HomeTec Software for Security Aspects of Smart Home Devices Based on IOT

Parth Rustagi[1]*, Rohit Sroa[2], Priyanshu Sinha[3], Ashish Sharma[4] and Sandeep Tayal[5],

[1]Department of Information Technology, Maharaja Agrasen Institute of Technology, Delhi, India,

[2]Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India,

[3]Departmnet of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India,

[4]Assistant Professor, Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India,

[5]Assistant Professor, Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India,

***Corresponding Author: Parth Rustagi** parthrustagi1@gmail.com

1. Abstract

As useful as it gets to connect devices to the internet to make life easier and more comfortable, it also opens the gates to various cyber threats. The connection of Smart Home devices to the internet makes them vulnerable to malicious hackers that infiltrate the system. Hackers can penetrate these systems and have full control over devices. This can lead to denial of service, data leakage, invasion of privacy, etc. Thus security is a major aspect of Smart home devices. However, many companies manufacturing these Smart Home devices have little to no security protocols in their devices. In the process of making the IoT devices cheaper, various cost-cutting is done on the security protocols in IoT devices. In some way, many manufactures of the devices don't even consider this as a factor to build upon. This leaves the devices vulnerable to attacks. Various authorities have worked upon to standardize the security aspects for the IoT and listed out guidelines for manufactures to follow, but many fail to abide by them. This paper introduces and talks about the various threats, various Security threats to Smart Home devices. It takes a deep dive into the solutions for the discussed threats. It also discusses their prevention. Lastly, it discusses various preventive measures and good practices to be incorporated to protect devices from any future attacks.

Keywords: *SQL Injection, Digital Certificate, Eavesdropping, Biometric Security, Botnets.*

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020

DOI: 10.5281/zenodo.4099720

2. Introduction

The number of Smart Home devices is on the rise. According to research, there would be about 25 billion devices connected to the internet by the end of 2020. Smart Home devices offer a wide range of opportunities for both the manufacturers and the consumers, it also poses major risks in terms of security. Smart Home devices have little to no security, which makes them an easy target by hackers. These attacks lead to data loss, invasion of privacy, loss of control, denial of service, etc. In this paper, we introduce our software HomeTec which undertakes various security aspects in Smart Home devices. Our software will explore each and every security aspects discussed below thoroughly and will help protect them from anonymous users and hackers. Our software's approach will help to detect the vulnerability in the devices has been discussed and a novel approach to protect the device from these vulnerabilities has also been explained in detail. The following aspects are discussed in the paper:

2.1 SQL Injection

SQL injection allows hackers to have unauthorized access to personal information such as passwords, credit card details, etc. Our software HomeTec will be integrated to help protect against these SQL injections. The different types of SQL injection techniques used and their resolution techniques have been discussed.

2.2 Digital Certificates

HomeTec will provide an approach that uses the issuing of Digital Certificates while data transmission in devices to protect from SQL injection attack has been discussed in detail.

2.3 Eavesdropping

Eavesdropping attacks allow hackers to gain access to information and control of devices while data is being transmitted over a network. HomeTec software comes with a built in firewall that will confirm and check for the user and admin authentications before establishing the network.

2.4 Biometric Security

Biometrics Technology provides a certain degree of security which only allows the user to have access to the system. HomeTec will allow users to encrypt their data with their own fingerprints which would make the data more secured. This security approach has been discussed in detail.

2.5 Botnets

Botnets attacks use a cluster of computers to infiltrate into systems. Botnets allow hackers to introduce malware into systems thus resulting in data leakage. HomeTec software will authenticate and run both

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020

times while encrypting and decrypting which will verify the data packets two different times making the system invulnerable. Different types of botnets and their prevention techniques have been discussed in this paper.

3. Methodologies

3.1 SQL Injection

The development of the IOT has changed the world in incalculable manners. Numerous individuals are as yet attempting to adjust to it. One of the greatest expectations to absorb information that the vast majority face is attempting to comprehend the security vulnerabilities that the IOT organize faces. SQL injection can be a considerably greater peril to the IOT than existing systems (Kim, 2017).

