A Hybrid Honey Pot-As-A-Service Model To Secure The Network From Brute Force Attacks

Pothumani.Parvathi Research Scholar, Computer Science and Engineering, University College of Engineering and Technology, Acharya Nagarjuna University, ANUCET, Guntur, A.P. India.

Anuradha Chinta Assistant Professor, Department of Computer Science and Engineering,
Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, A.P. India.

S.R.Chandra Murthy Patnala Assistant Professor, Department of Computer Science and Engineering, University College of Engineering and Technology, Acharya Nagarjuna University, ANUCET, Guntur, A.P. India.

Abstract

The term IoT suggests an internet-like construct into which network-compatible devices can be integrated to communicate with each other at any time. Security is a major concern in the IoT networks. Honey pot is used to prepare a decoy before an unauthorized intrusion or malware infection actually occurs, catch the trend in advance, and use it as a counter measure against cyber-attacks. By making the server or network vulnerable, it is targeted by the attacker. This paper describes a hybrid honey pot as a service framework that provides security in a number of ways. The proposed framework examines the available servers for defects. When any server appears to be under attack, the honey pot system is activated. The use of multiple dummy ports complicates port scanning. When brute force attacks are detected, the honey pot model is activated, feeding false data to the attackers. This contributes to the network's security against various types of attacks, and the data is securely stored in the servers. The proposed honey pot-as-a-service can protect multiple servers at the same time. These frameworks have two modules: networking module and client server module. Networking module is used to know the open ports and status of servers. In client server module, server ask client login ID, then if credentials are correct then the client get access to the original server. If client gives wrong credentials for random no. of times then divert him to access honey pot server. N Map tool was successes in finding no. of open ports and python code were used to know status of server. We took random number generator to generate random number to find hacker and client server architecture was implemented with multi threading .

Keywords: Honey pot, unauthorized intrusion attacks, cyber-attacks, , IoT networks ,honey pot-as-a-service, brute force, port scanning, Brute force attack

1. Introduction

The use of IoT technology is a leading technology, so that more and more sensitive data from a wide variety of applications areas are generated. The Household or health / fitness needs industries in which the entire information was of high personal importance enjoy the opportunity. In the context of smart home, systems will generate a lot of data such as temperature, water and electricity need etc. With the help of such data, attackers could move and create behavioural profiles of people, from which it can be derived, for example, when the residents leave the house or are on vacation. At the same time, one can control many components remotely due to their connection to the Internet are attacked.

IDS is application or device which can be used to watch system or network for unauthorized access or malfunctioning if it finds any intrusion then informs to the system admin. Intrusion detection (Intrusion Detection) refers to system monitoring for the purpose of detecting different attempts at attacks, behavioural attacks, or results of attacks to ensure that systems resources are confidential, integrity and available. The intrusion detection system is the combination of software and hardware (IDS). The figure shows the Network Based Intruder Detection System.
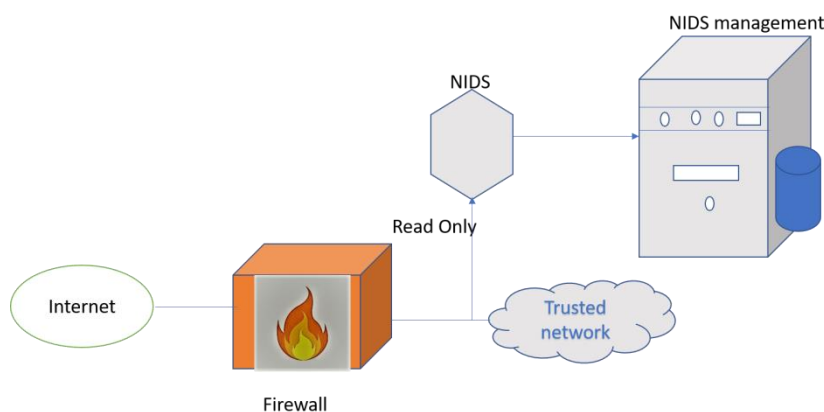
Figure 1. Network Based Intruder Detection System

Alert, IDS will issue an alert message when an intrusion occurs or tries to occur to the network manager. The information for the alarm is displayed on the monitor if the console and IDS are on the same machine and voice calls are made available. The alarm will be provided by the IDS (typically encrypted) and the SNMP (non-encrypted), email (Electronic Mail, E-mail), Short message Service (Current Message Service, SMS), IM (Instant Messaging) or by combination of methods mentioned above. Take it over to admin.

Anomaly. Most IDS alerting an event when the signal of the known attack is the same and a rough outline for the active host or network will be constructed by anomaly-based IDS. IDS will alert when other incidents occur. Signature. Attack signature is the core of the IDS, which allows IDS to alert when an intrusion occurs. If the functional data is too small, IDS is frequently triggered and this leads to false alarms or alarms and slows down too

quickly. IDS products are commonly known as IDS standards to include the number of features supported by IDS. For example, some providers use an option to cover several attacks while some providers list the features individually. How long is the ability to detect threats not defined.

