A Security Framework for a Sustainable Smart Home Ecosystem using Permissioned Blockchain

[1]George Gabriel Richard Roy, [2]S. Britto Ramesh Kumar
[1]Assistant Professor, [2] Assistant Professor
[1]Department of Information Technology, [2] Department of Computer Science
[1] St. Joseph's College (Autonomous), Tiruchirappalli, India

Abstract: Studies have been made on the automation of tasks in an around a normal household. These are tasks which would usually take a long time to complete or which is daunting at hand. Studies which contribute towards automation of these tasks is called Home Automation. Home Automation goes hand in hand with the term Smart Home. Smart Homes are houses that are capable of highly advanced automated systems that enables control and monitoring the task of comfort or necessity either with the interaction of the user or without. With the sophistication of Smart Homes or Domotics there is a heavy implication on the technology which is used leads to more threats and risks. A Smart Home empowers users in various means, it also puts power into the hands of the people with malicious intent. Thus there are huge security risks associated with the implementation of Home Automation. This paper proposes a security framework to protect the Smart Homes from such attacks using internal IoT Security algorithms and Permissioned Blockchains. The framework has been penetration tested by Colasoft Caspa, Metasploit and benchmarked using Gauge for Permissioned Blockchains.

***IndexTerms* – Blockchain, Multi-chain, IoT, Smart Home, Ecosystem, Security, Blake2b, Domotics.**

I. Introduction

Smart Homes (SH) are houses which have state of the art systems which are used for automating different tasks in an around the premises. They have advanced system to check the status of the automation systems and also to control the actions of those systems. There are many types of tasks that can be automated in a SH controlling and monitoring the lighting, multi-media devices, temperature, physical security systems, gardens, surveillance, appliances, groceries etc., all of this in the comfort of the user. This control and monitoring is possible in premises or remotely with the help of wireless communication and computerization. The devices and components within a SH is said to be "Smart" because they can are connected to all the devices and appliances in the premises and they communicate to the user as well as they communicate within themselves [1, 2].

Any appliance or device which is able to power on and function on electricity can be converted into a smart device in the SH network. The devices on the network can be controlled by smartphones, computers, tablets, voice or remotes. They also can function without the intervention of the user depending on the pre-programmed functions the devices are tasked to do [3, 4].

SHs were once considered a luxury or something only possible in Sci-Fi movies where only wealthy people could afford something of this proportion, now has become common among households due to the rise of uber-portable microcomputers and Single Board Computers (SBC), these devices have the capability of connecting to the Internet and thereby making it possible to connect to other devices on the Internet too.

This is possible with Internet of Things (IoT) where Smart Appliances, Devices, SBCs, and other Things can be connected to a network through the Internet where each device is capable of communicating with each other and moreover they are uniquely identifiable, this technical revolution is the driving force of SHs. IoT enables devices and things to be connected with each other for information gathering, performing actions on the information which is collected and also used to analyze the collected data [8]. IoT enables or provides a whole new opportunity to save time, money and other nuances. Services such as electricity, cooking gas, supermarkets, banks, etc. can interact with SHs to innovatively and automatically deliver services, products and goods. IoT takes context awareness to another level where the potential it has is limitless [11, 12].

With great power comes greater threats to be handled, IoT has a fair share of threats that plague its existence. There are many issues pertaining to the effective functionality of IoT. Out of all challenges, security plays a vital role in the productivity of the network.

Cyberattacks on IoT and its related problems are considered as high priority and prominence. A Smart Home is an IoT network which has its fair share of vulnerabilities due to the complex nature of connections between devices. Smart Homes are designed to aid the user and not bring more problems, especially when the user is not tech savvy it would be hard to protect them from the adversaries. Attacks such as Distributed Denial of Service (DDOS), Replay Attacks, Brute Force attacks, Eavesdropping, Man in the Middle (MITM) attacks are some of the few attacks which plague the Smart Home Ecosystem [10].

Blockchain which was initially designed to be the backbone of cryptocurrency, the append-only distributed ledger system has proved to have more than what meets the eye. It has many uses in providing confidentiality of data, protecting the identity of the users and providing privacy of the information which transacted through the network. This would be provide the required functionality to provide security to the Smart Home. There are different types of Blockchains public, private, permissioned and permissionless, out of which a private and permissioned Blockchain has good security tolerance and would be much easier to govern the communications which happens in the Blockchain [9].

This paper proposes a Framework to create a Secure Sustainable Smart Home ecosystem using the distributed ledger technology of permissioned Blockchains.

This paper is organized as I – Introduction, II – Literature Review, III – Proposed Framework, IV – Experimental Study and Security Analysis, and V – Conclusion and Future Direction.

