ARCSECURE - CENTRALIZED HUB FOR SECURING A NETWORK OF IOT DEVICES

Project ID: 2020-086

Project Proposal Report

IT17009614 - A.M.I.S Abeykoon

IT17127356 - A.M.S.P.B Atapattu

IT17078306 - H.N Jayawardhane

IT17126816 - C.N Samarasekara

Bachelor of Science (Hons) Degree in Information Technology

Specialized in Cyber Security

Department of Information Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

February 2020

ARCSECURE - CENTRALIZED HUB FOR SECURING A NETWORK OF IOT DEVICES

Project ID: 2020-086

Project Proposal Report

IT17009614 - A.M.I.S Abeykoon

IT17127356 - A.M.S.P.B Atapattu

IT17078306 - H.N Jayawardhane

IT17126816 - C.N Samarasekara

Supervisor - Mr. Kavinga Yapa Abeywardena

Co supervisor – Ms. Tharika Munasinghe

Bachelor of Science (Hons) Degree in Information Technology Specialized in Cyber Security

Department of Information Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

February 2020

DECLARATION

We declare that this is our own work and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
A.M.I.S Abeykoon	IT17009614	
A.M.S.P.B Atapattu	IT17127356	
H.N Jayawardhane	IT17078306	
C.N Samarasekara	IT17126816	

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of the Supervisor: Date:

ABSTRACT

As far as it is considered, IoT has been a game changer in the advancement of technology. In the current context, the major issue that users face is the threat to their information stored in these devices. Modern day attackers are well aware of vulnerabilities in existence in the current IoT environment. Therefore, securing information from being gone into the hands of unauthorized parties is of top priority. With the need of securing the information came the need of protecting the devices which the data is being stored. Small Office/Home Office (SOHO) environments working with IoT devices are particularly in need of such mechanism to protect the data and information that they hold in order to sustain their operations. Hence, this research will be addressing the means and needs of protecting a network of IoT devices in a SOHO environment. In order come up with a well-rounded security mechanism from every possible aspect, this research proposes a plug and play device "ARCSECURE" with not only mechanisms to detect and mitigate attacks but also will be going deeper into authorizing access centrally as well as automating the updating process as a method of prevention for better user experience and provide uninterrupted business operations.

Keywords: Internet of Things, Information Security, Machine Learning, DoS, DDoS, Blockchain, Authentication, Authorization, Detection, Mitigation

Table of Contents

I List of Figures

II List of Tables

III List of Abbreviations

IOT	Internet of Things
DOS	Denial of Service File System
DDOS	Distributed Denial of Service
SOHO	Small Office Home Office
ML	Machine Learning
HTTP	Hypertext Transfer Protocol
OWASP	Open Web Application Security Project
SVM	Support Vector Machine
FCM	Fuzzy C- Means
OS	Operating System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SSO	Single Sign-On
MFA	Multi-Factor Authentication
PIN	Personal Identification Number
SVM	Support Vector Machine
GA	Genetic Algorithm
App	Application
Et al.	‘and others’

1 INTRODUCTION

1.1 Background

Protecting information, providing security for information is a major concern of any user. In a business environment, loss or unauthorized modification of information/ data could put the whole business's functions at a hold and even create great losses financially and reputationally. For a Small Office/ Home Office (SOHO) environment the organization will hold various information related to the organization [1], customers and suppliers etc. If in case one of this device are compromised the whole network of devices will be at a risk of being attacked. Therefore, each and every one of the devices within the network should be protected to guarantee that the network is safeguarded [2].

Malware attacks such as trojan horses and spyware could easily go undetected and the user could lose information without their knowledge. Many attacks go undetected due to the lack of expertise within the users to detect suspicious behavior and in some cases even if the user was able to identify anomalies in the functionality of the system it can be hard to come up with a mitigation option without the proper knowledge and expertise because simply shutting down the machine won't help in this case. Therefore, it is essential that better mechanisms have been put into place to immediately detect and address such attacks [3].

Even if such attacks are detected and stopped from entering the system at an early stage, their can be instances where authentication stage is compromised. For an instance if the user writes down his/ her password to the system on a piece of paper and it goes to the hands of an attacker the system will be unable to detect if this user is a legitimate user in the system or not. Or there could also be situations where an attacker would brute force their way to the system. All these are possible ways to bypass the way into the systems. These attackers could be competitors, hacktivists or

even an internal employee. Hence all possibilities should be considered when coming up with a well-rounded solution for the business.

Another aspect that goes undetected are the vulnerabilities of the system. Many operating systems running on the devices are constantly being identified to be having vulnerabilities [4]. Attackers with the knowledge upon these could easily exploit the systems and get ahold of information stored in the devices. Hence, the vendors make sure that these vulnerabilities are regularly patched in order to provide protection for user's information and sensitive data. Even though vendor protection is provided by these patches, often times users are used to deferring the update procedures without the knowledge of the need of these being essential for the device's to be up and running.