1.1Honey pot

Originally, honey pot, as the name implies, seems to refer to a pot containing honey. And, as the name suggests, honey pots are sweet traps that lure malicious hackers (intruders, attackers).Honey pot plays a vital role to provide security to the network against attacks. Honey pot Traps the attackers by intentionally exposing servers and networks with vulnerabilities to the internet. First create a right environment (virtual server or physical server) to implement Honey pot and separate Honey pot from the real server and open the ports with an intention to attract hackers to get in. Whenever request comes to real server the system, ip tables are used to convert all SSH requests from port 22 to port 2222 and telnet on port 23 to port 23,where Cowrie will wait for incoming traffic. Here the honey pot which we have taken is Cowrie honey pot(medium interaction honey pot).

The mechanism and way of thinking of honey pots is really simple, and intentionally expose servers and networks with security problems (vulnerable) to the Internet. Then, by thoroughly monitoring and investigating them, the method of the attacker and the behaviour of the intruder.

Also, set up a honey pot separate from the important server, the attacker's interest will be directed to the relatively vulnerable honey pot. By doing so, it also has the purpose of diverting attacks on important servers and understanding the behaviour of attackers (Fig. 1).
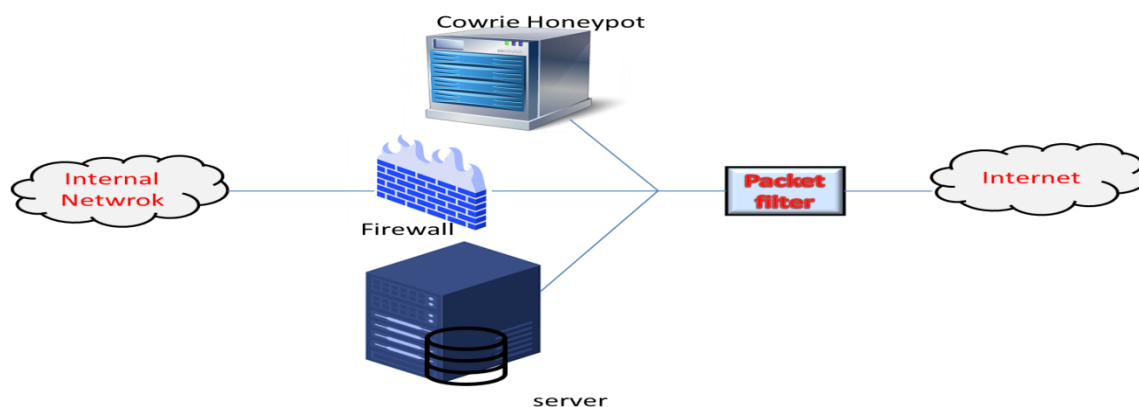
Figure 2 Example of installing a honey pot that attracts attackers

With the honey pot, the actions of intruders and attackers are all out of control. Therefore, it is said that if the psychology that a honey pot may be installed in the network works on an intruder or an attacker, it also has the effect of deterring unauthorized access. However, as will be described later, it is also dangerous to install a honey pot

easily because the honey pot may promote unauthorized access. For this reason, honey pots have long been treated as underground.

1.2. Brute Force attacks

Brute force attack is nothing but, attacker's many attempts to get password. Introducing proper rules helps to create a strong passwords and by encrypting passwords with right algorithms leads to more security.

To reduce vulnerability for brute-force attacks, Parvathiet. et.al (2021) [20] the author used PBKDF1 (Password-Based Key Derivation Function 1) and PBKDF2 are used with a sliding computational cost in cryptography. A pseudorandom function implements in PBKDF2 for the input password or passphrase like hash-based message authentication code (HMAC) in addition to the salt value. The repetition of the process is performed frequently for generating a derived key. In subsequent operations, it can be used as a cryptographic key. The password cracking is more difficult by the added computational work and is called as essential stretching.

Brute force Attack involves a method of cipher breaking and crack the password based on every possible key trails. It is also a technique of defeating the cryptographic scheme based on a large number of possibilities systematically. Owing to the number of likely arrangement of special characters, letters, and numbers, the Brute force attack is a time-consuming method [1, 4]. All key combinations can try using the additional complex brute force attacks while attempting the right password. To getting access to the system or logging into the account, a list of words or regular passwords may consider by the attacker and all sequences of words try from initial to end phases. The brute force attack occurrence is relied on

(i)   How the attacker knows the target,
(ii)   The computational power amount that being used to perform the attack,
(iii)   The password strength,
(iv)   The Password complexity, and
(v)   The Password length.

Brute force attacks can take a lot of days, months, hours, and even years although they are capable to get illegal admittance to the account. The vital resources scale can rise exponentially for brute force attack with the increasing of password length and this wouldn't be linear. Based on the following criteria, the password can create by the users to overcome this brute force attack:

(i)   Password should be a combination of Lower case, upper case, numbers, and special characters,
(ii)   Frequent proper noun doesn't enclose in the Password,
(iii)   Avoid to repeat the characters,
(iv)   Should not be a dictionary word, and
(v)   Password length should be at least 10 characters.

2. Literature Survey

Vetterl and Alexanderet al (2020) [10], in this paper it triggers a large number of security incidents. In a multi-source and heterogeneous IoT environment, traditional intrusion detection, firewall and other security protection tools are prone to omission and proneness. The problem of false positives. As an emerging active defence technology, honey pots can actively guide hacker attacks by constructing a controllable decoy environment to capture high-quality original attack data. According to data, the threat of attack can be detected with low false positives. The author basic concepts and technical development lines of IoT honey pots by investigating a large number of IoT honey pot literature, focusing on the introduction three key technologies of redirection, identification and de-identification, and data analysis are introduced. In addition, this article proposes.