II. Literature Review

Tam et al. has proposed in their paper that Cloud based Smart Homes are ever present with a threat from adversarial activities. They have propagated a RES-Hub device to make sure that the services rendered to the smart home will not be susceptible to damage even if any adversary tries to tamper with it when there is no connection to the cloud. They have integrated OAuth 2.0 authentication and authorization framework to assure that the user will always have their home protected with secure access and secure control of their homes from adversaries. They have also discussed the probable outcomes of the unavailability of cloud services thereby affecting the functionality of the smart home and how secure would that home be without the cloud services. They have also listed types of essential services within a Smart Home like User Connectivity, Health Care, Security, Local Storage and Local Automation [5].

Fadi et al. stated in their paper that Smart grid networks enhances many aspects when compared to conventional networks but they do bring complexity and makes it more susceptible to different type of attacks. There go further and explain those types of attack which allows attackers access to Smart grid network. The vulnerabilities which were discussed are Customer Security, increased number of intelligent devices, threats to physical security, the overall lifetime of the system, the trust between devices and the inclusion of several stakeholders into the grid. The vulnerabilities could be exploited by the adversaries in various proportions causing damage to the grid in different levels. Distributed Denial of Service (DDOS) attacks were said to be the most predominant attack which disturbs the whole functionality of the network. Added to this, attacks such as Malware spreading, database link attacks, communication equipment composability, replay attacks and eavesdropping enter the fray. They have mentioned a few workarounds for these attacks such as including robust protocols, constant updating and upgradation of equipment and not using vendor specific devices [7].

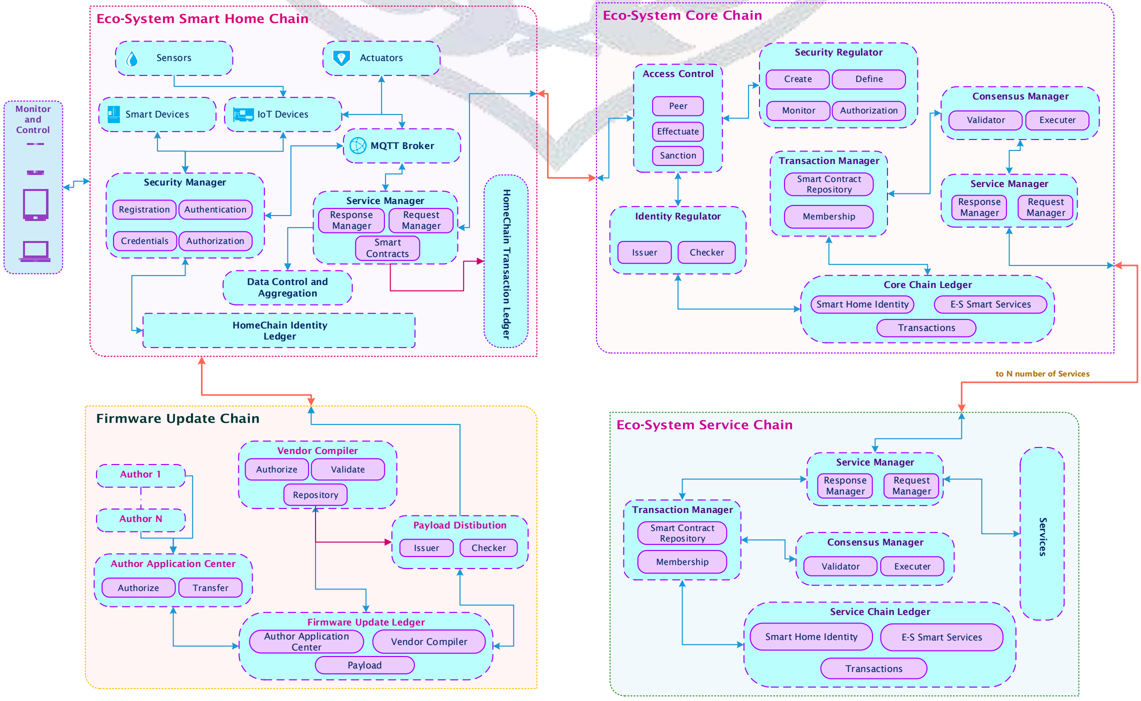
Tommaso et al. mentioned that as Smart Homes ups the antics with smarter devices the more it becomes susceptible to cyberattacks. They have mentioned that many attacks have been performed on toys for mistakes configuration, and other small devices were attacked targeting its vulnerabilities. The increase in the number of devices makes the Smart Home a haven for malicious attacker who target vulnerabilities to perform DDoS attacks, not only compromising the integrity of the network by also the safety of the user. Many people have accessed such devices with malicious intent with freely available tools on the Internet. They stated that security measures that were traditionally used will not be enough to protect the network because of the difficulty in deciding for the setup or either they were too weak. They have proposed a dynamic method to provide security to the IoT Networks by network sentiment analysis using Intrusion Detection Systems [6].

From the literature it is evident that there is an urgent need to protect IoT networks and users from people with malicious intent to hijack the devices and the information of the Smart Home users. Therefore A security framework is designed to protect a sustainable Smart Home Ecosystem with permissioned Blockchain technology.