Taking all above mentioned aspects into account is a necessity when coming up with a solution to protect business functionalities in a SOHO environment working with a network of IoT devices. Hence the device proposed by this research "ARCSECURE" will be addressing all these issues in order to come up with a conversant solution.

2 LITERATURE REVIEW

This section depicts a literature survey about the purposed system and its functions. Some of the eminent researches and products are also reviewed here. Since the research is in the domain of networking and internet of things, the final product is designed to plug and play, the development environment must be configured such that a single codebase can be pushed to multiple peers simultaneously. This section will be subdivided into 4 sub-sections based on the components that will be covered through this research.

2.1 Botnet Prevention

Shivaramu K and Prasobh P.S discuss in their research paper Security Vulnerabilities that the Wireless Ad-hoc network is vulnerable due to cooperative algorithms, lack of monitoring and management and lack of a particular line of defense [7]. The approach considered is to use feature selection mechanism and build the classifier using various machine learning algorithms such as SVM, K-NN, Fuzzy c-means clustering and decision tree. An important conclusion drawn from the experimental results is that, of the various methods used, Fuzzy c-means clustering is very efficient in detecting DDoS attacks [8].

2.2 DOS Detection and P2P Connection

Recent botnet attacks show a high vulnerability of IoT systems and devices. From the basis of this research, literature has been reviewed. Per the [1], explains that common IoT vulnerabilities such as,

- Insecure web/mobile/cloud interface
- Insufficient authentication/ authorization
- Insecure network services
- Lack of transport encryption/integrity verification
- Privacy concerns
- Insufficient security configuration
- Insecure software/firmware
- Poor physical security

In September 2016, an IoT botnet built from the Mirai malware perhaps the largest botnet on record was responsible for a 600 Gbps attack targeting Brian Krebs's security blog (krebsonsecurity.com). Mirai's strategy is quite simple; it uses a list of 62 common default usernames and passwords to gain access primarily to home routers, network-enabled cameras, and digital video recorders, which usually have less robust protection than other consumer IoT devices. The same month, a Mirai-based attack against the French WebHost OVH broke the record for the largest recorded distributed denial of service attack.

2.3 User authentication with Keystroke dynamics

Keystroke dynamics have been researched for a long time. In 2002 Bergadano et al [5] researched keystroke dynamics for user authentication using the volunteer's self-collected dataset, data collected using the same text for all individuals, resulting in only 0.01 percent passing the authentication impostor. In 2003, Yu and Cho [6] performed preliminary experimental research on the selection of a function subset selection of keystroke dynamics identity verification and found that GA-SVM yielded good accuracy and speed of learning. Revett et al. [7] researched user authentication in 2007 and began researching authentication for a dynamic keystroke. The author has suggested that biometrics are robust, specifically fingerprints, but they can be easily spoofed.

2.4 Update automation with blockchain

It is recommended by OWASP that systems are regularly updated as a countermeasure to securing IoT[2]. The bottleneck, in this case, is that a SOHO environment might not have the necessary technical teams when compared to a large scale enterprise where necessary updates can be checked and deployed into the systems[3]. Hence automating the process will be the best possible option under the given circumstances. In this case, even if the process was automated it is necessary to have a mechanism to check if the update is legitimate because an attacker could disguise an old version of the software which contains security vulnerability as the version offered as the latest by the vendor[3]. This would revert the system to a faulty version giving attacker access[3]. A faulty software could

leave the hardware vulnerable involuntarily[4]. Hence by the use of an integrity checker this research aims to overcome the risk of installing a faulty hoax version of software into the user's system without the involvement of the user. After the update has been done it is essential to check if it has been done successfully which is where blockchain will come into the light. Blockchain has 4 main components. [5]

1) Network of Nodes: Nodes that are connected through the internet will maintain all transactions made on the network of blockchain. Once a transaction has taken place it will add it to the past transactions ledger. This will be named as "mining"[5]

2) Distributed database system: Every node of the system will contain copies of information of the composed blocks. Each block will contain a timestamp and a list of transactions that will link blocks of the previous chain.[5]

3) Shared ledger: Each time a transaction takes place, the ledger will be updated.[5]

4) Cryptography: Data bound with a strong crypto mechanism. Which will be hard to track by an external unauthorized party.[5]

3 RESEARCH GAP

In the present, most hardware/software vendors have identified the need of user's requirement of information stored in their devices being protected. To an extent, vendors have been able to provide the users with satisfiable solutions, but they are areas that have not been identified and addressed in order to come up with a fool proof solution built into one device.

There are many devices such as Bitdefender Box and Avira Safe things [1] to ensure security within a network of IoT devices. Yet for example Bitdefender Box does not provide functionalities to mitigate detected attacks, access control amongst users or push updates without user interaction [2]. Therefore, it will require the user to manually push updates and take care of access control criteria, but in a SOHO environment there might not have the necessary expertise in cyber security and networking to facilitate such requirement in order to take necessary measures to take immediate actions against such detection.