Kapil et al., (2020) [11], The protection of personal privacy data is of great significance. Currently, password-based encryption methods are often used to protect personal private data. The security of this method depends on the strength of password selection, and users tend to choose simple and predictable passwords. When using an incorrectly guessed password to decrypt a message, this method will output an invalid message to indicate a failed attack attempt, so it cannot effectively resist brute force attacks. Therefore, the author introduces honey pot encryption algorithm to solve the problems. On the basis of password encryption, the concept of distributed conversion encoder is introduced. When an attacker uses brute force brute force attacks to decrypt messages, the system will provide seemingly effective to confuse the attacker. The author applies the honey pot encryption algorithm to personal electronic wallets to solve the problem of weak passwords for protecting users' bank card account numbers and passwords. The author first introduces the basic idea of honey pot encryption algorithm; then designs a fine-grained message space for the application to provide credible lure messages; introduces machine learning methods for the first time to discuss the security of honey pot encryption algorithms.

Baddar et al (2019) [12], The addresses increasing negative impact of malicious network behaviours such as network intrusion, network deception, and online spam on network security. Network behaviour recognition has become an important part of network security. The author proposes the construction of a network monitoring system based on honey net technology. Effective The honey net system's sandbox execution, feature simulation, daily benefit audit and redirection agent mechanisms are used. Solve the mathematical model based on passive monitoring It is difficult to effectively describe the problem of malicious behaviour on the Internet. Good results have been achieved in actual operation.

Pliatsios et al., (2019) [13] The rapid development of network technology, the network security of the Industrial Internet has also been seriously threatened. However, the traditional defence technology has its inherent passive defence defects. Therefore, active defence technologies similar to "honey pots" have received more and more attention. The

author will explain the working principle of "honey pot" technology and combine the current industrial network architecture characteristics, and analyze the feasibility of "honey pot" technology in industrial network detection

Pahl et al., (2020) [14] the author introduced the Hos TaGe a honey pot. There are many industrial plants are infected by malware or attackers have been compromised and prove again and again how important it is to secure these systems. Because of their age but many of the systems are not able to implement current security measures. Still exist with honey pots and Intrusion Detection Systems Opportunities to improve the security of industrial plants. In this seminar paper that will Honey Phy framework presented, which is supposed to make the detection of honey pots more difficult by expanding the simulations. A Hos TaGe a honey pot, which automatically generates signatures for intrusion detection systems in order to prevent malicious Block network traffic.

The IT systems are attacked, honey pots are usually used. A honey pot is a system that is supposed to attract attackers and records how an attacker attacks this system Nursetyo et al., (2019) [15]. Accordingly, honey pots are designed so that everything that happens to them persists around it then analyze it. Preferably happened this without the attacker noticing that it is one Honey pot acts. The data from honey pots can subsequently use to address security vulnerabilities close to creating signatures for malware and IDS and determine the attack vector of attackers.

Honey pots are also suitable for answering the questions to illuminate for ICS. However, it is necessary special Develop honey pots for them because others too Protocols are used. Many projects are devoted to the study of Attacks on ICS, such as that Kviesis et al., (2020) [16]. With the Honey train it is a simulation of a transport company. Not only software simulations were used, but also hardware that is used in a real traffic operation would occur. So were web interfaces, needed security cameras, a rail network and others Systems simulated. The results of the Honey train that most attacks are automated over dictionary attacks occur and come from China. However, only a few attackers actually managed to penetrate the system.

Udhani et al., (2020)[17], Honey pots are used to provide as much information as possible to collect. Even if an attacker realizes it is a honey pot, it's interesting how he found out . But it must be observed be that a honey pot doesn't have any after its discovery can collect more information about the attacker conversely, a honey pot must not be too closed so the attacker can hardly use the honey pot can interact. Accordingly, honey pots have to be well hidden and inconspicuous, but not too much either hidden and inconspicuous.

Karabulut et al., (2020) [18] the authors, Analyse and compare the traditional firewall technology to protect the security of computer network and the newly developed "honey pot" technology. It is believed that the latter gets rid of the former's passiveness in responding to attacks, and has active countermeasures against various attacks, and can

be combined the form of computer crime forensics resists various attacks, so it has a broader development prospect.

A significant amount of research has been done to detect the malware in IOT network environment. This survey describes some of them. In securing IOT Networks Experts are taking Honey pot As a deception tool to include additional layer of safeguard. In parvathi.et.al (2020)[19], surveyed that six sorts of honey pot to recognize the malware interruption in the broadband systems. The implantation of honey pot along the broadband system can keep the IoT gadgets from pernicious assault, for example, DDoS assault, spamming and so on. [5] Proposed the primary Honey pot to be specific IoT PoT alongside sandbox called as IoT BoX. This honey pot imitates the telnet administrations of various IoT gadgets. Since the greater part of the intruders incline toward telnet convention to login IoT gadget remotely, author design his honey pot and sandbox investigation just for the telnet convention traffic. The IoT BoX is prepared to help telnet banner for various architectures, for example, spreading over MIPS, ARM, and PPC and so forth. By joining both IOT PoT and IOT BoX, absolutely five sorts of malware families which performing DDOS assaults have been recognized effectively. The execution of the IoT PoT depends on the desire for the aggressor on the telnet which is introduced on the IoT gadgets. With the goal that it is easy to catch all kinds assault happens with respect to the IoT gadget.

