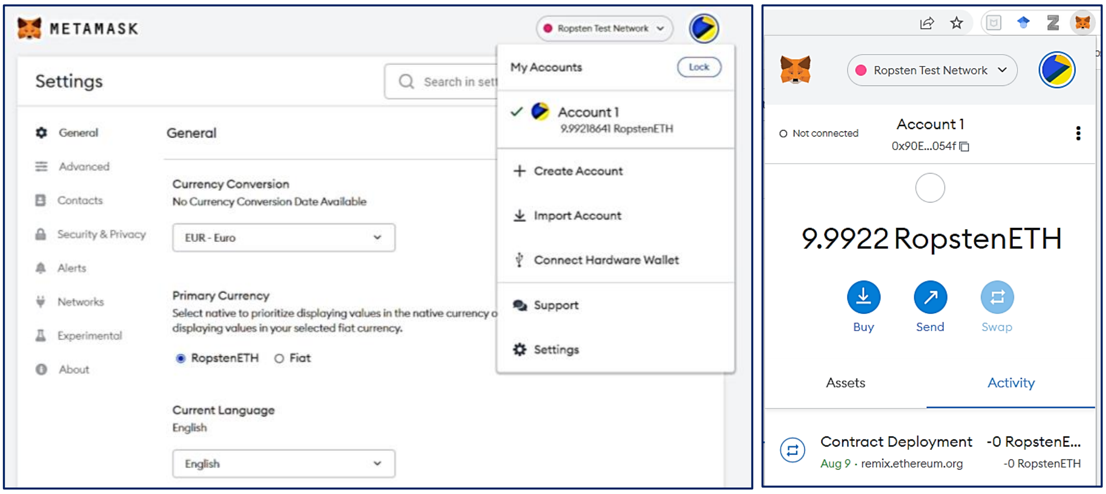
```
Nagraj@Nagraj:~$ sudo wget https://www.snort.org/downloads/snort/snort-2.9.20.t
ar.gz
--2022-08-14 20:15:48--  https://www.snort.org/downloads/snort/snort-2.9.20.tar
.gz
Resolving www.snort.org (www.snort.org)... 2606:4700::6812:8b09, 2606:4700::681
2:8a09, 104.18.139.9, ...
Connecting to www.snort.org (www.snort.org)|2606:4700::6812:8b09|:443... connec
ted.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/file
s/000/025/687/original/snort-2.9.20.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-A
mz-Credential=AKIAU7AK5ITMJQBJPARJ%2F20220814%2Fus-east-1%2Fs3%2Faws4_request&X
-Amz-Date=20220814T191549Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Si
gnature=8e01a2c076cdbadd57f623a1faab9233437f4e62f0f53982b93e7ed6ce0e50ef [follo
wing]
--2022-08-14 20:15:49--  https://snort-org-site.s3.amazonaws.com/production/rel
ease_files/files/000/025/687/original/snort-2.9.20.tar.gz?X-Amz-Algorithm=AWS4-
HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMJQBJPARJ%2F20220814%2Fus-east-1%2Fs3%2
Faws4_request&X-Amz-Date=20220814T191549Z&X-Amz-Expires=3600&X-Amz-SignedHeader
s=host&X-Amz-Signature=8e01a2c076cdbadd57f623a1faab9233437f4e62f0f53982b93e7ed6
ce0e50ef
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)...
54.231.171.105
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)
|54.231.171.105|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7009894 (6.7M) [binary/octet-stream]
Saving to: ‘snort-2.9.20.tar.gz.1’
```

```
  GNU nano 6.2                /etc/snort/rules/local.rules

# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert icmp any any -> 192.168.0.221 any (msg:"NMAP ping sweep Scan";dsize:0;si>
alert tcp any any -> $HOME_NET 22 (msg:"NMAP TCP Scan"; sid:10000005; rev:2;)
alert tcp any any -> 192.168.0.221 22 (msg:"NMAP XMAS Tree Scan";flags:FPU; si>
alert tcp any any -> 192.168.0.221 22 (msg:"NMAP FIN Scan";flags:F; sid:100000>
```

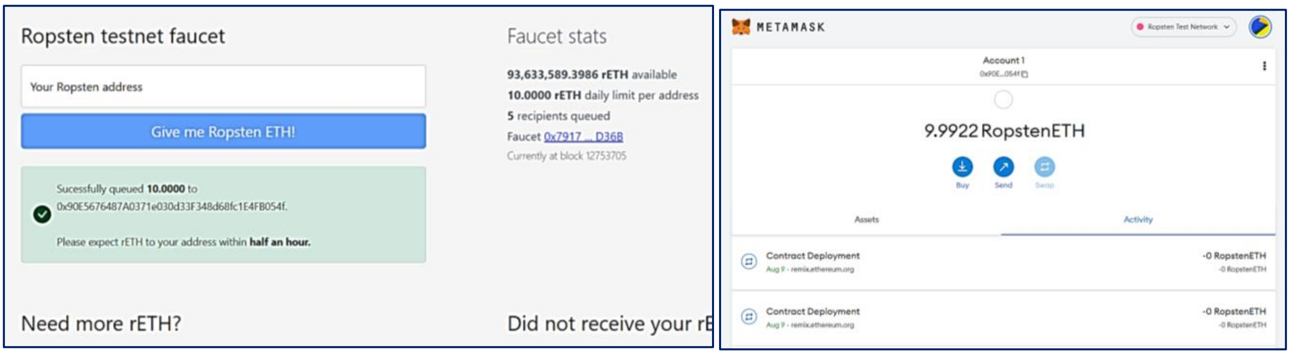
Blockchain: We will be carrying out various steps to achieve successful implementation of a Smart Contract from the Host or IoT node, we are using Blockchain network and utilising test Tokens form Ropsten Test network via Metamask, below are the details of the steps being carried out:

Smart Contract Deployment related steps:

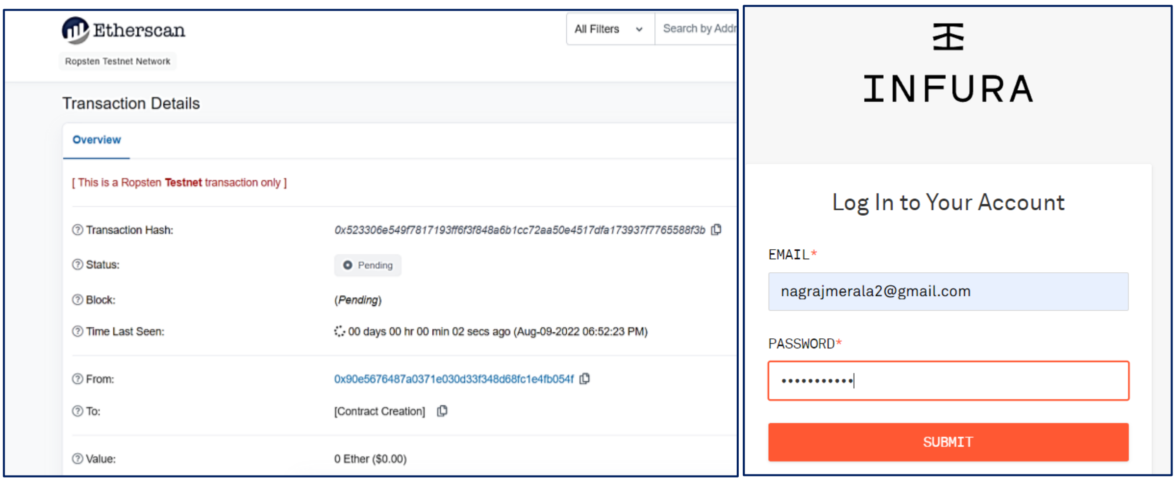
Step 1: Creation of Metamask account and selecting Ropsten Test network for simulation



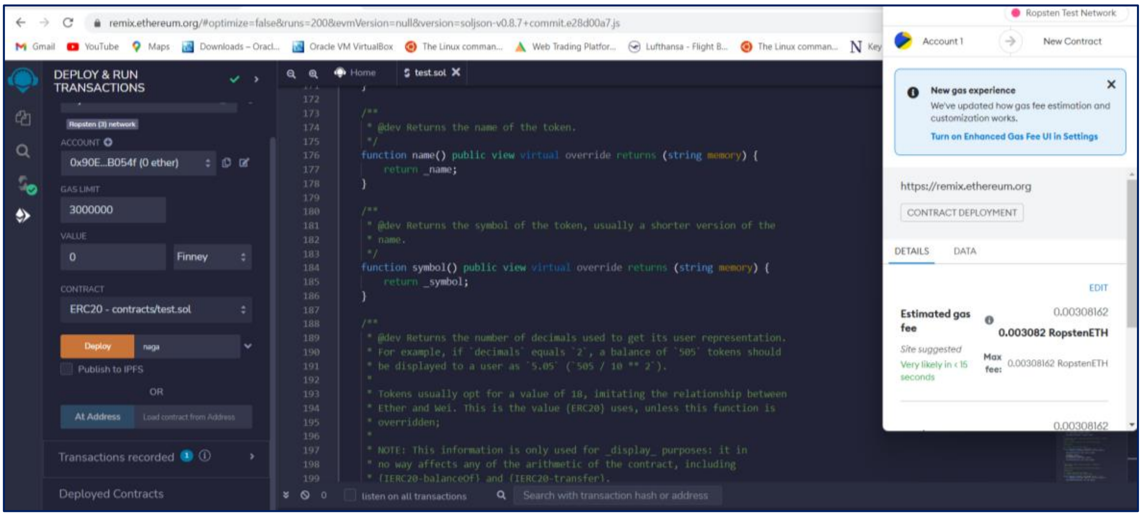
Step 2 & 3: Adding Free Faucet Tokens – required to execute smart contracts and simulate tests, and Receipt of Ropsten Tokens on our Metamask account.



Step 4 & 5: Etherscan for validation – Validated the Token transaction on Etherscan tool, and Creation of INFURA account - required for automation