Hence, there is a requirement for a device that would know how to not only detect but also has the ability to mitigate such attack, provide a mechanism to absolutely make sure that this is the legitimate user access the device and keep the system up to date but also could rollback the version in to the previous version if the system ends up failing to perform normal tasks.

In order to bridge this gap, we propose the device "ARCSECURE" as a fully functional, well-rounded system for SOHO environment to protect data and information without the need of expert knowledge.

Features	Bitdefender BOX	CUJO Firewall	F-Secure	ZingBOX	LUMA	Praetorian	ARCSECURE
1. Device Management portal with user friendly interface	✓	✓	✓	✓	✓	✓	✓
2. Vulnerability assessment of the devices in the network	✓		✓				✓
3. Scanning all the traffic coming from the network before forward to IoT device	✓	✓					✓
4. DDoS, Botnet attack detection with self-learning algorithm	✓			✓			✓
5. Enable user privacy by securing the communication with blockchain technology							✓
6. Exploit prevention in the IoT devices		✓					✓
7. Brute force protection with account lookout mechanism	✓		✓		✓		✓
8. Update automation mechanism							✓
9. User identification with behavioral traits							✓
10. Advanced parental control over IoT environment	✓		✓			✓	✓

1 Figure 3.1 Features of ARCSECURE DDoS and Secure communication module

4 RESEARCH PROBLEM

Ensuring security of the users in an IoT enabled environment is quite challenging yet this research aims to address the problem with a unique approach. The problem to be addressed here is that how this can be done. As stated in the gap it is evident that devices in the current market does not address all issues under discussion, detecting attacks such DoS/DDoS and immediately establishing a mechanism to fight against it, making sure that even legitimate user credentials are checked for other factors before providing system access and making sure that the system is kept up to date and all known vulnerabilities are patched. It is essential that the system performs its desired functions in order for the user to perform business functions to keep the business running. If in case the system loses stability in shows abnormal behavior the user will face great difficulty in performing their day to day work, hence it should also be kept in mind that system stability is protected throughout the course of business. Therefore, "ARCSECURE" will address this issue effectively by establishing controls and options to keep user information secure while maintaining system stability, which will be further discussed.

5 OBJECTIVES

5.1 Main Objectives

The main objective of the research is to provide a plug and play device targeting for IoT enabled environment of SOHO business environments and small-scale businesses to provide a secure communication and risk-free experience with a well-secured IoT environment. Most of the networking IoT devices are very difficult to maintain because of the lack of security issues and lack of knowledge on these devices. There should be a proper mechanism to protect IoT devices to take the maximum use of that device as well as to get maximum security out of that device. Most of the time organizations have to pay a huge amount of money to hire an expert to configure these devices and it takes more time to get the final usability of that device. The proposed device 'ARCSECURE' will be able to adopt to the network and do the needed configurations by itself. Even without a thorough knowledge in IT, the users will be able to get the similar productivity provided by proposed device achieved with unsupervised and supervised machine learning techniques and blockchain technology.

5.2 Specific Objectives

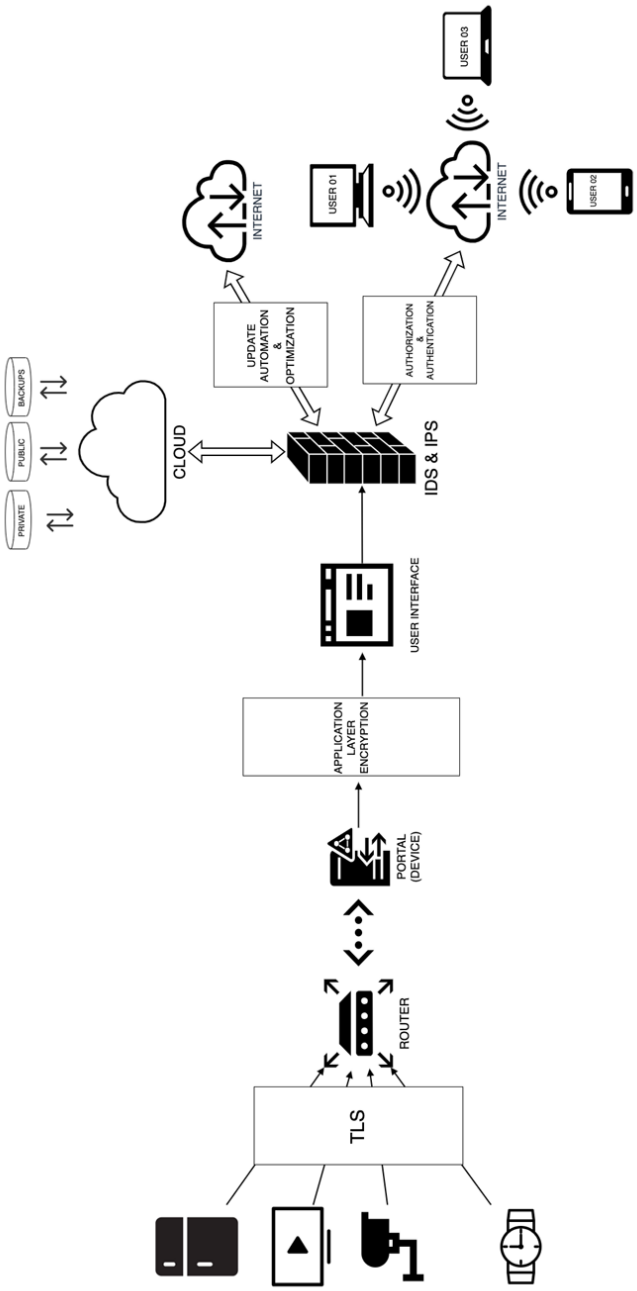
- Create a way to implement backend of the IDS to collect all the packets passing through.
- Implement the IDS engine to process the collected packets to capture any intrusion attempt of any data packet.
- Identify a method to notify the user when an any malicious data packet is found and store the collected details in a Db and use that information to train the ML algorithm.
- Identify a Machine Learning algorithm for find malicious data packets when scanning process.
- Identify a method to secure the communication between IoT devices.
- Implement a process to identify and analyze the malicious packets receiving trough the network daily basis.