III. Proposed Framework

The proposed framework is divided into four major divisions (Fig. 1), each division has a complex amount of work going on. The major divisions can be named as follows:

Figure 1: Proposed Security Framework for a Sustainable Smart Ecosystem



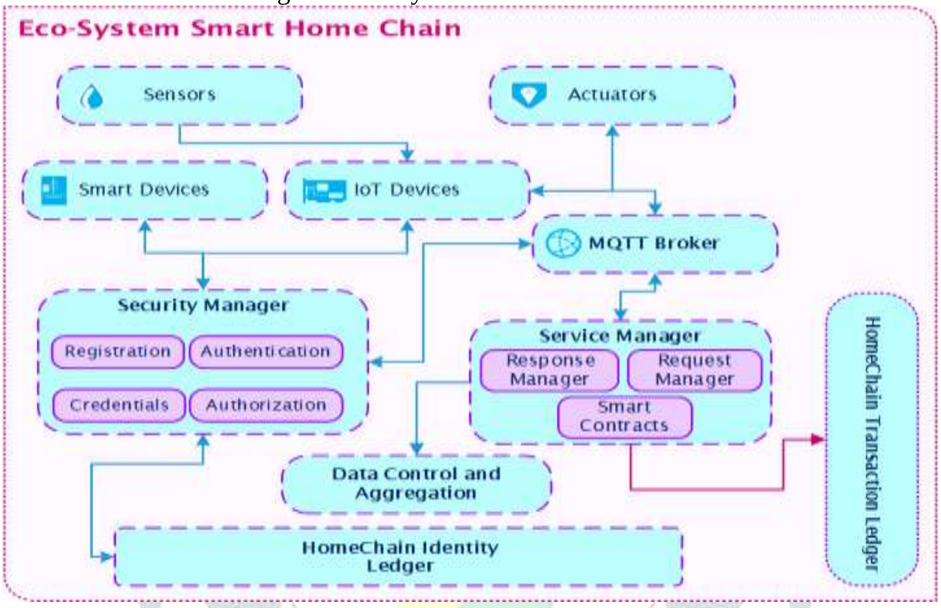
- Ecosystem Home Chain (ESHC)
- Ecosystem Core Chain (ESCC)
- Ecosystem Service Chain (ESSC)
- Ecosystem Firmware Update Chain (ESFC)

This proposed system follows a multichain model, where there are multiple blockchains communicating with each other to form a whole system. The individual chains are detailed as below:

3.1 Ecosystem Home Chain (ESHC)

The ESHC (Fig. 2) is the Smart Home which comprises of the user equipment. There can be n number of ESHCs in the network where every n+1 ESHC will be added to the ESCC if permissioned. The ESHC is responsible to make requests to the services available in the suitable ESSC. The ESHC as a standalone system has many operations which are taking place inside, moreover it has many components which work in accord to provide secure Home Automation to the user.

Figure 2: Ecosystem Smart Home Chain



The components of ESHC are as follows:

3.1.1 Sensors

A Sensor is an electronic input device which specializes in providing a dedicated output based on the type of the signals it receives as input. A sensor is the basic building block of every automated household. It is responsible to sense the surrounding for any changes which are programmed for it to capture and sends an output signal to where it is programmed to do so. The Sensors are connected to the IoT Devices which governs the transmission of data to either actuate or to further send requests for services.

3.1.2 Actuators

An Actuator is a mechanical or an electro-mechanical device that can provide limited and controlled movements based on the input given to it. Actuators are mostly classified into output devices due to their nature but some actuators can act as input furthermore to other devices and other actuators. In ESHC the actuators acquire input from the sensor through the IoT devices.

3.1.3 IoT Devices

The Sensors and Actuators are not capable of transferring or receiving data on their own unless they are special dedicated smart sensors. To enable transfer of data and to enable communication between sensors and other devices in the smart home they need to be connected to IoT Devices. These IoT Devices are development boards, and other special purpose boards which can act as a mediator between the sensors, actuators, smart sensors and other devices. They can connect to the Internet to send requests and receive responses. They are responsible for holding a replica of the Identity Ledger which stores information of the devices in append only mode and Smart Contracts to transact with the other peers.

3.1.4 Smart Devices (SD)

Smart Devices do not need any external IoT device to connect or communicate within other devices. It is solely capable of transmitting and receiving, sending requests and receiving responses from services. There are many SDs in an ESHC such as

Smart Refrigerator, Smart Washing Machine, Smart Television, Smart Microwave oven etc., These SDs are responsible to send requests to various services available in the ESSC. These requests and responses can be handled by Smart Contracts with little to no intervention from the user.

3.1.5 MQTT Broker

To enable Lightweight and bandwidth efficient data transfer and communication between IoT devices MQTT Brokers (MQB) are used. In this case of ESHC the sensors and sometimes even actuators act as publishers that publishes its current state to the subscribers that are currently subscribed to the topic to which the sensor publishes. It is the job of the MQB to handle the plethora of connected MQTT clients. The MQB has the job to receive messages, filter them, send appropriate messages to the right subscriber. The MQTT Clients always connect to the MQB to send messages and this is the most exposed component which handles all requests and responses.