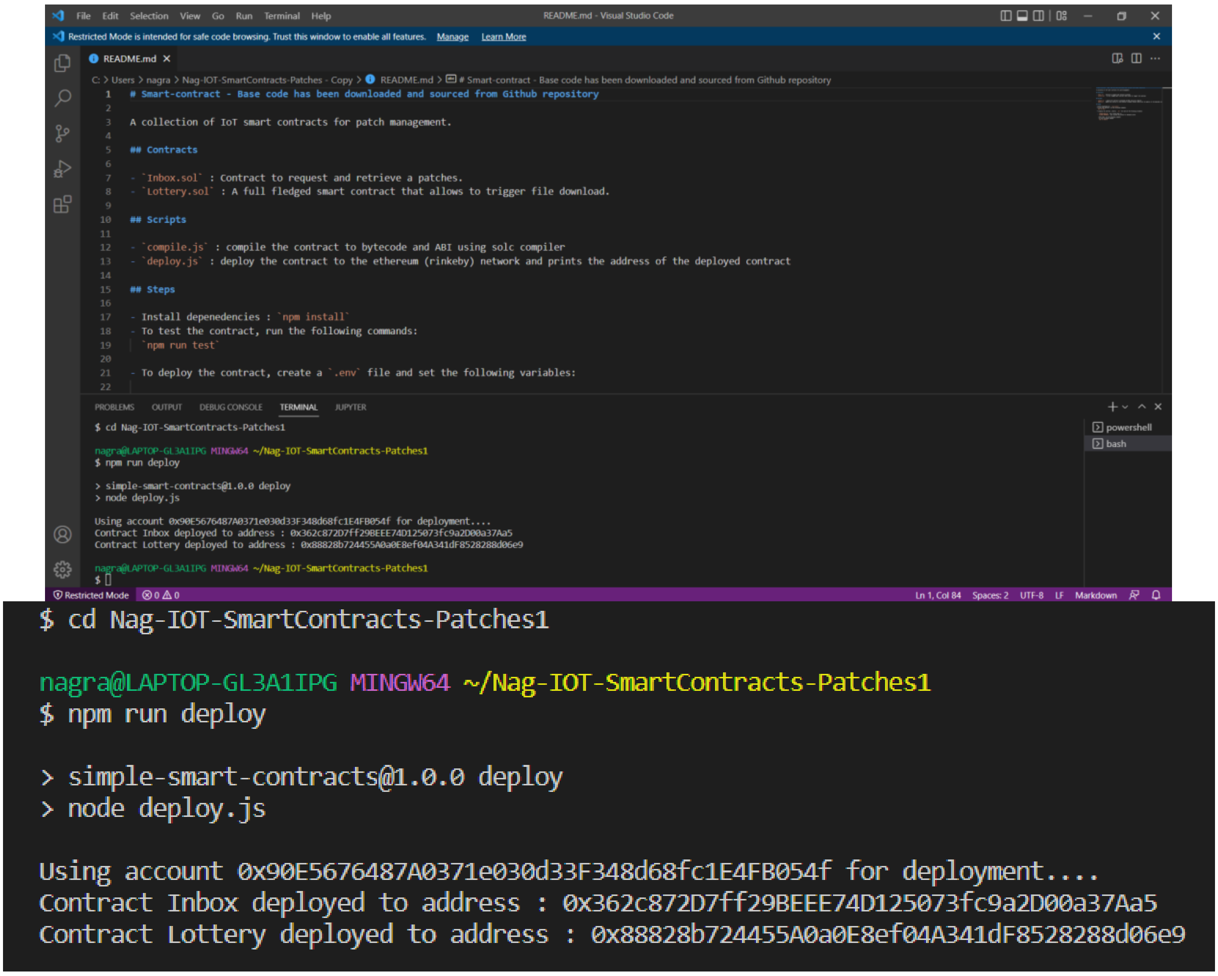


Step 6: Creating and testing Smart Contract in Remix, confirming the transaction through Metamask extension on browser (Das, 2022).

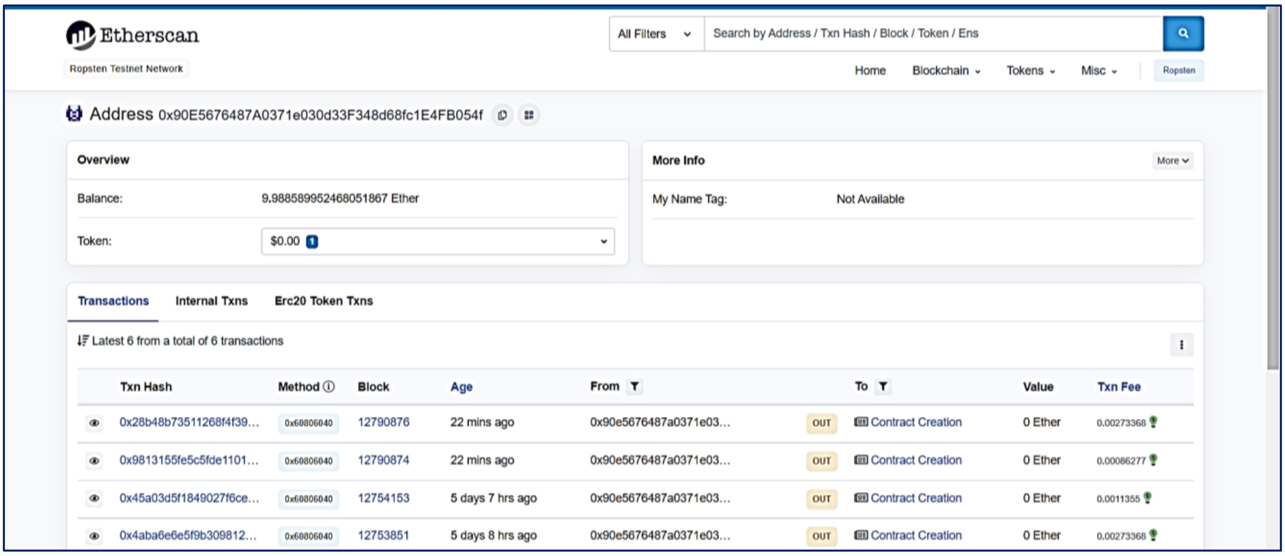


Step 7: Using Node.js & Visual studio code for automated script on Smart Contract creation

Step 8: Deploying Smart Contract – Base code has been sourced from Github repository (Das, 2022)



Step 9: Verifying transaction on Etherscan for the deployed Smart contract



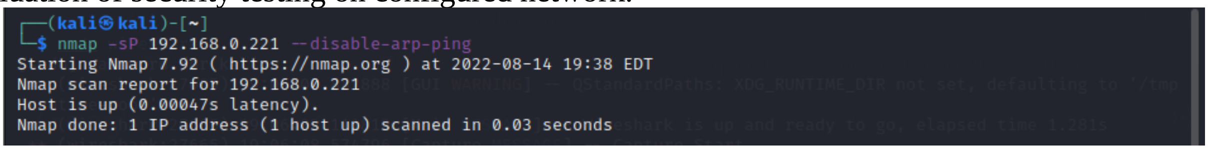
Smart Contracts: We were able to successfully demonstrate the deployment of Smart contracts using Blockchain platforms and solutions, this was the major part of the Blockchain solution planned to be deployed to achieve the objective of this research to involve Blockchain solution with the aim of addressing improper patch management capabilities. We are utilising Blockchain for two aspects, first is to utilise the ledger feature where the transactions are recorded and will help in root cause analysis or pure tracking purpose, this objective has been achieve with the above listed steps of deploying smart contracts. Second aspect was to trigger Patch download or file download post the smart contract deployment, but there is a limitation in Blockchain to handle large files or pay load transfers on blockchain networks and this requires another solution to be deployed, one of the possible solutions is using IPFS which will be discussed further.

IPFS (InterPlanetary File System): Integrating IPFS with Blockchain would have been the ideal next step to achieve an end-to-end secured File Transfer platform which can help achieve the objective and hypothesis of using Blockchain for secured Patch updates. We have been able to complete the first objective of deploying smart contract and maintaining a ledger of transaction for tracking and future root cause analysis purpose, we attempted at deploying an IPFS solution but needs more work in future to achieve this in a real-world scenario. We have looked at few research papers and found it to be a feasible option to deploy IPFS for achieving Patch downloads post Smart contract step.