Fan, Wenjun, Zhihui Du, Max Smith-Creasey, and David Fernandez et al (2019) [6] proposed a honey pot which mimics the WAN like network with exceptionally handling backend segment. In this paper, the traffic emerge from one source at brief timeframe is considered as one session. This honey pot contains of four modules to be specific: Sensor, Backend, Frontend and Analyzer. The job of sensor is to recover all the data from the unauthorized login. In the backend all the gathered information is exposed to the procedure of encryption and it frames a relational database. In analyzer the statistics of the gathered information will be recovered. Ultimately, the frontend is a GUI segment to see the statistics of all the gathered raw information..

Recently, machine learning algorithms are used to enhance the IoT security. In earlier times, utilizing machine learning classifiers to help security in IoT environment has become amazingly critical to confront the difficulties. However, we have not discovered an excessive number of works that utilized machine learning with regards to security challenges in IoT based environment.

Sharma, Sparsh, and Ajay Kaul et al (2018) [7] proposed a lightweight malware recognition utilizing hardware features. The inspiration of the author to pick the characteristics of hardware rather than software is the necessity of the power and memory to the previous is less when contrasted with the later. This proposed algorithm is intended for the Android OS that most of the Google item depends on the Android OS. In this paper CPU and memory related highlights are utilized for dynamic investigation. To separate indulgent files from malicious files they utilized various machine learning

classifiers, for example, Naive Bayes, Logistic Regression, and J48 Decision Tree. author has favored android based malware datasets to test his identification algorithm. Table2 shows various machine learning algorithms used To secure IOT network
.

Babash, Alexander V., Valery A. Sizov, and A. A. Mikryukovet al (2019) [8] proposed a network forensic technique to distinguish the botnet in the IoT condition utilizing machine learning strategies. In this paper, author has used four diverse arrangement methods in particular: Decision Tree, Association Rule Mining, Artificial Neural Network and Naïve Bayes. This framework includes four unique modules. The main module is traffic assortment where all raw packets of the network are gained. The subsequent module is selection of feature where the important data are chosen from the raw information utilizing Information gain feature selection technique. The third module is preparing the four distinctive classification algorithm. The last module is an evaluation metrics where the exhibition of the four classification algorithm has been assessed utilizing perplexity lattice. The exhibition of the calculation has been assessed utilizing two measurements, for example, accuracy and false alarm rate.

There are so many approaches to detect and prevention of attacks using honey pot . Each and every approach will server for different purpose, most of them used Honey pot to detect for attackers. However, traditional honey pot technology has inherent shortcomings such as static configuration and fixed deployment, and it is very easy to be attacked. Attacker identification bypasses and loses decoy value. Therefore, how to improve the dynamic and deceptive nature of honey pots has become a key issue in the field of honey pots. First, the development history of honey pots is summarized. Then, the key technology of honey pots is the core, and the implementation process, department. It analyzes the method of signature, anti-identification thinking, and the theoretical basis of game; finally, it classifies and narrates the defence results of different honey pots in recent years, and develops the honey pot technology. Development trends are analyzed and stated, aiming at potential security threats, and looking forward to defence applications in emerging areas. In this paper, AES algorithm has been developed. In addition key management feature is added which provides more secure for registered users.

3. Framework for Honey pot Security:

Honey pot is a deception technology for attackers to monitor, detect, analyze, and trace the source of the attack and also Honey pot technology is a trap which itself can provide a security to the IOT network by open ports intentionally, we can enhance the capacity of honey pot with encryption techniques to provide ,more security from the attackers.

In parvathi et.al (2021) [20], proposed added key management features to secure registered genuine users account details and for each user they created keys with an algorithm called PBKDF2 (Password-Based Key Derivation Function 2) and using this

KEYS they encrypted users account details by using AES algorithm. By encrypting user account, they avoided misuse of data as internal employees of database can view all those records if we store in plain format and can misuse it and by encrypting, we can avoid such misuse. Another advantage of encrypting data with keys is they have sent encrypted data in network so no hackers can understand it after stealing from network. In this work user data will exchange between browser and honey pot in the form of encrypted data.

It has no business purpose. All traffic flowing into/out of the honey pot indicates scanning or attack behaviour, so it can be better. Focus on attack traffic. Honey pots can actively trap attackers, can record many traces of attackers in detail, and can collect a large amount of valuable data, such as the source code of viruses or worms, hackers' operations, etc., so as to facilitate the provision of rich Traceability data. In addition, the honey pot can also consume the attacker's time and obtain the attacker's portrait based on JSONP and other methods.

3.1 Honey Pot Working Principle Includes:

1. The attacks perform by attackers through the requests via the internet is involved in the first process.

2. Second process includes the request activities carried out by the attacker when the internet provides a response.

3. A follow-up action is involved in the third process, where the gateway can access by the attacker after connecting the activities successfully through the interest. Here, gateway refers to the device that connecting one computer network or more computer networks based on various communication media. So that, the data will be different if the computer network is switched to different media.