- Identify number of users connected and using IoT devices over the network and alert them for any intrusion attempts using a method of communication
- Identify a tactical way to learn Machine Learning algorithm by itself using receiving data packets and pre-defined configurations.
- Implement policies to track all incoming packets other than using only Machine Learning algorithms.
- Create signature-based engine for attack detection module for support the scanning stage of the module
- Implement mechanisms for countermeasure selection to mitigation module for received data packets after the ML training process.
- Disabling the auto-update option of the device.
- Mechanism to cross check the file size of the received update on the device and cross check the file size with the device's site's update file size.
- If the sizes are the same, push update into the device. If not, establish a mechanism to delete the corrupted file from the system.
- Store the hash value of the device's pre-update block as well as the hash value of the device post-update block by using the blockchain.
- Establish a mechanism to check the values against each other to confirm if the update has been successful.
- Find a suitable Machine Learning algorithm to detect any kind of behavior in the system which deviates from the normal/anticipated behavior.
- Find test data and training the machine with the use of selected algorithms.
- Store backup of the device's previous software version file.
- Enable a mechanism to install the previous version software file if in case any abnormality within the system is detected.
- Disabling open unwanted IP ports of the device.
- Monitoring IP ports 2323/TCP and 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet).
- Monitoring for anomalous traffic on port 48101, as infected devices often attempt to spread malware by using this port to send results to the threat actor.

- Implement way to identify half open connections with learning module.
- Implement IP filtering mechanism.
- Implement protocol-based IDS to monitoring and analysis on a specific device protocol.
- Find suitable machine learning algorithms to detect anomaly of the system.
- Implement anomaly-based IPS to detect any type of misuse that falls out of normal system operation with learning module.
- Implement network monitoring system to monitor incoming and outgoing sensitive data.
- Create a captive portal.
- Create a token-based multi-factor authentication mechanism.
- Create a mobile application.
- Create a mechanism for device authentication.
- Create a fingerprint scanner in the mobile app.
- Have the mobile application pop a simple yes/no to validate the user upon signing in.
- Implement an access control feature that governs the authority of a user.
- Developing a machine learning algorithm for keystroke dynamics.
- Train the algorithm to identify keystrokes.
- Create a feature to temporarily block a user's IP upon being proven false.
- Create a mechanism to alert the user on possible false intrusion attempts.

6 RESEARCH METHODOLOGY

This section will explore the research components and the methodology in which the research workload is carried out to build the plug and play device **ARCSECURE**. The final output of this research is a portable device with 4 core functions.

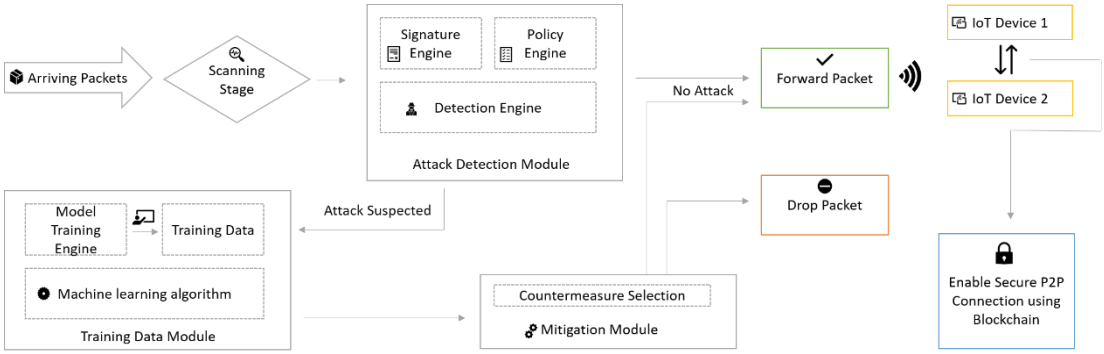


2 Overall system diagram

6.1 DDoS prevention and enabling secure communication module

One of those core functions is enabling secure communication over IoT devices while detecting DDoS threats to utilize and communicate IoT devices with a proper manner. Eg: By analyzing all data packets coming from the internet to the device and learn ML algorithm using that information. The whole process is illustrated in Figure 8.1.