3.1.6 Service Manager

The Service manager is a part of the MQB which is used to segregate the requests from the responses and store them accordingly or to send requests respectively. The information that is needed to be stored is done by the Data Control and Aggregator (DCA) which gets its information from the Service Manager.

3.1.7 Security Manager (SqM)

The heart of security of the ESHC is the Security Manager (SqM). The SqM is responsible to Register new devices, apply credentials to the devices based on what those devices can access, authorize devices and authenticate them. The SqM has a direct link to the Home Chain Identity Ledger where all the information of the SqM is stored and is used later for authentication.

3.1.8 Data Control and Aggregator (DCA)

The purpose of the DCA is to collect data collected from the IoT Devices and the SDs which can be used later for statistical analysis. This is done to in order to enhance the overall efficiency of the network by aggregating data packets, to study about power consumption and to find any congestion in traffic to increase the accuracy of the network along with its accuracy in providing the necessary services. The DCA is also used to keep track of the alive status of the nodes in the network.

3.1.9 Home Chain Identity Ledger (HCIL)

The HCIL is an append only ledger which utilizes a modified Practical Byzantine Fault Tolerance (mPBFT) consensus to write blocks on to the ledger. The SqM behaves as an ordering service node using the mPBFT by Kafka ordering, the nodes communicate with each other and the blocks get written finalizing the transaction. The replicas of the HCIL is placed in all participating peers which would be pre-selected IoT devices and SDs.

3.1.10 Home Chain Transaction Ledger (HCTL)

With the ESHC acting as one of the Validating Peers (VP) the transactions that the ESHC does for e.g. Sending requests, receiving responses, publishing data etc., are sent to a trusted VP on the network which could be another ESHC Smart Home. This VP transmits the transaction as a broadcast to all the participating VPs which are governed by the ESCC. The participating VPs arrive to a consensus to execute the transaction and the HCTL gets updated with a block written with the latest transaction. A replica of the HCTL will be stored in every participating VP and will be synced.

3.2 Ecosystem Core Chain (ESCC)

The ESCC (Fig. 3) is a Permissioned Blockchain network that allows the network to permit a cluster of participating nodes in the network who have prearranged authority to behave as VPs to validate blocks of transactions or to be a part of the consensus

The components of ESCC are as follows:

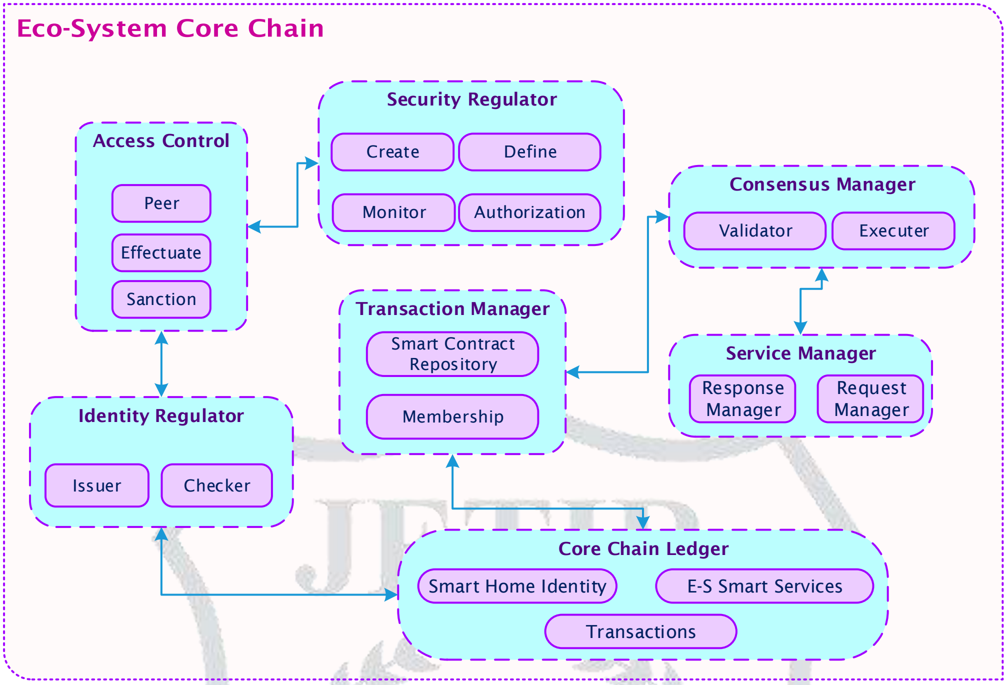
3.2.1 Security Regulator (CCSR)

The SR is responsible for adding permissions to peers on the network, this is the first module that is invoked when a network is created. SR is used to create, define, monitor and authorize the members of the network. It also behaves as the manager of identity of the members in the network. This module is the one that provides access control to the members.