Anyone that utilizes gadgets that are associated with the IOT must know about these dangers. IOT engineers should likewise avoid potential risk to guarantee they are appropriately made sure about. Numerous security specialists contend that settling any security vulnerabilities that uncover any IOT gadgets to a SQL injection should be a first concern. The most well-known way these gadgets are hacked is if the programmer utilized a SQL injection to deal with a cell phone that controls these gadgets. Some gadgets are greater meant to prone than others. Cameras are most in danger, since they can be hacked and transformed into spy frameworks. Phone locks are better made sure about, yet at the same time should be ensured. So as to totally capture IOT gadgets, programmers need to expect root level of control of it. Probably the most straightforward ways for them to do this is by utilizing a SQL injection. The extent of this hazard is as yet being evaluated by driving security specialists. In any case, they have discharged certain discoveries proposing that SQL vulnerabilities can devastatingly affect IOT networks .A number of botnets have been concentrated cautiously. They misuse a few diverse security vulnerabilities, yet those that permit them to start SQL infusion assaults are among the most well-known botnets. One IOT worm known as Hajime cases to be battling this pestilence. The mysterious designers of the Hajime worm guarantee that their creation is customized to chase down malevolent systems and square them from tainting different gadgets. It works by recognizing apparently defenseless IOT gadgets and fixing the defects that open them to being captured by a SQL infusion (Pearson & Bethel, 2016). Up until now, Hajime is by all accounts conveying on its guarantees. Oneself declared vigilante worm has accepted access to more than 300,000 IOT gadgets and refreshed security patches to obstruct SQL infusion assaults (Pearson & Bethel, 2016).

As selfless as it sounds, security specialists alert against trusting Hajime. They despite everything don't know precisely what the worm truly does. It is conceivable that it has a progressively vile intention and is being veiled as a vigilante application to keep individuals off their protection. Regardless of whether

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020

DOI: 10.5281/zenodo.4099720

the application does what it is asserting, it could unintentionally exchange some SQL infusion vulnerabilities with others. All things considered, the Hajime has helped feature the seriousness of the dangers that SQL infusions have made (Shah & Venkatesan, 2018).

IOT gadgets are hard to make fully protected for various reasons. Perhaps the greatest concern is that these gadgets should have the option to be operated remotely, which implies they can't be protected with a firewall. This leaves IOT gadgets presented to numerous kinds of assaults that would effortlessly be defeated by work area or cell phones. Because of the threats of SQL infusions, they should be probably the greatest concern. Since SQL assaults are intended to take over control of a gadget, having an enemy of root feature is probably the most ideal approaches to make sure about the gadget. This will distinguish any endeavour to get to the root level controls. On the off chance that such an endeavour is made, the gadget can bolt out any intercepting traffic.

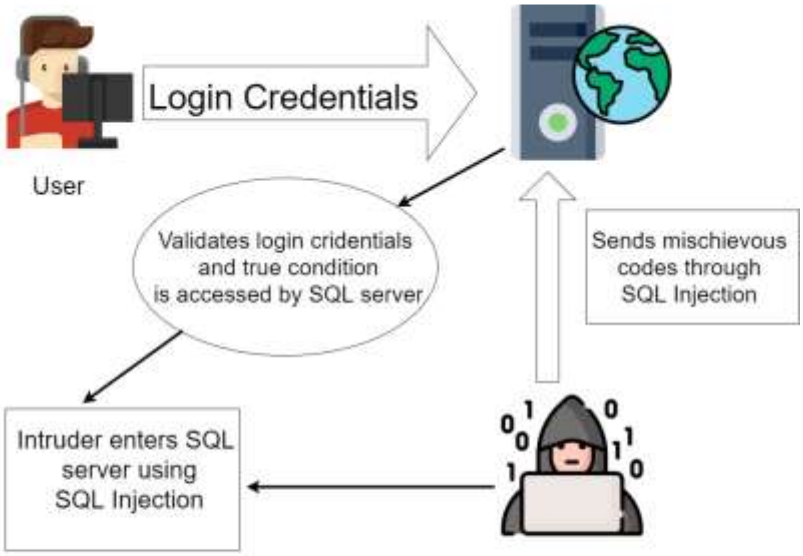
This would make it a lot harder for a programmer to arrange a SQL infusion assault. They would need to:

- Decompile source code of any powerless applications utilized on an IOT gadget that they could infiltrate
- Dispose of any SSL sticking capacities and hostile to root highlights
- Gather the application once more
- Physically or remotely reinstall it on the gadget

This would be an exceptionally lumbering procedure. A few programmers would have the commitment and determination to proceed with it. Be that as it may, essentially outfitting all helpless applications with against defeat this would be an extremely lumbering procedure. A few programmers would have the devotion and guts to proceed with it. In any case, just outfitting all defenceless applications with against root capacities would be sufficient to deflect at any rate 90% of would be programmers from propelling SQL infusion assaults.

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020

DOI: 10.5281/zenodo.4099720


Login Credentials
User
Validates login cridentials and true condition is accessed by SQL server
Sends mischievous codes through SQL Injection
Intruder enters SQL server using SQL Injection
0 1 0 0 1 1 1 0

3.1.1 SQL Injection Flow Chart

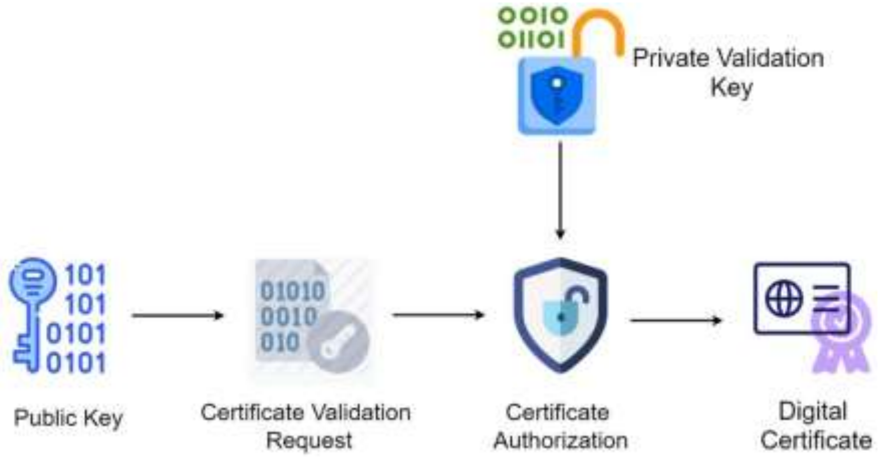
3.2 Digital Certificates

Digital Certificates perform a pivotal job in building up safety, uniqueness and keeping up information and gadget trustworthiness (Liu, Zhang , Chen, & Wang, An efficient privacy protection solution for smart home application platform, 2016). PKI utilizes digital certificates to empower gadget to-gadget or gadget to-server authorization and validation. Authentications additionally secure the information traded between gadgets. Computerized declarations i.e. Digital Certificate are the establishment of a system's IoT security, ensuring its information, confirming its gadgets, and making trust for everybody collaborating with the system. With the IoT, systems are extending and turning out to be all the more impressive in this way keeping up the trustworthiness of information and security has never been increasingly significant. A PKI-based authentication arrangement doesn't require tokens or passwords. Rather, digital certificates are utilized to tackle the confirmation challenge. PKI handles the test by utilizing these validated certificates in spite of security conventions to encode and make sure about interchanges inside an IoT network (Chien, 2018). Cloud innovation and mobility of data activities have driven an expansion in PKI selection throughout the most recent couple of years. With proficient authentication conveyance arrangements accessible, more associations have improved their system security by sending PKI administrations. Transferring digital certificates to IoT gadgets is the optimal available solution which is a lightweight arrangement that can be provided by not giving up the cost of security. These certificates require just a limited quantity of deployment on the gadget and give solid verification and information transmission securities.