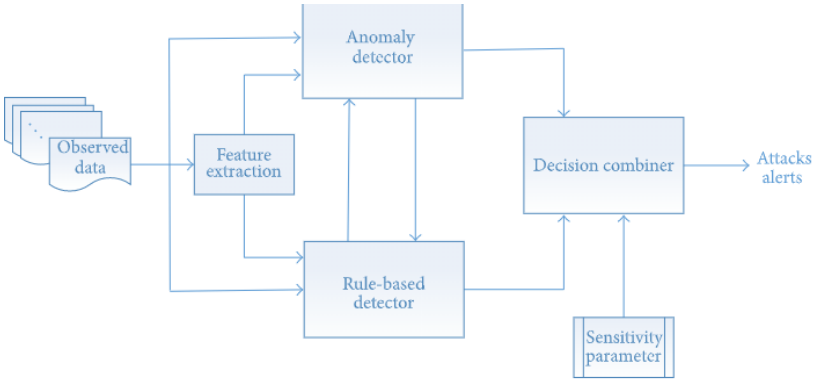
In this function we will be managing all the incoming data packets in advanced scanning process considering few pre-defined variables and our ML algorithm. There are three main modules in this function and those functions methodologies are described in following. We are introducing this method to utilize and communicate IoT devices and give customers an outstanding risk-free secured experience.



3 Figure 6.1.1: DDoS attack detection and enabling Secure connection

6.1.1 Attack detection Module

All incoming traffic will be going through this module for complete the scanning process of this function and this module contain Signature and Policy engine. DDoS attacks can be detected by examining of the network traffic changes. In study performed by Chonka et al. [4], by using the property of network self-similarity a model is developed to find out DDoS flooding attack traffic. The parameters of the detectors are controlled by a centralized node. The design goal of this intrusion detection system is to enhance the overall performance of DDoS attack detection, by shortening the detection delay, while increasing the detection accuracy and seed of the network communication. The block diagram is show in figure 8.1.1. As in the figure the data containing normal traffic and DDoS attacks is processed some features and then the data linked to signature-based detector blocks to detect attacks.



4 Figure 6.1.2: Proposed model of IDS for signature-based attack detection

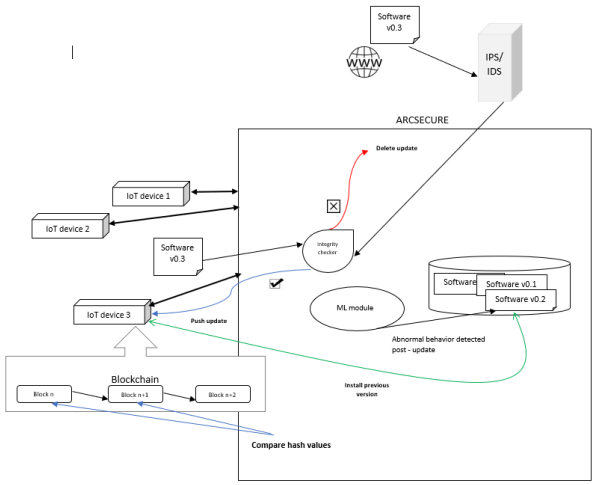
6.1.2 Data Training Module

In this module we a purposed to train the machine using data which have been gathered for training purpose and the second approach is to test the captured data. Well trained ML algorithm will clearly classify the abnormal patterns from normal data packets. It will easily identify any anomalies inside the IoT environment.

6.1.3 Mitigation Module

This will be the final module in the framework and all incoming network traffic will also be going through here for IoT devices [13] or if the purposed system will be able to detect any anomalies the packets are dropped in this stage as well.

6.2 Update automation module



5 Figure 6.2.1: Overall system diagram of update automation module

As the high-level diagram itself presents the hub that will be presented as the final product will be connected as an intermediary between the IoT devices and the IDS/IPS. In this case, as the specific objectives suggest under the main objective of:

1) Automating and optimizing the process of updating of devices
2) Establishing an update verification mechanism
3) Establishing a rollback mechanism in case of detecting system instability

6.2.1 Automating and optimizing the process of updating devices

Basically, every device within the network will be receiving updates from time to time. But these files received are not being checked for legitimacy.

A file received on the device might be a fabricated by an attacker which might contain a malware code. In this case once the file has been received by the device, the system will cross-check the file's has value against the device's official site's update file using an integrity checker. Initially the device's auto update option will be disabled, and it will only enable the auto-update feature if the two values are the same. If not, the file will be considered as corrupted and will be deleted from the device.