3.2.2 Access Control (CCAC)

In the access control the members are split into three different categories. The members here are called Peers, they are the basic element of every Blockchain network, smart contracts and ledgers are stored in Peers. Special nodes called Orderers ensure that the ledgers which are in the peers are intact and they are responsible to keep them consistent. Sanctioners are special peers who can endorse a transaction before it reaches its committed state. Every Smart Contract will have several peers associated with it for a transaction to be effectuated in the endorsement policy. Effectuators are peers who can commit the transaction. The Effectuator has performs several checks to consensus process based on the endorsement policy if successful then the Effectuator will commit the transaction.

Figure 3: Ecosystem Core Chain



3.2.3 Transaction Manager (CCTM)

The Transaction manager is responsible to manage the transactions that happens across the multichain. It holds the Smart Contract Repository (SCR) where all the Smart Contracts are stored and appropriate action is taken according to the transaction. Every participating peer who wants to take part in a transaction has a Smart Contract which is taken from the SCR by proving that the peer is a member by checking the membership details stored in the Core Chain Ledger that can access the Smart Contract. A Smart Contract is responsible to initiate the transaction proposal to the peers. The Sanctioner receives the transaction proposal from the submitting peer, produces the desired results based on the smart contract, and transmits the results to the Orderers. It is the duty of the TM to validate the transaction proposal using the Sanctioner, and commit the transaction block to the Core Chain Ledger. The Order sends the completed block to all the participating peers.

3.2.4 Consensus Manager (CCCM)

The general agreement of all the participating nodes in the network come under a protocol called a consensus. The CM is used to implement the algorithm for consensual agreement among the peers. The Ordering node validates the transaction using the Validator to create a block on the participating peers. After ensuring the fulfillment of the endorsement policy by the peers, the block of transactions are committed by the Executer to the Blockchain.

3.2.5 Identity Regulator (CCIR)

The Identity Regulator is used to authenticate and authorize the members of the Blockchain with reference to the information that is stored in the Core Chain Ledger.

3.2.6 Service Manager (CCSM)

The Service manager is responsible to send the transactions from the ESCH to the required ESSC based on the transaction and the Smart Contract that is invoked by the participating peers. The Service manage handles the requests and responses and aids to the CM and TM accordingly to complete the terms of the Smart Contract thereby committing the block.

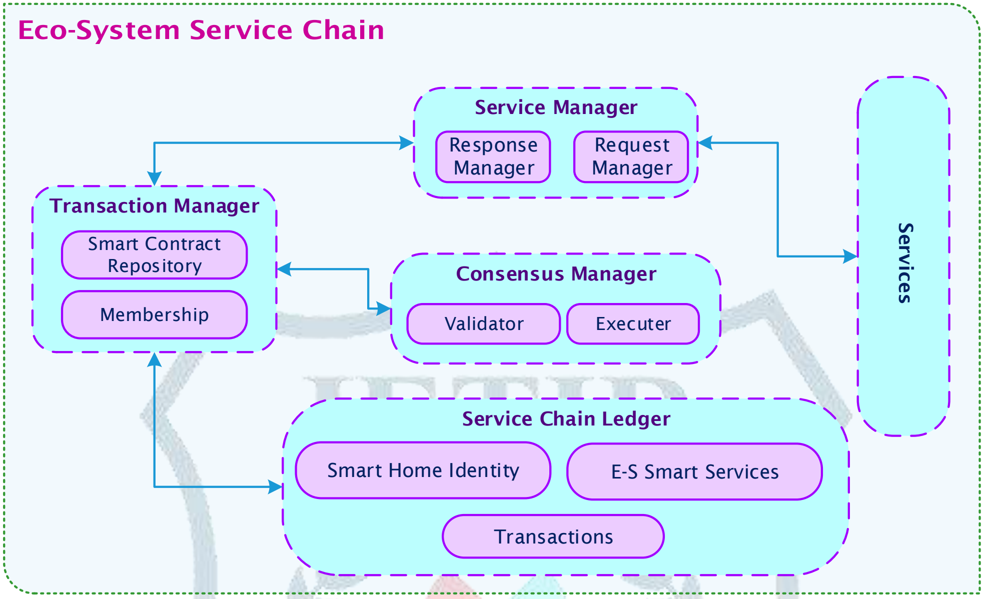
3.2.7 Core Chain Ledger (CCL)

The CCL houses a Smart Home Identity Ledger (SHIL), a Transaction Ledger (TL), and a Service Identity Ledger (SIL). Each ledger has its own purpose and all ledgers do not have the same information stored into them. The SHIL contains the n number of ESHCs where the membership details are stored along with access control privileges provided through the Identity Regulator. These ESHCs are taken into account as Smart Home Nodes and they can be participating nodes in the transactions they propose. The SIL houses all the available Smart Services that are permitted and registered to the Ecosystem, as mentioned earlier the Smart Home Nodes can only avail services of permitted and registered services which is available in the CCL and the HCTL. The TL consists of all the transaction blocks which takes place in the ecosystem. A replica of the transaction block pertaining to a participating node is synced only with the participating node and not all nodes.