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020

DOI: 10.5281/zenodo.4099720

An IoT gadget furnished with a certificate additionally can be equipped with characteristics for identifying the authorized individuals. On the off chance that your association has numerous gadgets that change regularly, they can be handily distinguished and refreshed frequently. Certifications can be tweaked to have a protracted lifestyles expectancy, so each individual machine can be organized and now not be a worry for IT. All together for the answer for be viable, the association must be prepared to deal with a PKI arrangement. It must be expandable, modifiable, and economical. With different individualized computing gadgets, there are standard strategies for certification provisioning. IoT gadgets are reason invented to perform different tasks, from low force/process gadgets to off-the-rack equipment/programming, this makes it hard to select them. In spite of this, the EST and SCEP conventions have demonstrated a ton of guarantee with IoT gadgets. Overseen Devices can auto-enlist by sending SCEP arrangement profiles through a MDM (Chien, 2018). Utilizing this strategy, numerous IoT gadgets can select for testaments. The usage of ECC (elliptic bend cryptography) certifications are less operationally extreme contrasted with traditional RSA and suitable to IoT gadgets. With a secured and reliable digital certification system, we can without much of a stretch produce customized customer certifications and introduce them on our IoT gadgets. We can utilize any Root or Intermediate CA using our Managed PKI to make a custom, one-off certificate and introduce it on our IoT gadgets. This is especially helpful in light of the fact that we can utilize the CA that is utilized by different gadgets on the system, permitting our IoT to consistently interface with the system.



3.2.1 Digital Certification Flow Chart

3.3 Eavesdropping

In network eavesdropping attacks, hackers exploit the weakest connections and intercept data packets traversing the network. Any network, if not encrypted, can be read by hacker (Kim, 2017). Hackers install

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020
DOI: 10.5281/zenodo.4099720

applications that are often used by security teams to monitor and detect issues and exploit them. There are two types of eavesdropping attacks, passive and active. In passive type of attack, the program only gathers Intel but the data is never altered. In active eavesdropping attack the person inserts into the connection and masquerade they as the admin or any legitimate connection. In active attack hackers may insert, modify or remove data packets.

Detecting and preventing passive network eavesdropping attacks are unfortunately very difficult as there are no changes to the network. However, active attacks are easier to detect and prevent. Some preventions and methods again eavesdropping are briefly discussed in the succeeding passages.

1. Encryption.

   Encryptions of email, network and communications can help prevent entry of a hacker. This way any hacker will not be able to decrypt even if the data is intercepted. All web-based communication should use HTTPS.

2. Authentication.

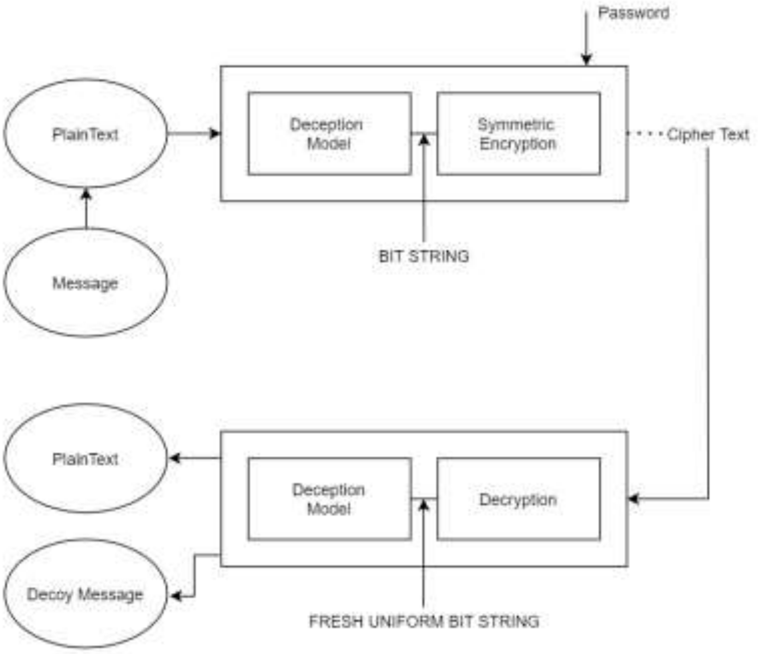
   IP spoofing and MAC address spoofing are perpetrate by spoofed packets that are used by the hackers and authenticating the incoming packets can be used to prevent that. Use standards and protocols that provide authentications.