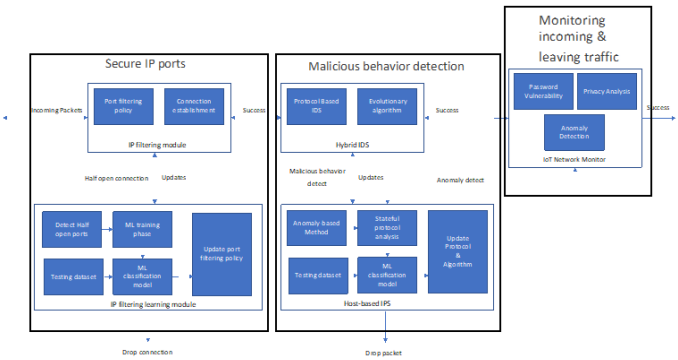
6.2.2 Establishing an update verification mechanism

Using blockchain, the block's hash value of the particular device will be always maintained before an update. And another block will be maintained for the device post-update. Post-update block's hash value and the pre-update hash value will be checked against each other to check if the update has been done successfully with the use of blockchain.

6.2.3 Establishing a rollback mechanism in case of detecting system instability

In this case, the system will be trained by using machine learning algorithms to detect any deviation [11] in the device from its normal behavior. For this purpose, a supervised machine learning approach will be used such as Naïve Bayes to make sure that a less false positives are generated. This will be the data training module of this particular section. Data sets will be fed into the module and will be trained over time in order to achieve this. If the system detects any deviation within the network post-update from a device, it will reinstall the previous software version file into the device. For this purpose, the system will at all times hold the previous software version file of the device an reinstall it if system reaches an unstable phase.

6.3 Botnet prevention module



6*Figure 6.3.1: Overall system diagram of Botnet prevention system*

As illustrated in the high-level diagram incoming packets passes through three modules.

- IP filtering module
- Hybrid IDS and Host based IPS
- Network monitoring module

6.3.1 IP filtering module

IP filtering module main objective is identifying incoming IP address and establish connection. When identifying process, it checks port address incoming connections trying to reach. Botnet trying to establish connections through TCP ports 23 or 2323

6.3.2 Hybrid IDS and Host based IPS

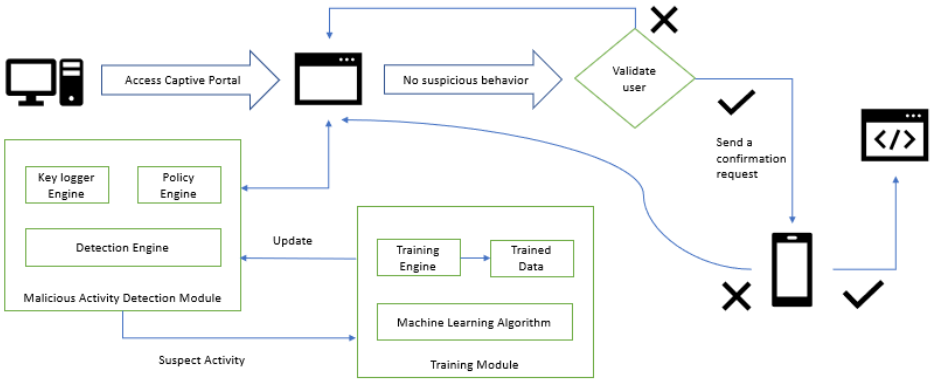
In this module system detects malicious behaviors of the packets. This module captures the incoming pcap file and analyze it with the protocol based IDS. Protocol based IDS used to monitor and analyze the protocol (rather than the profile of normal activity it has built) used by that system. The advantage here is that protocols are relatively well-defined (in comparison to "normal activity" profiles), so normal use cases can be created with greater accuracy.

6.3.3 Network monitoring module

This module include user friendly that integrates with an ARC secure. Network monitor captures packets as PCAP files [14]. Then runs a variety of scripts to parse and analyze the latest PCAP files. It looks for vulnerabilities in three categories [5]

6.4 User authentication module

This section will explore the expected approach that will be taken to arrive at our final goal which is ultimately ensuring that a user authenticating via the ARCSECURE plug and play portable device gains secure access to their IoT network devices.



7 Figure 6.4.1: Overall system diagram of user authentication system

As the above diagram interprets a user trying to gain access to the IoT network would first be greeted with a captive portal [12] where he/she would be required to enter their user credentials. Since this is a SSO feature a user who is successfully granted access to the network would have complete access to all devices at once. This is a critical issue as it can lead to a single point of failure. To overcome this issue a simple user credential validation will not suffice. To raise the level of security a notch MFA will be used. The first section of this MFA process utilizes keystroke dynamics and the other utilizing a combination of biometrics and token-based authentication.