3.3 Ecosystem Service Chain (ESSC)

Smart Homes in the Ecosystem can avail many Smart Services albeit should be a registered service acknowledged by the Core Chain governance. Services could be anything like Supermarkets, Smart Electricity, Smart Cooking Gas provider, Logistics, Banking etc., these services each have a dedicated Ecosystem Service Chain of their own and they have specific members who have registered to the services. It is not mandatory that all ESHC Smart Homes should be registered to all ESSCs. Only participating and registered nodes will be able to enjoy the services provided by the Smart Services. The ESSC (Fig. 3) is a Sidechain which is used to reduce the burden by distributing the service aspect of the ESCC.

Figure 3: Ecosystem Service Chain



The components of ESSC are as follows:

3.3.1 Transaction Manager (SCTM)

The SCTM functions in a similar way like the CCTM. The Smart Contract request from the ESCC goes to the Service manager where the service manager checks the Service Chain Ledger for the credentials based on the provided credentials if present the necessary service is provided to the requester to finalize the contract.

3.3.2 Consensus Manager (SCCM)

The consensus depends on which nodes are permitted, in a permissioned network only selected predefined permitted nodes are allowed to participate in the consensus depending on the membership they hold in the access control provided by the Blockchain governance. The SCCM is validates the transaction based on the availability of the Smart Contract in the repository which matches that of the request which is made. When the conditions are satisfied the Executer commits the transaction and sends it to the service manager.

3.3.3 Service Manager (SCSM)

The SCSM receives the request from the CCSM which is sent to the SCTM where the request is processed and the necessary service is provided when the SCCM commits the transaction thereby responding with the required service back to the CCSM.

3.3.4 Services

Every ESSC has Smart Services which are unique to that chain. There are several services that a Smart Home can avail but the Smart Home should be registered in the ESSC to avail them.

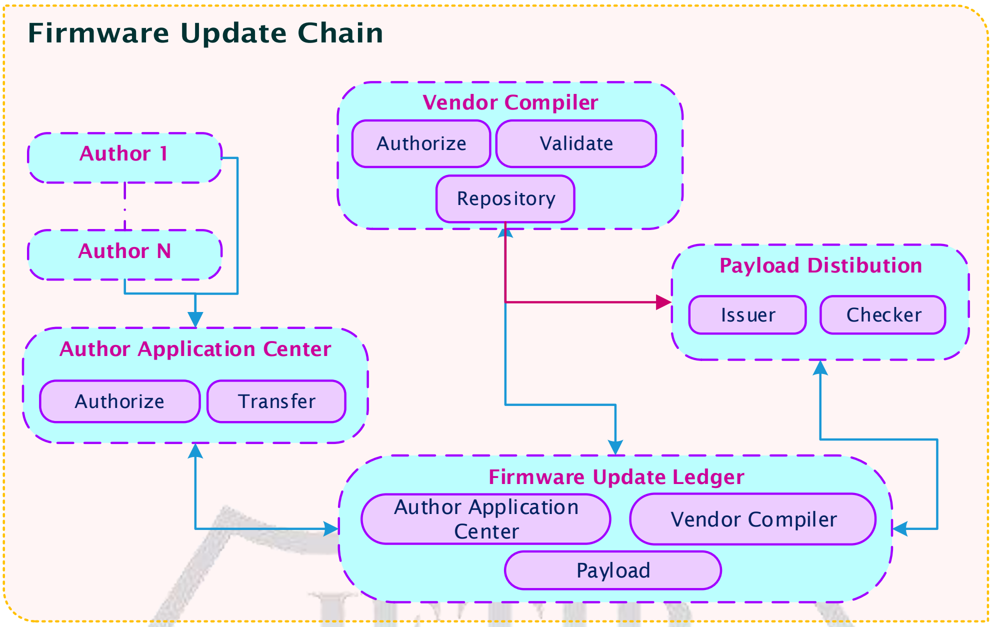
3.3.5 Service Chain Ledger (SCL)

The SCL houses a different Smart Home Identity Ledger (SHIL), a Transaction Ledger (TL), and a Service Identity Ledger (SIL) than the CCL. Each ledger is different because the amount of transactions processed will be only the ones unique to that particular Smart Service. The SHIL contains the n number of ESHCs who are registered with that specific Smart Service, Each ESSC may have different numbers of registered ESHCs. The TL consists of all the transaction blocks which takes place between the Smart Home and the Smart Service. A replica of the transaction block pertaining to a participating node is synced with the CCL, and permitted participating nodes.

3.4 Ecosystem Firmware Update Chain (ESFC)

A Firmware is a software which is written to the deepest system level which is used to control the functionality of the hardware device that it is written on. Attacker who desire to change devices into bots and thereby create botnets usually target the devices which has outdated firmware so loopholes could be exploited. It is always advisable to update the firmware and it should be done in a secure way. The ESFC proposes a secure methodology to update firmware on IoT Devices. Fig. 4.