3. Network Monitoring.

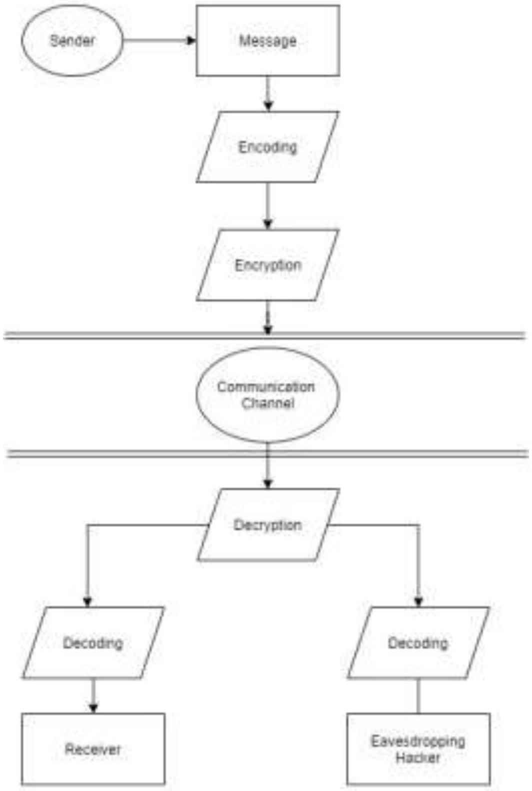
   Security teams should constantly monitor networks for abnormal activity by using intrusion detection systems or endpoint detection and response software. Security teams should also use the same sniffer programs that nefarious actors use to detect vulnerabilities on the network.

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020

3.3.1 Deception Model For Eavesdrop Attack



3.3.2 Eavesdrop Attack Flow Chart



Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020
DOI: 10.5281/zenodo.4099720

1.1 Biometric Security

IoT is best served by a lot of secure information focuses, it depends on the uprightness of the information sent and received (Kim, 2017). Those information focuses share fundamental data and make significant associations that build up connections and suggestions. Those suggestions regularly contain delicate client information, this is the place the security of biometrics turns out to be generally significant and a key player in solid security for associated gadgets and held information.

Biometric safety efforts exist at different focuses in the information pathway that makes up the IoT. From protecting a gadget with a unique finger impression sensor to using a smartcard to confirm your personality, these security focuses help make a consistent encounter and permit information to stream unreservedly and immediately between focuses. That information showing up non tampered data is significant. This takes into account brisk and productive associations that can be made, and keeps the information used to make those associations as secure as conceivable during the exchange and conveyance forms.

As the quantity of associated gadgets keeps on developing, the requirement for safeguard security turns out to be progressively significant and will keep on remaining in the bleeding edge of security master and engineers minds.

Biometrics give a protected method to move information just as recognize information ports and gadgets and guarantee that they stay secure and their information unblemished. Biometrics are an ideal safety effort, and their advancement with time will be a key segment to making hard to penetrate security conventions. Since the qualities recognized by biometric scanners don't change and are extraordinary to every person, they make a safe methods for conveying information and making identifiers for sharing made sure about information.

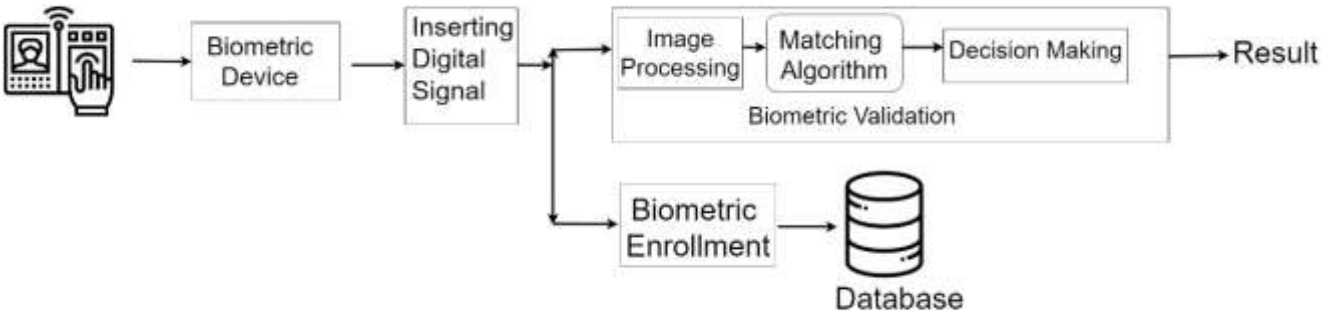
More grounded than encryptions or secret key securities the two of which can be penetrated with training and tolerance biometric qualities are very hard to copy or imitate. This element alone makes them deserving of thought in any security framework.