4. In fourth process, the attacker performs the activities to obtain the device information including a user name and password connecting to a computer network. The attacker can make the activity on the main server if the server doesn't install a honey pot. The shadow server activities will be allowed by the attacker when the honey pot installs. However, the attacker will not be succeeding in cracking a password, adding files, and a backdoor installation.

Various concepts require to play a role in training, forming, and building before establishing a honey pot. In system requirements, some of the models require as a step. To overcome the attacks that occur in the system, the honey pot is essential for being an additional device. In honey pot, different elements have found out such as

1. Packet Analyser;
2. Keystroke Logger;
3. Alerting Mechanism;
4. Monitoring or Logging Tools;
5. Forensic Tools.

A little data is collected by the honey pot but it can be used to do rapid analysis and response with a high value. Even though honey pot system has complex ideas for research, it can be easier to configure while utilization purpose. The smaller the risk with the simpler honey pot such as if the data volume is not as much as a log on a firewall system or IDS.

The detection of attackers has included one major issue is the 'needle in the haystack'. Because, one don't know the attacker access the data from which connections among the gigabytes of data over the network. One also not able to find the few that are logging in by an attacker from the millions of log entries.

To overcome these problems, honey pots is the one opportunity. It's better to find a needle in an empty room rather than searching for a needle in a haystack. Most often, honey pots develop as a host that is not being utilized by employees. The security team receives alerts from honey pot if an attacker is attempted to scan the host or log in.The security team receives alerts from honey pot if an attacker is attempted to scan the host or log in. Whenever Honey pot installed in some host it is keep on busy to listen for the request, when ever request comes then it will send a response and will ask for login details, then the hacker get an access after credentials entered. Then Honey pot will keep a record in the log to monitor his behaviour and alert the security admin. If hacker knows he is in honey pot then the request of hacker will forward to shadow server.

Honey pots can use for research purpose and the Kippo SSH honey pot follows the operations similar to an SSH server. If in case they display to be brute forcing, an attacker is allowed in. Accordingly, the defenders and researchers can get to know about an attacker actions. A similar idea of either heavily instrumented or emulating normal behaviour is followed by self-implemented honey pot servers and most of the honey pot services to know information about the attackers, their intent, and tools as much possible. For example, Sys Dig on Linux is allowed the instrumentation of what happens on the host to understand the attacker's operations easily.

Other opportunities are not considered with honey pot hosts. The attackers should detect by defenders everywhere. They are trying to find out whether a honey pot could design around the attackers or not. For example, 'honey creds' have used that can set up unused privileged accounts and the security team getting an alert when attempt occurs to log into these accounts. If domain admin is identified and a default password is attempted by an attacker, immediately it becomes obvious.

The individual files are also 'honey potted'. Fake versions can create by evaluation of files of the company that considers to be the most valuable assets and investing the files attackers' types that trying to be collected. An attacker snooping around or an overly nosey employee can reveal by those files' monitoring access.
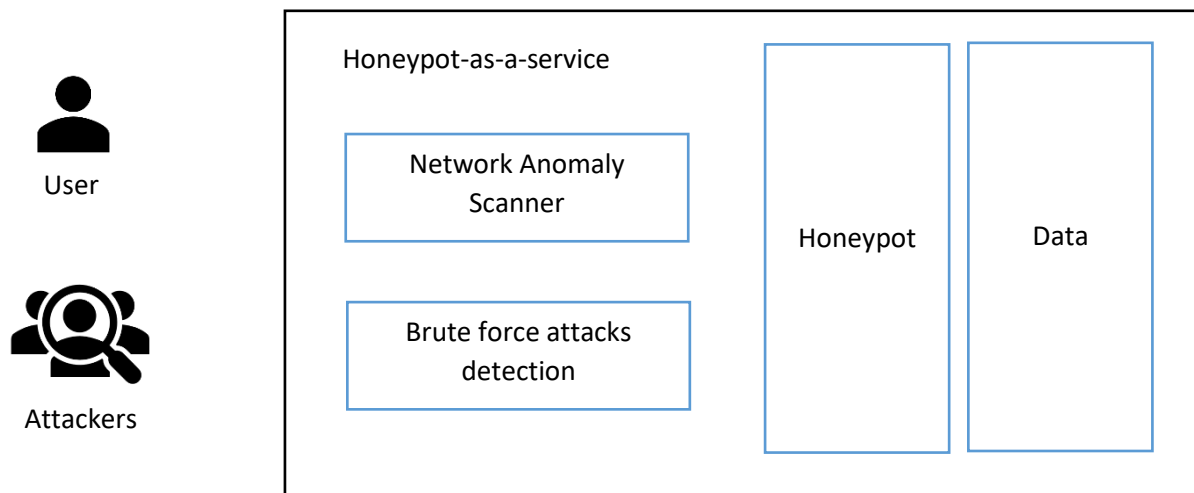
3.2. Honey pot as a Service

Before going to discuss about Honey pot as service first we should know how hacker can attack the system or server, When an attacker tries to attack or access the server, then activities of attacker are

a) ping- to know the address of the target server.

b) Nmap- port scanning

c) use soft ware's- to perform Brute force attacks on SSH service to find password

once they got password they take a control of target server which causes high volume of loss to the network, so to avoid all these things one of the best approach is implement Honey pot with fake data and fake services and also make honey pot to create shadow server so that we can easily trap the attacker and This allows the server admin to know the attacker's info in the form of an IP address, date of the attack, and activities that the attacker is doing on that server. Later server admin update the firewall with honey pot log files to avoid damage to the network in future.