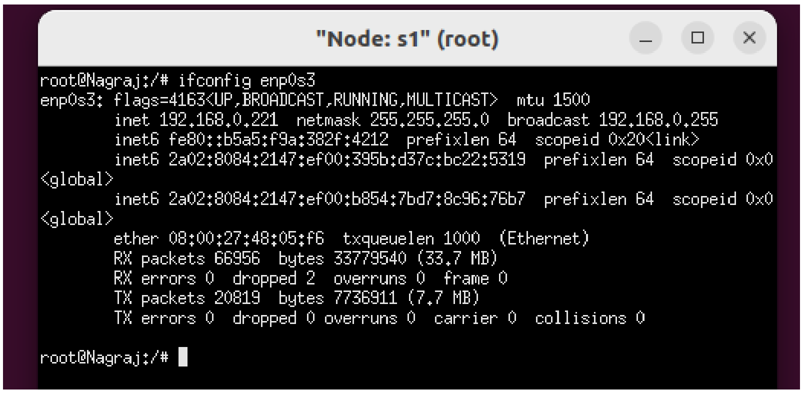
6 Evaluation

6.1 Simulate attacks and validation of alerts

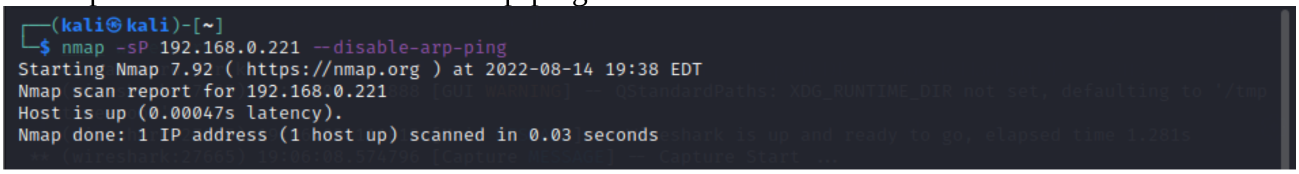
- Kali Linux virtual machine is being used as an external attacker to simulate penetration testing and for evaluation of security testing on configured network.



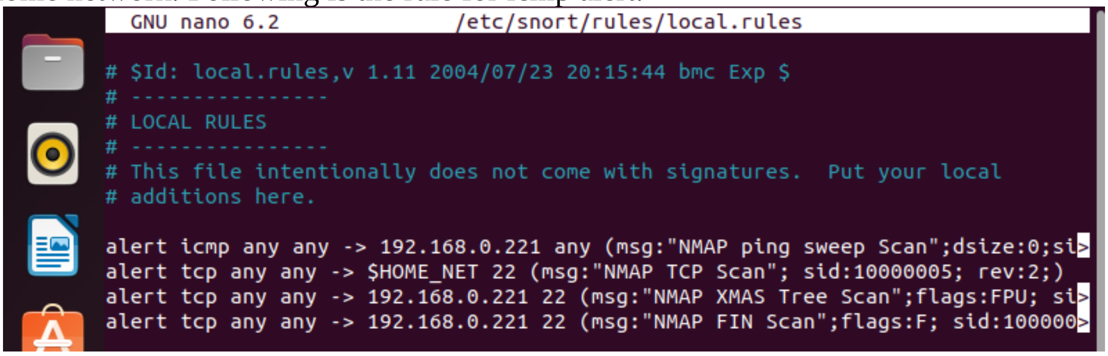
- Using mininet SDN on Ubuntu machine we have set up two host h1 and h2. To know the ip address of the node h1 first use following command which will open terminal of host 1.
  xterm h1
- Once the terminal is up use command ifconfig to know the ip address of it



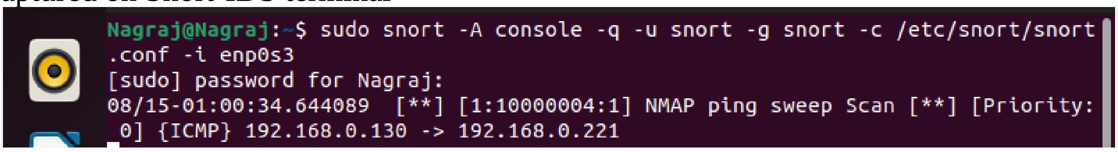
- We have set rules on Snort-IDS to alert the administrator, we will test the rules using nmap on kali linux.
- We will use below command to send icmp packages to host machine to know whether the host is up or not: nmap -sP 192.168.0.221 –disable -arp-ping



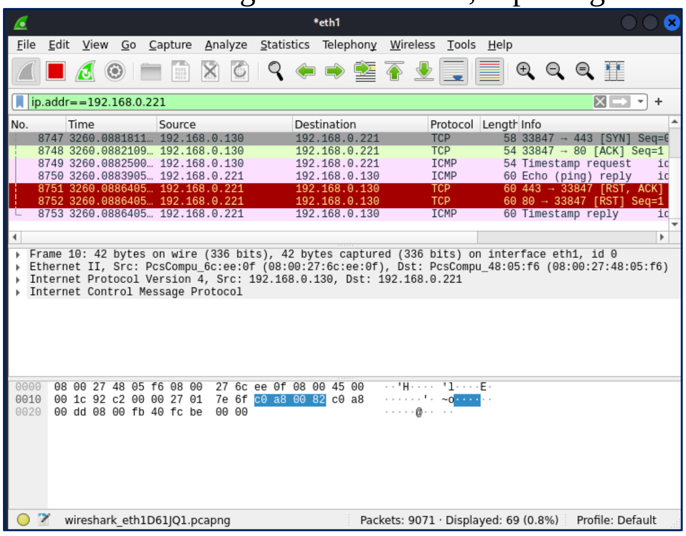
- We have set the rule for icmp packet to alert the administrator when coming from any external network to our home network. Following is the rule for icmp alert.



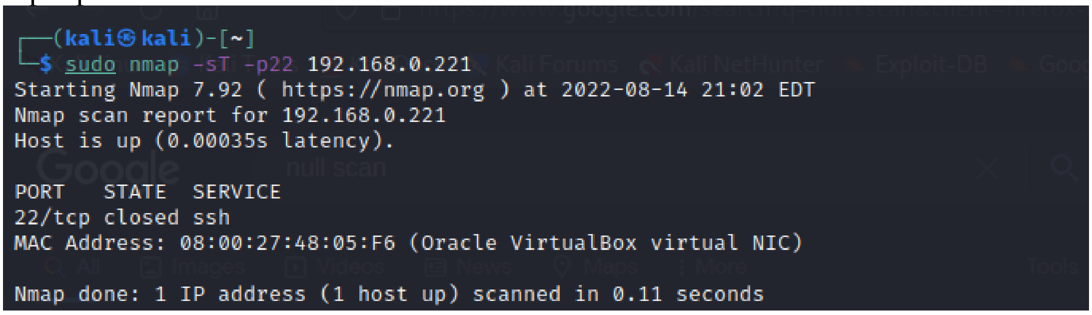
- Alert captured on Snort-IDS terminal



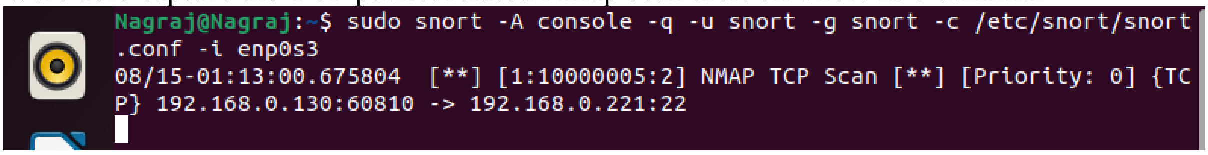
- Refer to below screenshot for wireshark logs related to snort, capturing the icmp packets