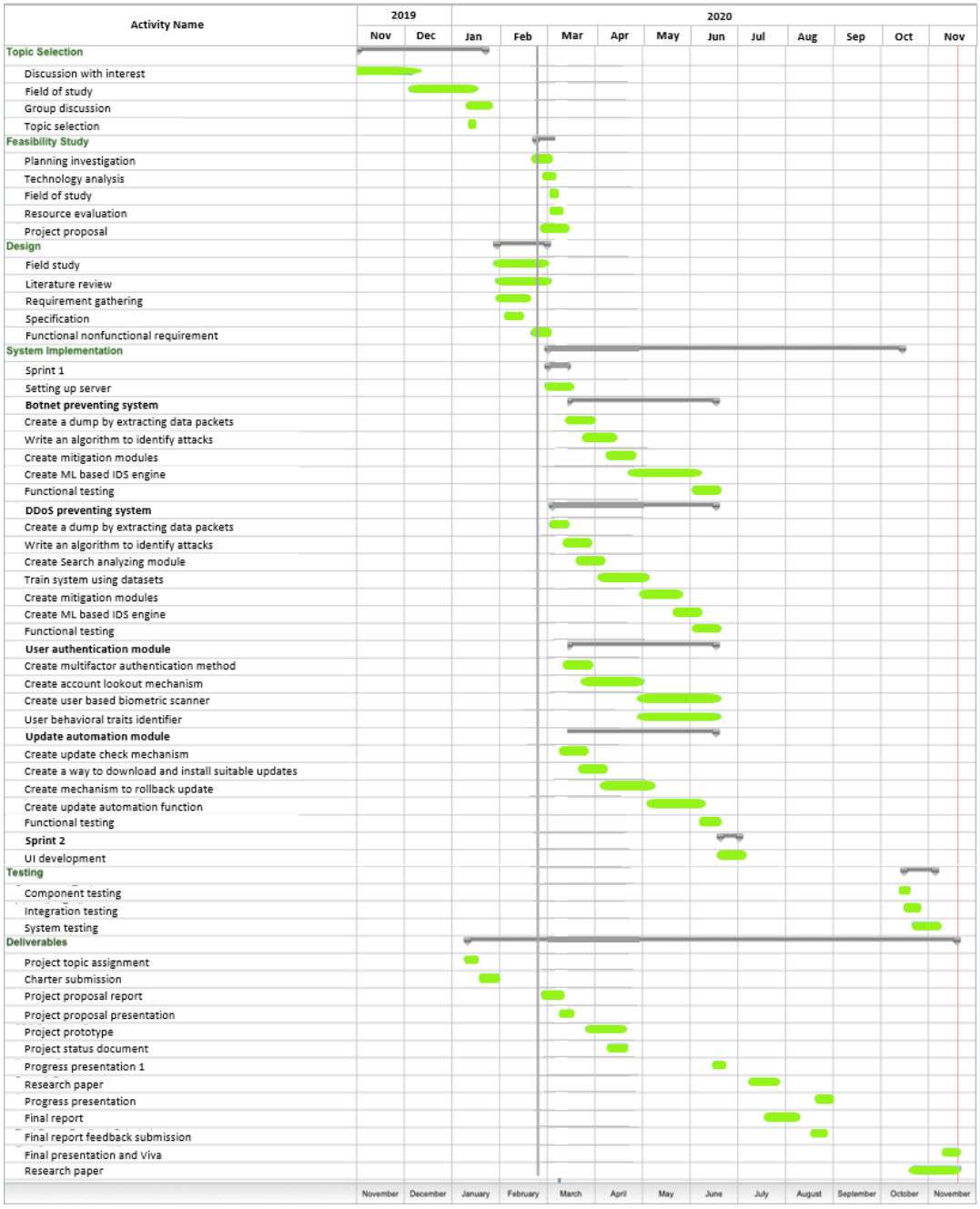
6.4.1 Keystroke Dynamics for Authentication

The user will be required to type in some text for the machine learning algorithm to figure out if the typing pattern matches with the initial pattern it learned from the user. The distinctive, behavioral characteristics measured by Keystroke Recognition include the subsequent variables [10].

6.4.2 MFA Process

As part of the MFA process, the user upon successful validation of user credentials will have to accept a simple Yes/No response which will be sent to a specially made app in the user's mobile phone. The app upon opening will request the user to authenticate to the app using a fingerprint scanner. Once validated he/she can confirm the Yes/No request sent to the specific mobile app. The user will now be able to access the IoT network based on their authorization [9] right that the user is granted

6.5 Gantt Chart



8 Figure 6.4.1: Gantt Chart

7 DESCRIPTION OF PERSONAL AND FACILITES

The workload of this research is assigned to a group of four members where each member has an equal workload to complete

7.1 Botnet prevention module – A.M.I.S Abeykoon – IT17009614

- Requirements Gathering
- Create a dump using network packets.
- Creation of a Machine Learning detection engine.
- Develop an Intrusion detection system.