So the advance in honey pot is using "honey potting as a service" is being implemented, where the organizations can reduce the effort and time for setting up and monitoring a honey pot through the purchasing of honey potting services that can help to investigate the attacker activities with user-friendly environment.

Fig 3: Proposed Honey pot-as-a-service framework

In the proposed framework we have taken genuine user as USER and unauthorized users as Attacker. When ever user or attacker tries to access the network first need to find the whether the user is normal user or attacker so hence we implemented brute force attack method to find unauthorized users.

- The server asks the clients to send the user credentials namely login ID and password.
- If the user exists in the database, access to the IoT sensor information is passed to the user.

- If invalid user details are provided more number of times, the server identifies that a brute force attack is being initiated.
- After random login attempts, the honey pot server is imported and the hacker is fed false information from though the honey pot.
- The hacker cannot identify that the data being received is fake.

3.3 Network Anomaly scanner do the following activities

- The network monitoring module scans the available ports and checks if the servers are responding or not.
- The servers send their response to the Network Monitoring Module with the following details:
  1. Working status (Open/ Down)
  2. Number of active clients
  3. Blocked hacker IDs
- The number of active clients can be monitored using this information. The hacker IDs blocked by one server can be stored in a central database so that all the servers can access this information.
- The Network Monitoring Module can immediately identify the servers which are down (hacked) and necessary action can be taken.

3.4 The features of the proposed model include:

1. Monitors network behaviour-we developed efficient Honey pot to monitor hackers who are coming and going out of the network.
2. Brute force attack detection-By implementing Honey pot with fake file system and fake data we detected attacker when ever he tries to get the password file from the system using brute force technique.
3. Security against brute force attacks-providing guidance to the user to create strong password.
4. Security against port scanning-we created multiple dummy ports to provide security against port scanning.
5. Spam the hackers with multiple ports-we created trap servers to deceive hacker.
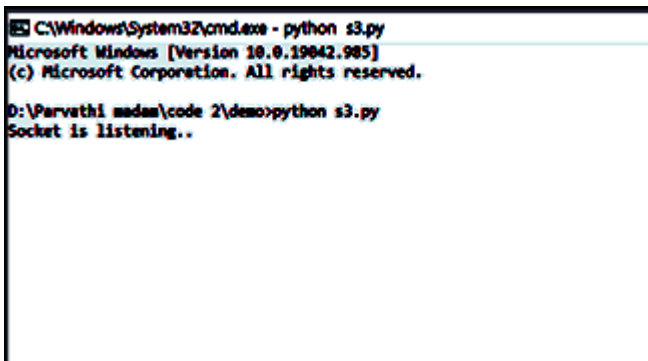
Another emerging application is adaptive honey pots and 'active defence' which doesn't include alerting defensive teams but reacting to the attackers actively after detection. However, the response nature can be varied. The automatic flagging of all other behaviour from IP address or account causes by detection in the enhanced monitoring. The attackers' isolation or segregation have demonstrated in other concepts. For placing the attacker in a zone, networks need to be configured in a way that they are restricted to the damage. To mitigate the attacker or investigate about their actions, the network isolation or some potential elements of a fake network can create.

Sometimes, the coupling of such 'active defences' and honey pot concept considers as automated response to the attacks. In case of attacks detection has low false positives

only, it can be done safely. Most of the organizations don't want to adapt the system, in which employees may be frozen out of business systems unnecessarily. The low false positive rates can provide if honey pots implemented correctly. It's required to evaluate the future directions and version of regular honey pots to know whether they may suffer from same drawbacks as the traditional strategies of honey pot.

4. Experimental Results

Parvathi et.al [2021] [20],the author has designed 5 honey pot servers to handle multiple attacks when ever request comes ,the request will be send to the random honey pot server after request has been classified as attacker request. Then the Honey pot server process the attacker's request and send fake data to him. Honey pot also alerts the admin and other devices not to communicate with him. Honey pot also maintain log to know the behaviour of attacker so that can prevent IoT network from those attacks in future. Honey pot is operated as a security system that creates a trap server or a shadow server. The attacker enters and accesses the server if an attacker has tried to access or attack the server. But, the honey pot created the shadow server that can be accessed by an attacker. It helps the server admin to get the information of an attacker including the attack date, an IP address, and the activities that performed on the server by the attacker. The server becomes online as shown in figure 4.
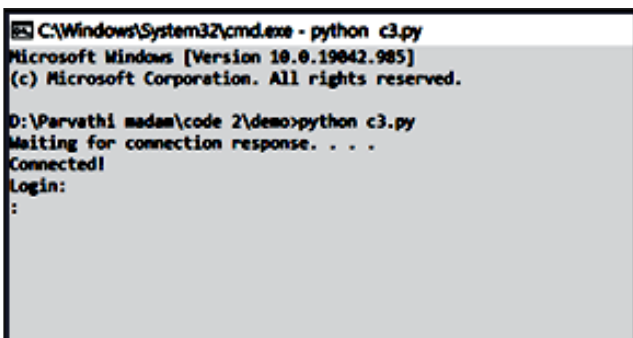


```
C:\Windows\System32\cmd.exe - python s3.py
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

D:\Parvathi madam\code 2\demo>python s3.py
Socket is listening..
```

Fig 4: Server listens for the clients

The client tries to connect to the server as shown in figure 4.


```
C:\Windows\System32\cmd.exe - python c3.py
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

D:\Parvathi madam\code 2\demo>python c3.py
Waiting for connection response. . . .
Connected!
Login:
:
```

Fig 5: Client connection request

When the client sends a request to the server, the client gets a message to enter the login details. The server stores the client's information and records it as shown in figure 6.