The development of the biometrics business will be proceeded at a quick pace, and biometrics will keep on entering all degrees of innovation. With a need to keep information secure and the simplicity of reconciliation into an assortment of frameworks, the innovation will proceed to extend and will help create consistent information move that is as secure as could reasonably be expected. Making the associations that are essential to the IoT and the proposals that end clients have come to depend on, the job of biometrics will develop and advance as the IoT keeps on developing and extending. The remarkable

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020

DOI: 10.5281/zenodo.4099720

idea of biometrics and the heap of ways that they can be utilized is probably going to assume a crucial job in the development of the IoT.



1.1.1 Biometric Security Implementation

1.2 Botnets

Botnets are collections of devices that are connected on the internet. The connection of devices to the internet makes them vulnerable to cyber-attacks. Hackers can control the devices by infecting them with malware (Kim, 2017). They use botnets to infiltrate the system and perform malicious activities such as data leakage, denial of service, data theft, invasion of privacy, unauthorized access, etc. Botnets have a big impact on IoT/Smart Home devices, even if one of the devices is compromised; all of the devices are compromised.

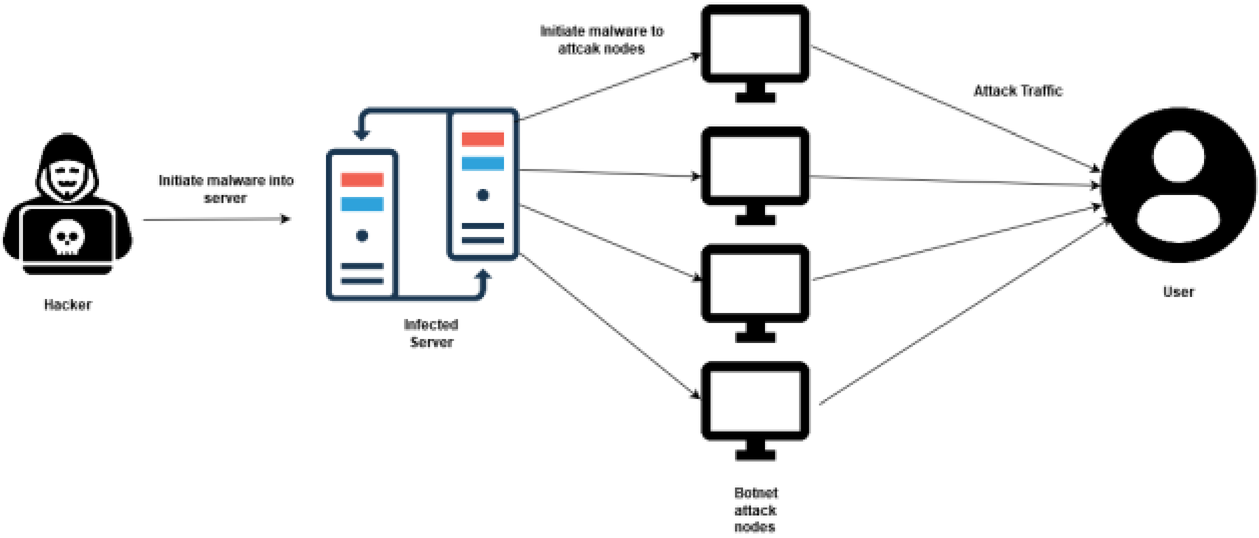
Botnets attacks are something that cannot be eradicated. One of the ways to detect a botnet attack by the use of honeypots. A cyber honeypot or honeypot works as a bait to the hackers (Meidan, et al., 2018). It is like a sacrificial computer system that acts as a decoy to attract cyber-attacks. It lures in the hackers and uses the information gained by their attempt to get into the system to learn about these hackers and their operating style. However, they do not completely prevent hacking.