Figure 4: Ecosystem Firmware Update Chain



The components of ESFC are as follows:

3.4.1 Author

Hardware device vendors are the default authors of Firmware for their devices, but there are many instances where the Author of the firmware could be outsourced to third parties. These Authors can develop the firmware and send it to the Author Application Center to be authorized and then transferred to the vendor Distributor to be checked for. When

3.4.2 Author Application Center (AAC)

The AAC is in control of all the submissions of the firmware submitted by the Authors, the AAC authorizes the firmware manifest after authenticating the submission of the author from the Firmware update Ledger. The Manifest is then updated and sent to the Vendor Distributor to be verified for any anomalies.

3.4.3 Vendor Compiler (VC)

The VC can distribute standalone OEM firmware updates or can authorize firmware updates from third party authors. The VC is a permitted node which also acts as an ordering service node which can validate the firmware and update the manifest. The Details of the manifest is updated to the Firmware Update Ledger. The payload goes to the Payload distributor for further connection.

3.4.4 Payload Distributor (PD)

The PD checks the Firmware Update chain for the manifest if it matches the one from the Vendor Distributor, if it does it sends the payload to the ESHC to the appropriate device which is requesting for an OTA update, the PD Checks with the HIL and then transfers the payload to the respective IoT Devices to update them.

3.4.5 Firmware Update Ledger (FUL)

The FUL contains information about the identity of the Authors, AACs, VCs and the payload manifest. It is responsible for providing a backbone for authorizing and authenticating the secure transfer of the firmware from Author to Device.

IV. Experimental Study and Security Analysis

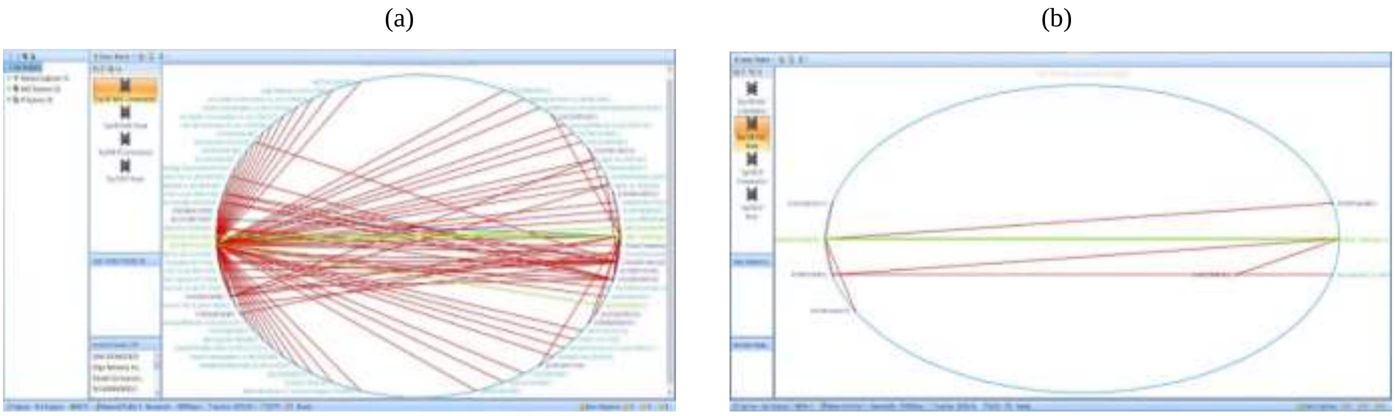
The security analysis of the proposed system is done using penetration testing and network analysis tools. Results are taken before and after security implementation to show the difference when the framework is secure from attacks.

The framework was tested for its vulnerability against DDoS attacks, where requests flood the system to an extent that it is not able to process anymore requests and stops functioning. Malicious attackers target small devices and coverts them to bots after hijacking them. These bots cluster up together to form botnets, the botnets are the major cause of service denial due to DDoS attacks.

Metasploit was used in Kali Linux to trigger DDoS attacks on a normal IoT network and on network using the proposed security framework. It was evident that the unsecure IoT Network suffered from massive MAC conversations between unknown sources and the IP conversations were always at peak load. In the case of the proposed framework the DDoS attack had no effect on the network since the attack did not even penetrate the network because it was not permissioned.

The screenshots Fig. 5 and Fig. 6 were taking on Colasoft Caspa a network analyzing tool.