Fig 6: Server records the client's information

Fig 7: Client login details

Once the client enters the login details, as shown in figure 7, the server validates them. If the user is genuine, the data is shared with the client. If a brute force attack is detected, the server redirects the client to the honey pot server and feeds false data.

The network scanner continuously scans if the open ports are available. In case any port is identified as closed, the administrator is alerted. This phenomena is shown in figure 8.

Figure 8: Network scanning

Next we have done web based approach to detect unauthorised user who are trying to access IOT network.

Figure 9 Admin Login Screen
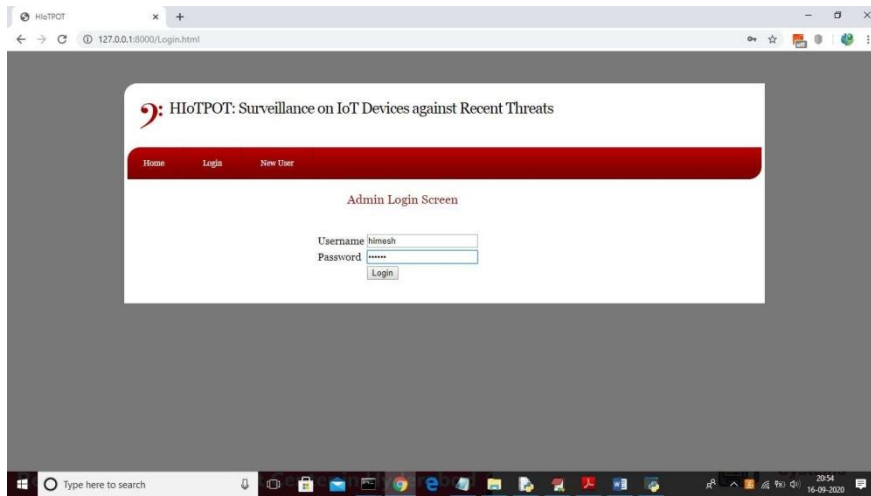
In above figure 9 represents the user logged in as himesh and after submitting button will get below screen.
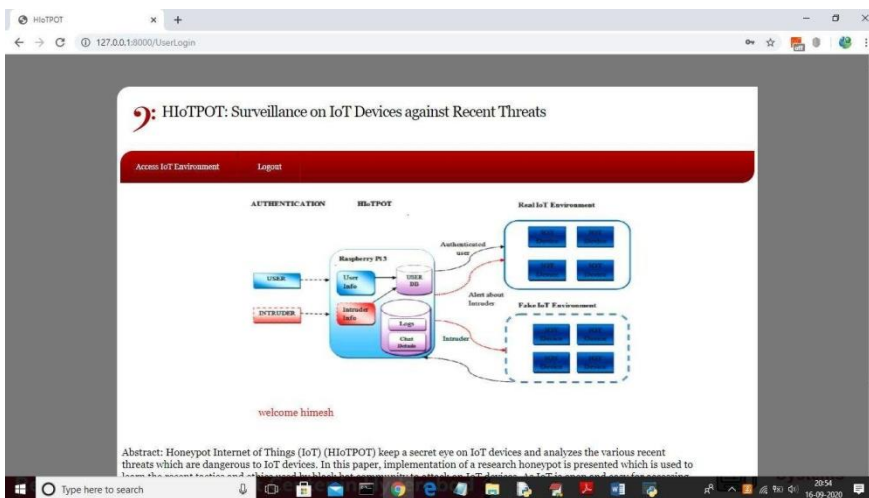
Figure 10 IoT Environment in Honey pot

In above figure 10 after login we got user home page where user can click on 'Access IoT Environment' link to access IoT data but before that we will see Honey pot directory for log file.
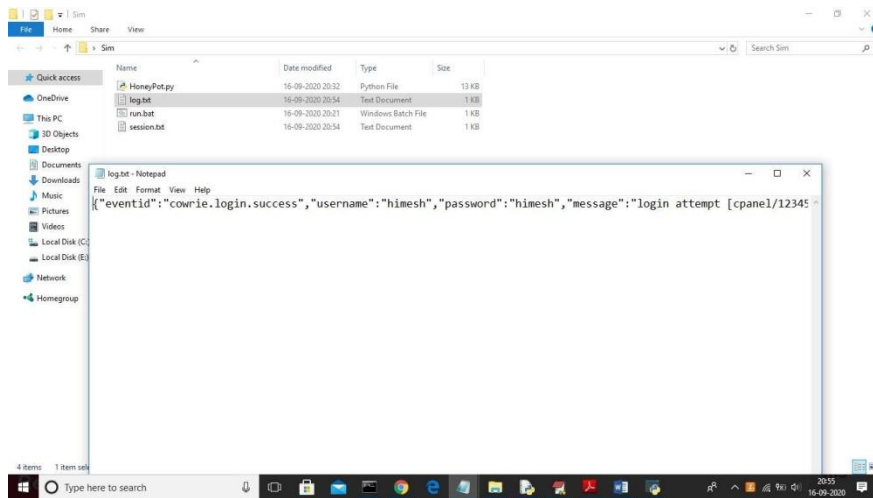
Figure 11 Honey pot Server Log File