Botnet prevention algorithms and security protocols have to embed in the IoT devices to secure them. Machine learning algorithms are very useful in tracking and preventing such attacks (Bertino & Islam, 2017). Graphical analysis and K-means Clustering algorithms help in the detection and classification of Botnets (Thakur, Khilnani, Gupta, Jain, & Agarwal, 2012). Machine Learning algorithms are useful as they help in understanding the type and way hackers attack. Thus helping to provide a solution soon (Bijalwan, 2020). Botnets that attack C&C(command and control) are easy to prevent, by simply shutting down the main server. Thus it cannot propagate to other connected devices. One of the other prevention methods uses Stand Alone Algorithms (Thakur, Khilnani, Gupta, Jain, & Agarwal, 2012). This algorithm parses

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020
DOI: 10.5281/zenodo.4099720

each node of the network(each of the devices connected to the network) and evaluates the data packets sent/received while also judging other parameters such as response time, output to input traffic ratio, etc. If any suspicion is raised in the algorithm a warning is sent to the main server to provide a solution.

Botnets attacks cannot be eradicated, thus the only way they can be prevented is by constant patches and software upgrades to the device. One of the major issues of such devices is the compromise on security protocols on IoT devices. Many companies have little to no security protocols as a way of cost-cutting to make the product less expensive. Many governments have fined companies to put security protocols because they fail to demonstrate their use. It was in 2019 that about 400,000 IoT devices were attacked by botnets (Bijalwan, 2020). Thus have security measures in devices is essential.


Initiate malware to attcak nodes
Attack Traffic
Initiate malware into server
Hacker
Infected Server
User
Botnet attack nodes

1.2.1 **Botnets Attack Representation**

2. Conclusion

This paper presented our proposed idea of HomeTec software that provides comprehensive approach to mitigating the attacks and various security threats in smart home devices. The threats and vulnerabilities in Smart Home devices have been studied in detail. The proposed solution to these threats has been developed in such a fashion as to cover a wide range of cyber-attacks. We have touched upon the various security aspects and provided a discussion ranging for our software from its detection to resolving the threat while keeping the system safe from future attacks.

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020
DOI: 10.5281/zenodo.4099720

3. Bibliography

1. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018, July). N-BaIoT—Network-Based Detection of IoT Botnet Deep Autoencoders. *IEEE*, 11.

2. Shah, T., & Venkatesan, S. (2018, August). Authentication of IoT Device and IoT Server Using Secure Vaults. *IEEE International Conference On Trust, Security And Privacy In Computing And Communications*.

3. Bijalwan, A. (2020, February). Botnet Forensic Analysis Using Machine Learning. *Hindawi Security and Communications Networks*, 9.

4. Chien, H. Y. (2018, July). Dynamic Public Key Certificates for IoT and WSN Scenarios. *Computer Software and Applications Conference*.

5. Yang, A., Zhang, C., Chen, Y., Zhuansun, Y., & Liu, H. (2020, April). Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms. *IEEE the Internet of Things*, 10.

6. Aly, M., Khohm,F., Haoues, M., Quintero, A., & Yacout, S(2019, June). Enforcing Security in Internet of Things frameworks: A Systematic Literature Review, *Elsevier ScienceDirect*, 6.
7. Keerthi, K., Roy, I., Hazra, A., & Rebeiro, C. (2018, December). Formal Verification For Security in IoT Devices. *Springer, Chem.*
8. Liao, Bin., Ali, Y., Nazir, S., He, L. & Khan, H. (2020, July). Security Analysis of IoT devices by Using Mobile Computing: A Systematic Literature Review. *IEEE the Internet of Things, 8*

Received: July 23, 2020 Revised: September 25, 2020 Accepted: October 10, 2020

DOI: 10.5281/zenodo.4099720