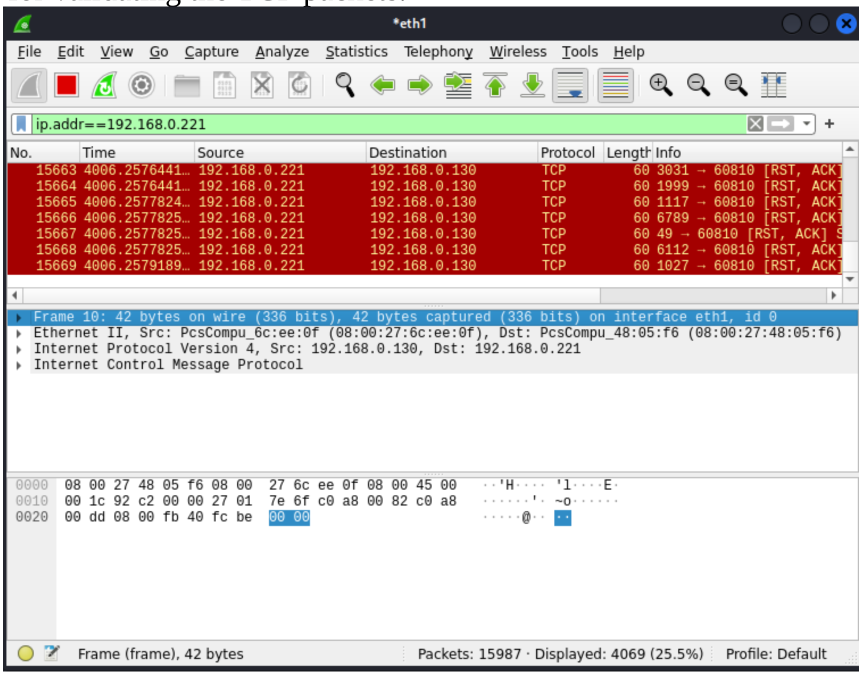
- Following screenshots demonstrates the alerts for tcp packets alert coming from any external network using nmap tcp scan



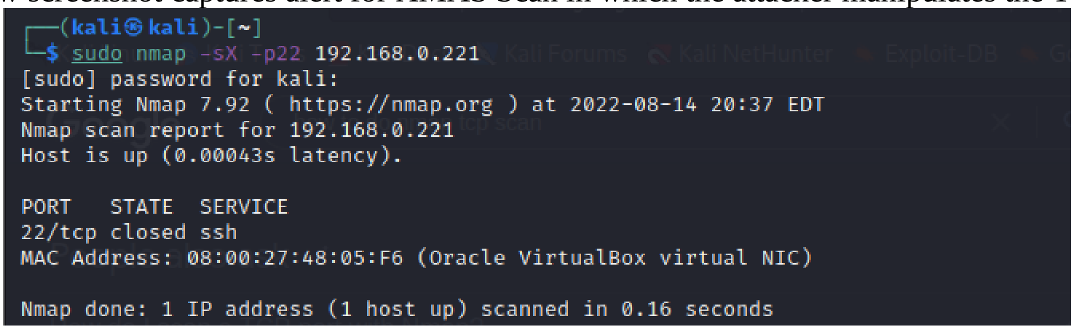
- We were able capture the TCP packet related Nmap scan alert on Snort-IDS terminal



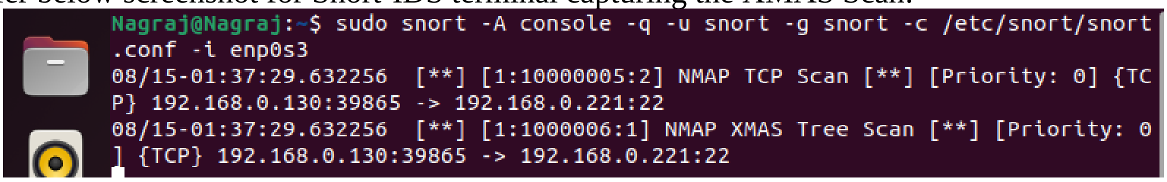
- Using Wireshark for validating the TCP packets.



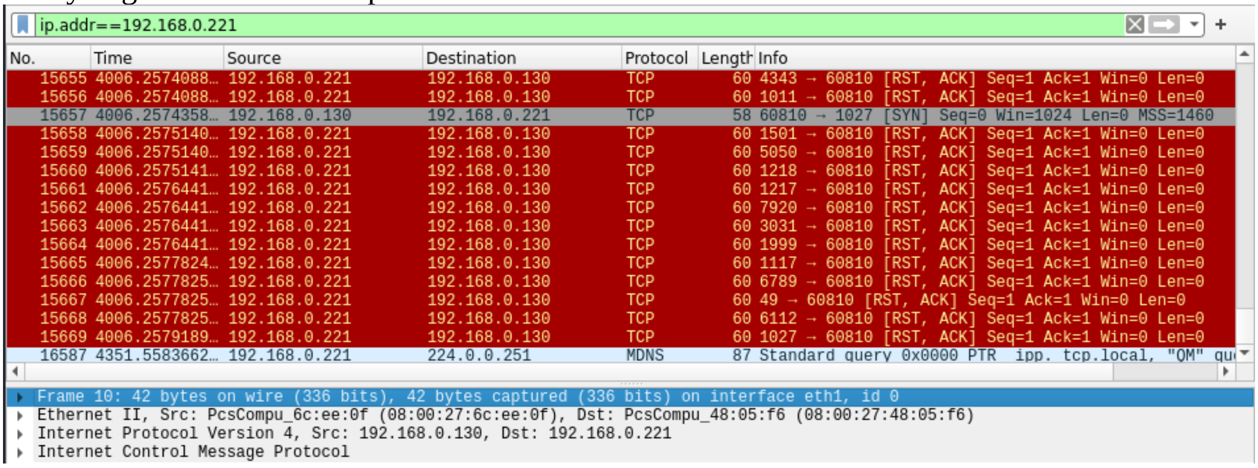
- Below screenshot captures alert for XMAS Scan in which the attacker manipulates the TCP header