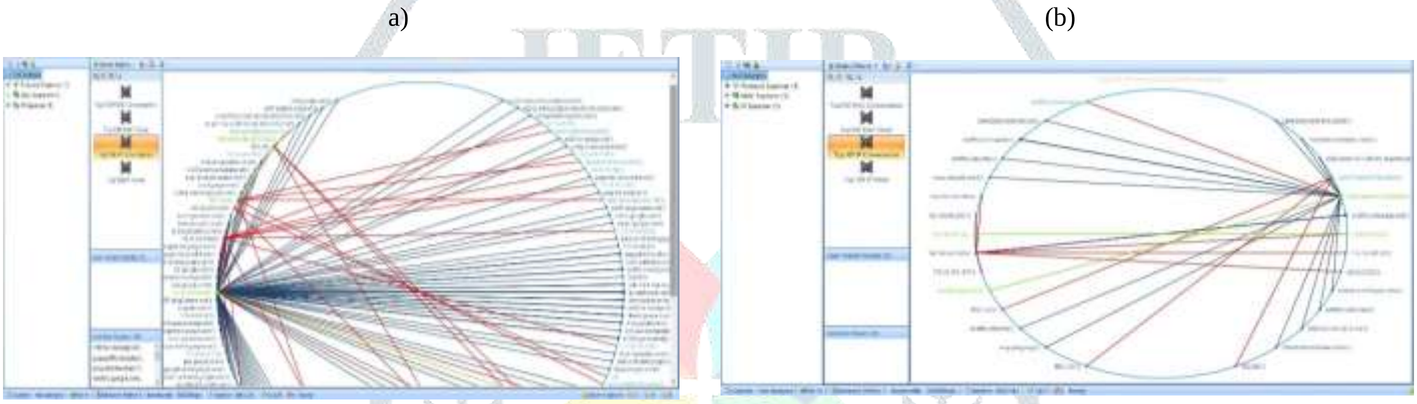
Figure 5: MAC Nodes on Insecure network (a), MAC Nodes on Proposed Framework (b)



(a)

(b)

Figure 6: IP conversations on insecure network (a), IP conversations on Proposed Framework (b)



a)

(b)

Syn flood was used to flood the insecure networks and by Fig. 5 (a) it is seen that there are many unwanted MAC conversations which cripple the network, but in the case of the network utilizing the poposed framework, the attack failed to take place because of its permissioned nature Fig. 5(b). Likewise the IP convorsations went erratic when the insecure network was attacked which lead to the network failure of unable to handle requests, but in the case of the proposed framework only IPs from registered sources were served Fig. 6(b).

V. Conclusion and Future Directions

In this paper a Secure Framework for a Smart Home Ecosystem is proposed using the distributed ledger technology of permissioned Blockchains. The idea is to provide security to the users and devices in a non-traditional way which is proven to be liable to attacks. The proposed system can be used by people who needs a safe sustainable environment where there is little to no intervention from the user. The secure framework also discusses a secure way to provide safe and prompt over the air updates to the devices. The framework was tested for vulnerabilities and it was found that it is more reliable than traditional IoT Networks.

As a future direction it is planned to include Intrusion Detection System to provide a dynamic approach of knowing the attacker and using Artificial Intelligence to adapt accordingly providing security to the Smart Home Ecosystem.

References

[1] Rosslin John Robles and Tai-hoon Kim, 2010. A Review on Security in Smart Home Development. International Journal of Advanced Science and Technology, 15(3): 13–22.

[2] Jean Pierre Nzabahimana. 2018. Analysis of Security and Privacy Challenges in Internet of Things. IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT, 175-178.

[3] Er. Pooja Yadav, Er. Ankur Mittal and Dr. Hemant Yadav. 2018. IoT: Challenges and Issues in Indian Perspective, IEEE.

[4] Bengt Ahlgren, Markus Hidell and Edith C.-H. Ngai, 2016. Internet of Things for Smart Cities: Interoperability and Open Data, IEEE Internet Computing, 52–56.

[5] Tam Thanh Doan, Reihaneh Safavi-Naini, Shuai Li, Sepideh Avizheh, Muni Venkateswarlu K., Philip W. L. Fong.2018. Towards a Resilient Smart Home. IoT S&P'2018, 15–21.

[6] Tommaso Pecorella, Laura Pierucci and Francesca Nizzi, 2018. "Network Sentiment" Framework to Improve Security and Privacy for Smart Home. Future Internet, 10(125).

[7] Fadi Aloul, A. R. Al-Ali, Rami Al-Dalky, Mamoun Al-Mardini and Wassim El-Hajj,2012. Smart Grid Security: Threats, Vulnerabilities and Solutions. International Journal of Smart Grid and Clean Energy, 1(1): 1-6.

[8] Bassam Al-Shargabi and Omar Sabri, 2017. Internet of Things: an Exploration Study of Opportunities and Challenges. ICEMIS2017, IEEE Xplore.

[9] Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo and Antonino Nocera.2017. Overcoming Limits of Blockchain for IoT Applications, ARES '17, (26).

[10] Jesus Pacheco, Salim Hariri**.** IoT Security Framework for Smart Cyber Infrastructures.2016. IEEE 1st International Workshops on Foundations and Applications of Self-* Systems, 242-247.

[11] Shafiq ur Rehman and Volker Gruhn, 2018. An Approach to Secure Smart Homes in Cyber-Physical Systems/Internet-of-Things, Fifth International Conference on Software Defined Systems (SDS), IEEE Xplore, 126-129.

[12] Vishwakarma, Pinki. (2018). A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation. International Conference on Smart City and Emerging Technology. 1-4.