7.2 DDoS attack detection and enable secure communication. A.M.S.P.B Atapattu – IT17127356

- Requirements Gathering
- Extraction of packet data which passes through the network create a dump.
- Creation of a Machine Learning Based Intrusion Detection Engine.
- Creation of local Database to store the Intrusions that are identified.
- Develop an Intrusion detection alarming system.
- Using Blockchain technology to enable secure communication between IoT devices

7.3 Update automation module - H.N Jayawardhane - IT17078306

- Requirements Gathering
- Create update check mechanism
- Create a way to download and install suitable updates
- Create a mechanism to rollback updates
- Create update automation function

7.4 User authentication module – C.N Samarasekara - IT17126816

- Requirements Gathering
- Create multi factor authentication method
- Create account lookout mechanism
- Creation of user-based bio metric scanner
- Create user behavioural traits identifier.

8 BUSINESS PLAN

Potential competitors include Azure, Bosch, Bitdefender Box

Expected Marketing Plan

1. To provide a limited trial version.
2. To provide a permanent purchase option
    - No restriction on the number of devices.
    - A fee upfront for the device.
    - A monthly subscription fee.
    - No termination fee for an in-between termination.

9 BUDGET AND JUSTIFICATION

9.1 Estimated budget for the networking Devices.

Device	Price	Quantity	Total Amount
Raspberry PI	Rs. 16000.00	1	Rs. 16000.00
IoT products	Rs 4000.00	2	Rs. 04000.00
Ethernet Cables	Rs. 500.00	1	Rs. 00500.00
Total Cost			Rs. 20500.00

Table 1 Estimated Budget

9.2 Estimated Budget for other expenses.

Items	**Price**	**Total Amount**
Stationary	Rs. 2500.00	Rs. 2500.00
Printing	Rs. 2000.00	Rs. 2000.00
Other	Rs. 2000.00	Rs. 2000.00
Total Cost		Rs. 6500.00

Table 2: Estimated Budget for other expenses

9.3 Total Expenses

Description	**Estimated costs**
Estimated budget for the networking Devices	Rs. 20500.00
Estimated Budget for other expenses	Rs. 06500.00
Total estimated cost for the year	Rs. 27000.00

Table 3 Total Expenses

10 REFERENCE

[1] MooseFS, "moosefs.com," MooseFS, 03 2019. [Online]. Available: https://moosefs.com/. [Accessed 20 Feb 2020].

[2] T. M. E. K. L. Chandramohan A. Thekkath, "Frangipani: A Scalable Distributed File System," Systems Research Center, Digital Equipment Corporation , 130 Lytton Ave, Palo Alto, CA 94301, 1997.

[3] K. . Shvachko, H. . Kuang, S. . Radia and R. . Chansler, "The Hadoop Distributed File System," , 2010. [Online]. Available: https://cs.uwaterloo.ca/~david/cs848s13/alex-presentation.pdf. [Accessed 20 Feb 2020].

[4] S. . Ghemawat, H. . Gobioff and S.-T. . Leung, "The Google File System," *Operating Systems Review*, vol. 37, no. 5, p. , 2003.

[5] G. Jonsdottir, D. Wood and R. Doshi, "IoT network monitor," 2017 IEEE MIT Undergraduate Research Technology Conference (URTC), Cambridge, MA, 2017, pp. 1-5. [Accessed 22 02 2020].

[6] Yu, E., Cho, S. Ga-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification. In: Neural Networks, 2003. Proceedings of the International Joint Conference on; vol. 3. IEEE; 2003, p. 2253–2257.

[7] Revett, K., Gorunescu, F., Gorunescu, M., Ene, M., Magalhaes, S., Santos, H.. A machine learning approach to keystroke dynamics-based user authentication. International Journal of Electronic Security and Digital Forensics 2007;1(1):55–70.

[8] Zahid, S., Shahzad, M., Khayam, S.A., Farooq, M.. Keystroke-based user identification on smartphones. In: International Workshop on Recent Advances in Intrusion Detection. Springer; 2009, p. 224–243.

[9] Epp, C., Lippold, M., Mandryk, R.L. Identifying emotional states using keystroke dynamics. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM; 2011, p. 715–724.

[10] Ali, M.L., Monaco, J.V., Tappert, C.C., Qiu, M.. Keystroke biometric systems for user authentication. JournalofSignalProcessingSystems 2017;86(2-3):175–190.

[11] S. Shaju, "BISC Authentication Algorithm : An Efficient New Authentication Algorithm Using Three Factor Authentication for Mobile Banking," 2016.

[12] P. Mahalle, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things," J. Cyber …, vol. 1, pp. 309–348, 2013.

[13] D. Chen et al., "S2M: A Lightweight Acoustic FingerprintsBased Wireless Device Authentication Protocol," IEEE Internet Things J., vol. 4, no. 1, pp. 88–100, 2017.

[14] Kim, S., Smyth, P., Luther S.: Modeling waveform shapes with random effects segmental Hidden Markov Models. In Proceedings of the 20th Conference on Uncertainty in Artificial Intelligence, 309–316 (2004)

11 APPENDICES

11.1 Work Breakdown Structure