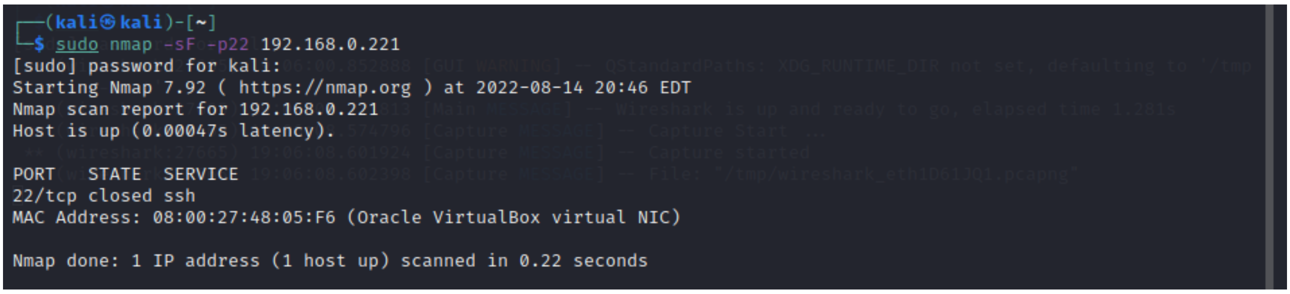
- Refer below screenshot for Snort-IDS terminal capturing the XMAS Scan:



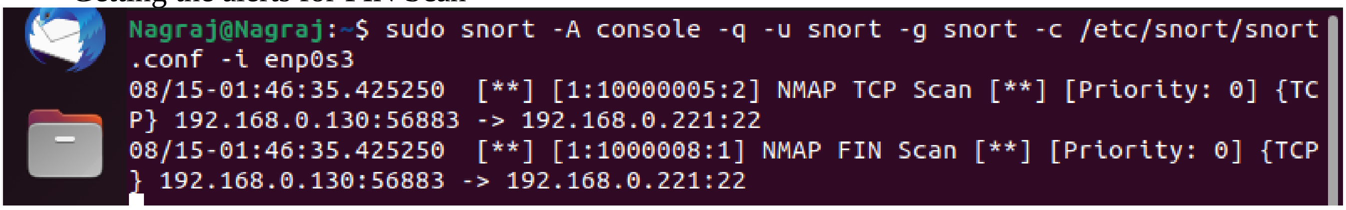
- Analyzing the wireshark output:



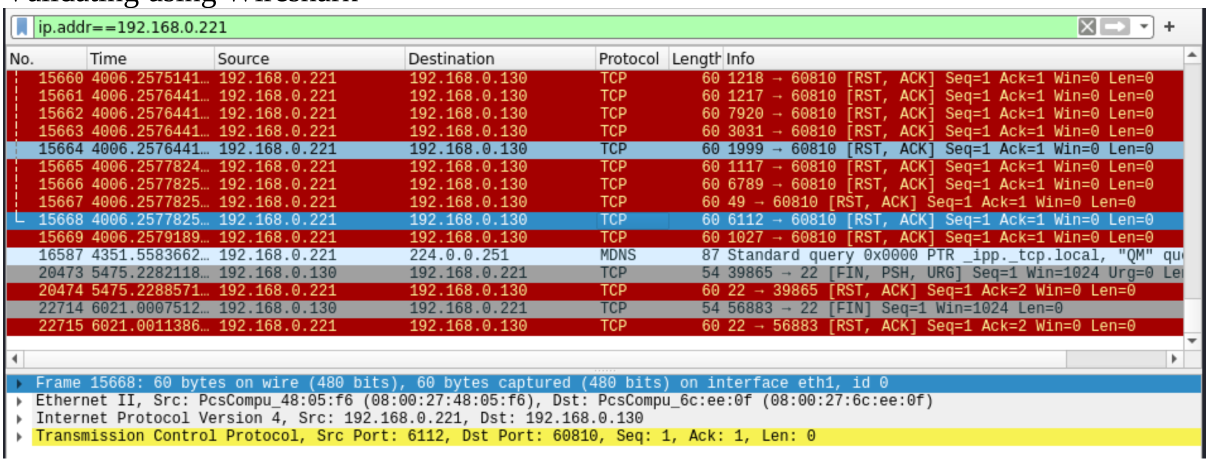
- Getting alert for FIN Scan which is used to terminate TCP connection after completion of the data transfer.



- Getting the alerts for FIN Scan



- Validating using Wireshark



- Capturing NULL Scan where the packets forwarded by the attacker are without flags

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sN -p22 192.168.0.221
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-14 20:56 EDT
Nmap scan report for 192.168.0.221
Host is up (0.00057s latency).

PORT   STATE  SERVICE
22/tcp closed ssh
MAC Address: 08:00:27:48:05:F6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

- Getting the alert message on Snort-IDS terminal

```
Nagraj@Nagraj:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort
.conf -i enp0s3
08/15-01:56:17.663552  [**] [1:10000005:2] NMAP TCP Scan [**] [Priority: 0] {TC
P} 192.168.0.130:35854 -> 192.168.0.221:22
08/15-01:56:17.663552  [**] [1:1000009:1] NMAP NULL Scan [**] [Priority: 0] {TC
P} 192.168.0.130:35854 -> 192.168.0.221:22
```

- Simulating DoS attack and replication a simple botnet attack: Getting alert for DOS Ping-Flood attack. For this, first using following command on attacker machine to send packets to victim machine : sudo hping3 -1 –fast 192.168.0,221

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -1 --fast 192.168.0.221
HPING 192.168.0.221 (eth1 192.168.0.221): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.221 ttl=64 id=13366 icmp_seq=0 rtt=4.7 ms
len=46 ip=192.168.0.221 ttl=64 id=13379 icmp_seq=1 rtt=11.9 ms
len=46 ip=192.168.0.221 ttl=64 id=13380 icmp_seq=2 rtt=3.9 ms
len=46 ip=192.168.0.221 ttl=64 id=13387 icmp_seq=3 rtt=6.1 ms
len=46 ip=192.168.0.221 ttl=64 id=13411 icmp_seq=4 rtt=5.1 ms
len=46 ip=192.168.0.221 ttl=64 id=13417 icmp_seq=5 rtt=4.4 ms
```

- Snort_IDS capturing the packets and giving alert on its terminal

```
Commencing packet processing (pid=36080)
08/15-02:39:49.098958  [**] [1:10000004:1] NMAP ping sweep Scan [**] [Priority:
 0] {ICMP} 192.168.0.130 -> 192.168.0.221
08/15-02:39:49.098958  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {ICMP} 192.168.0.130 -> 192.168.0.221
08/15-02:39:49.098958  [**] [1:384:5] ICMP PING [**] [Classification: Misc acti
vity] [Priority: 3] {ICMP} 192.168.0.130 -> 192.168.0.221
08/15-02:39:50.099722  [**] [1:10000004:1] NMAP ping sweep Scan [**] [Priority:
 0] {ICMP} 192.168.0.130 -> 192.168.0.221
08/15-02:39:50.099722  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {ICMP} 192.168.0.130 -> 192.168.0.221
08/15-02:39:50.099722  [**] [1:384:5] ICMP PING [**] [Classification: Misc acti
vity] [Priority: 3] {ICMP} 192.168.0.130 -> 192.168.0.221
08/15-02:39:51.100530  [**] [1:10000004:1] NMAP ping sweep Scan [**] [Priority:
 0] {ICMP} 192.168.0.130 -> 192.168.0.221
```

- Using Wireshark showing packet transfer

ip.addr==192.168.0.221

No.	Time	Source	Destination	Protocol	Length	Info
34097	9516.0655328…	192.168.0.221	192.168.0.130	ICMP	60	Echo (ping) reply id
34098	9516.1655202…	192.168.0.130	192.168.0.221	ICMP	42	Echo (ping) request id
34099	9516.1658601…	192.168.0.221	192.168.0.130	ICMP	60	Echo (ping) reply id
34100	9516.2662249…	192.168.0.130	192.168.0.221	ICMP	42	Echo (ping) request id
34101	9516.2666090…	192.168.0.221	192.168.0.130	ICMP	60	Echo (ping) reply id
34102	9516.3671508…	192.168.0.130	192.168.0.221	ICMP	42	Echo (ping) request id
34103	9516.3674554…	192.168.0.221	192.168.0.130	ICMP	60	Echo (ping) reply id
34104	9516.4675007…	192.168.0.130	192.168.0.221	ICMP	42	Echo (ping) request id
34105	9516.4679374…	192.168.0.221	192.168.0.130	ICMP	60	Echo (ping) reply id
34106	9516.5711100…	192.168.0.130	192.168.0.221	ICMP	42	Echo (ping) request id
34107	9516.5715135…	192.168.0.221	192.168.0.130	ICMP	60	Echo (ping) reply id
34108	9516.6714561…	192.168.0.130	192.168.0.221	ICMP	42	Echo (ping) request id
34109	9516.6717904…	192.168.0.221	192.168.0.130	ICMP	60	Echo (ping) reply id
34110	9516.7951995…	192.168.0.130	192.168.0.221	ICMP	42	Echo (ping) request id
34111	9516.7955832…	192.168.0.221	192.168.0.130	ICMP	60	Echo (ping) reply id

```
Frame 25192: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth1, id 0
Ethernet II, Src: PcsCompu_6c:ee:0f (08:00:27:6c:ee:0f), Dst: PcsCompu_48:05:f6 (08:00:27:48:05:f6)
Internet Protocol Version 4, Src: 192.168.0.130, Dst: 192.168.0.221
```

6.3 Discussion: I have conducted several tests during the course of these implementations and evaluations to review the functionality of the deployed tools and services, same time have conducted Penetration testing to evaluate the security capability and alert mechanisms, based on the observations I can state that the proposed solutions have tremendous potential to secure IoT in a Novel way and these solutions are scalable in nature as well hence applicable to wide variety of use cases starting from Home based IoT Network to Industrial, Healthcare and other similar setups.

7 Conclusion and Future Work

Conclusion: This work was aimed at securing and defending IoT using SDN, IDS and Blockchain capabilities and solutions. I have explored several possible solutions using these technologies and researched extensively, based on my research I have been able to establish that it is possible to achieve the objectives outlined in this research paper and research question.

I have used Mininet Tool to demonstrate an SDN based connectivity and combined it with Snort based IDS tool to provide a layer of security where Cyberthreats like Botnet attacks and Data privacy issues can be mitigated. This setup was tested using Penetration testing methodologies and we could observe the results where there is an enhanced level of protection provided by this setup compared to the standard home based IoT connectivity without any such security layer. Snort based IDS played a critical role in monitoring, analysing and detecting the potential security incidents.

I have used Blockchain based Smart contract solution and relevant tools to address the improper patch management capability and file download or transactions related security concerns. This particular objective has been achieved partially where we were able to demonstrate the deployment of Smart contract but could not utilise Blockchain as a standalone solution to transfer files, instead as per research we could observe other solutions or DAPP for achieving the final part of File transfer trigger.

These demonstrations were able to answer the maximum percentage of the Research question of security issues in IoT by using Blockchain, IDS and SDN solutions. The only pending part of transferring the Files using blockchain solution can be addressed using integration of Tools like IPFS as observed in some of the research papers and needs to be conducted as a future scope of work.

Future work: There is a scope to package all these components in a single VM or a lightweight tool etc. with an SOP which will make it easier for a layman or non-tech savvy people as well to utilise the security benefits of SDN, IDS and Blockchain in securing IoT Networks which includes Home IoT, Industrial IoT and Healthcare among others. Another future scope of work is to deploy a suitable IPFS (InterPlanetary File System) solution integrated with Blockchain to trigger a successful Patch download and File transfer mechanism for IoT.

Acknowledgement

I would like to thank my Professor and Supervisor Mr. Rohit Verma for all his guidance and support throughout this Thesis research project. His immense knowledge, patience and enthusiasm has kept me motivated. His inputs have helped me tremendously during the time of research, testing and writing this report.

References

Al-Kasassbeh, M., Almseidin, M., Alrfou, K., Kovacs, S., 2020. Detection of IoT-botnet attacks using fuzzy rule interpolation. J. Intell. Fuzzy Syst. 39, 421–431. https://doi.org/10.3233/JIFS-191432

Baliyan, A., Dhatterwal, J.S., Kaswan, K.S., Jain, V., 2022. Role of AI and IoT Techniques in Autonomous Transport Vehicles, in: Marati, N., Bhoi, A.K., De Albuquerque, V.H.C., Kalam, A. (Eds.), AI Enabled IoT for Electrification and Connected Transportation, Transactions on Computer Systems and Networks. Springer Nature, Singapore, pp. 1–23. https://doi.org/10.1007/978-981-19-2184-1_1

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K.N., Nadeau, E., O'Rourke, D.G., Piccarreta, B., Scarfone, K., 2019. Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks (No. NIST IR 8228). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8228

Borys, A., Kamruzzaman, A., Thakur, H.N., Brickley, J.C., Ali, M.L., Thakur, K., 2022. An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet, in: 2022 IEEE World AI IoT Congress (AIIoT). Presented at the 2022 IEEE World AI IoT Congress (AIIoT), pp. 725–729. https://doi.org/10.1109/AIIoT54504.2022.9817163

Boyes, H., Hallaq, B., Cunningham, J., Watson, T., 2018. The industrial internet of things (IIoT): An analysis framework. Comput. Ind. 101, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

Christidis, K., Devetsikiotis, M., 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Collela, P., n.d. Ushering In A Better Connected Future. URL https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/ushering-in-a-better-connected-future (accessed 4.4.22).

Das, S., 2022. simple-smart-contract - https://github.com/subhasis020299/simple-smart-contracts.

Djenna, A., Eddine Saidouni, D., 2018. Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure. Presented at the 2018 2nd Cyber Security in Networking Conference (CSNet), IEEE, Paris, pp. 1–4. https://doi.org/10.1109/CSNET.2018.8602974

Dorri, A., Kanhere, S.S., Jurdak, R., 2017. Towards an Optimized BlockChain for IoT, in: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). Presented at the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 173–178.

Farahani, B., Firouzi, F., Chakrabarty, K., 2020. Healthcare IoT, in: Firouzi, F., Chakrabarty, K., Nassif, S. (Eds.), Intelligent Internet of Things: From Device to Fog and Cloud. Springer International Publishing, Cham, pp. 515–545. https://doi.org/10.1007/978-3-030-30367-9_11

Farris, I., Taleb, T., Khettab, Y., Song, J., 2019. A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems. IEEE Commun. Surv. Tutor. 21, 812–837. https://doi.org/10.1109/COMST.2018.2862350

Flauzac, O., González, C., Hachani, A., Nolot, F., 2015. SDN Based Architecture for IoT and Improvement of the Security, in: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops. Presented at the 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, pp. 688–693. https://doi.org/10.1109/WAINA.2015.110

Herwig, S., Harvey, K., Hughey, G., Roberts, R., Levin, D., 2019. Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet, in: Proceedings 2019 Network and Distributed System Security Symposium. Presented at the Network and Distributed System Security Symposium, Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2019.23488

Islam, Md.T., Islam, N., Refat, Md.A., 2020. Node to Node Performance Evaluation through RYU SDN Controller. Wirel. Pers. Commun. 112, 555–570. https://doi.org/10.1007/s11277-020-07060-4

Javaid, A.Y., Bandekar, A., 2017. Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices. Presented at the 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), IEEE, Honolulu, HI, pp. 1631–1636. https://doi.org/10.1109/CYBER.2017.8446380

Jianjun, S., Ming, L., Jingang, M., 2020. Research and application of data sharing platform integrating Ethereum and IPFs Technology, in: 2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES). Presented at the 2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), pp. 279–282. https://doi.org/10.1109/DCABES50732.2020.00079

Kaur, K., Singh, J., Ghumman, N., 2014. Mininet as Software Defined Networking Testing Platform.

Kolias, C., Kambourakis, G., Stavrou, A., Voas, J., 2017. DDoS in the IoT: Mirai and Other Botnets. Computer 50, 80–84. https://doi.org/10.1109/MC.2017.201

Kshetri, N., 2017. Can Blockchain Strengthen the Internet of Things? IT Prof. 19, 68–72. https://doi.org/10.1109/MITP.2017.3051335

MediaDSCI, n.d. IOT TECHNOLOGY IN INDIA. IOT Technol. INDIA. URL https://community.nasscom.in/communities/emerging-tech/iot-ai/iot-technology-in-india.html (accessed 4.4.22).

Mylrea, M., Gourisetti, S.N.G., 2018. Blockchain for Supply Chain Cybersecurity, Optimization and Compliance. pp. 70–76. https://doi.org/10.1109/RWEEK.2018.8473517

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N., 2019. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutor. 21, 2702–2733. https://doi.org/10.1109/COMST.2019.2910750

Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R.U., Dou, W., 2020. Complementing IoT Services Through Software Defined Networking and Edge Computing: A Comprehensive Survey. IEEE Commun. Surv. Tutor. 22, 1761–1804. https://doi.org/10.1109/COMST.2020.2997475

Rahman, A., Islam, Md.J., Sunny, F.A., Nasir, M.K., 2019. DistBlockSDN: A Distributed Secure Blockchain Based SDN-IoT Architecture with NFV Implementation for Smart Cities, in: 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET). Presented at the 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), pp. 1–6. https://doi.org/10.1109/ICIET48527.2019.9290627

Rajeswari, D., R, S., S, R., M, P., 2022. Intelligent Refrigerator using Machine Learning and IoT, in: 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). Presented at the 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), pp. 1–9. https://doi.org/10.1109/ACCAI53970.2022.9752587

Shafagh, H., Burkhalter, L., Hithnawi, A., Duquennoy, S., 2017. Towards Blockchain-based Auditable Storage and Sharing of IoT Data, in: Proceedings of the 2017 on Cloud Computing Security Workshop. Presented at the CCS '17: 2017 ACM SIGSAC Conference on Computer and Communications Security, ACM, Dallas Texas USA, pp. 45–50. https://doi.org/10.1145/3140649.3140656

Soetens, N., Famaey, J., Verstappen, M., Latré, S., 2015. SDN-based management of heterogeneous home networks, in: 2015 11th International Conference on Network and Service Management (CNSM). Presented at the 2015 11th International Conference on Network and Service Management (CNSM), pp. 402–405. https://doi.org/10.1109/CNSM.2015.7367391

Solangi, Z.A., Solangi, Y.A., Chandio, S., bt. S. Abd. Aziz, M., bin Hamzah, M.S., Shah, A., 2018. The future of data privacy and security concerns in Internet of Things, in: 2018 IEEE International Conference on Innovative Research and Development (ICIRD). Presented at the 2018 IEEE International Conference on Innovative Research and Development (ICIRD), pp. 1–4. https://doi.org/10.1109/ICIRD.2018.8376320

Yassein, M.B., Abuein, Q., Alasal, S.A., 2017. Combining software-defined networking with Internet of Things: Survey on security and performance aspects, in: 2017 International Conference on Engineering & MIS (ICEMIS). Presented at the 2017 International Conference on Engineering & MIS (ICEMIS), pp. 1–7. https://doi.org/10.1109/ICEMIS.2017.8273027