In above figure 11 at Honey pot server log file created and in log file we can see the success event as him eshuser is authenticated in database. Now we will click on' Access IoT Environment' link to access IoT data.
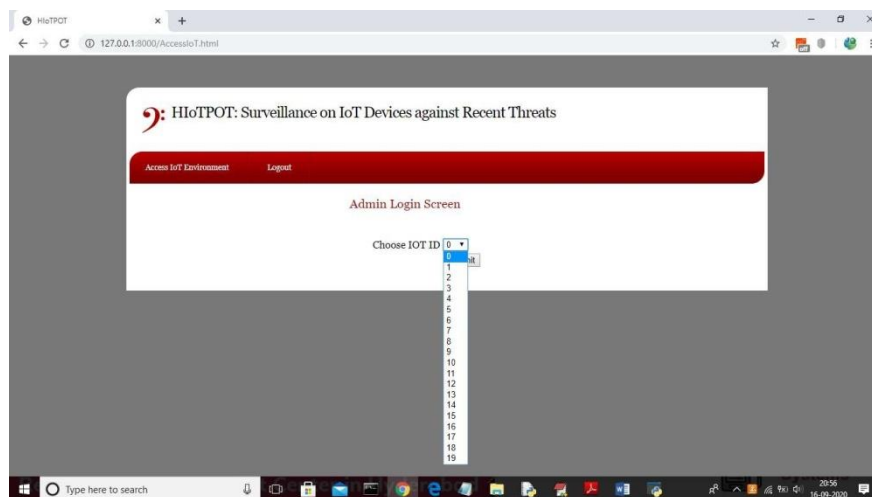
Figure 12 IoT ID Selection

In above figure 12 user can select any IoT id and then click on submit button to get its data.
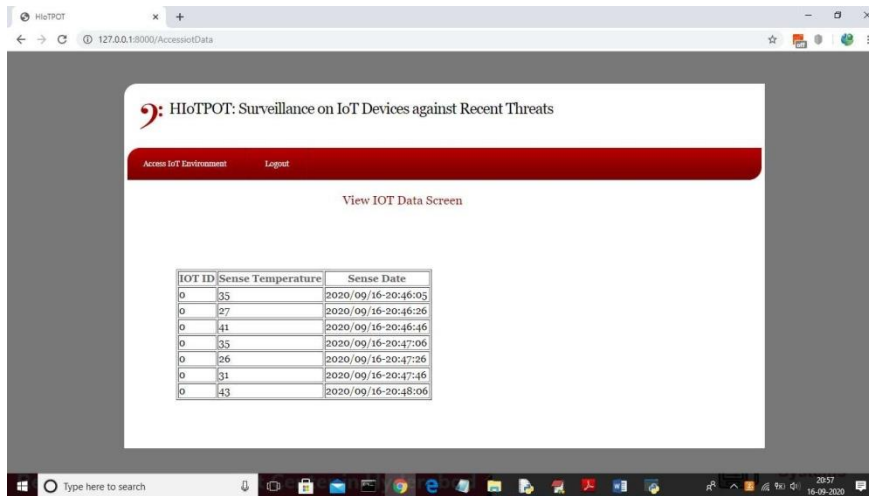
Figure 13 Screen for IoT ID 0

In above figure 13 for IoTID0 we got some records of temperature. Now we logout and try to login as attacker with fake id.
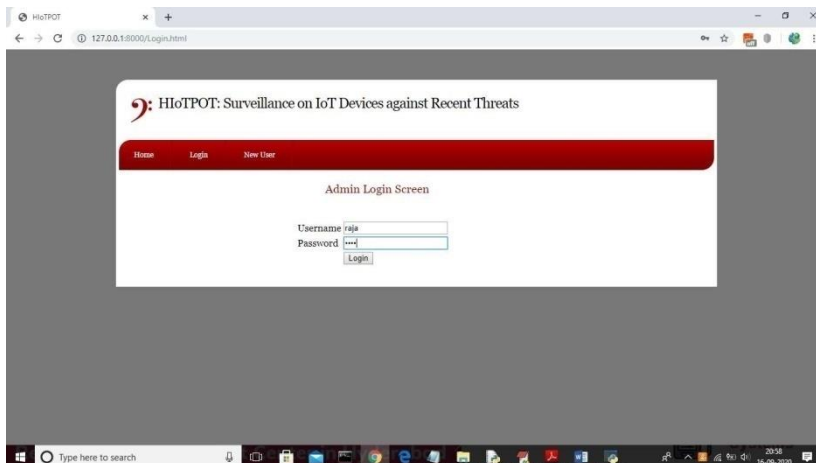
Figure 14 Hacker Trying to Login

In above figure 14 attackers is login as raja and this user is not signup and attacker try to login and Honey pot will identify this attacker and allow him to access dummy data.
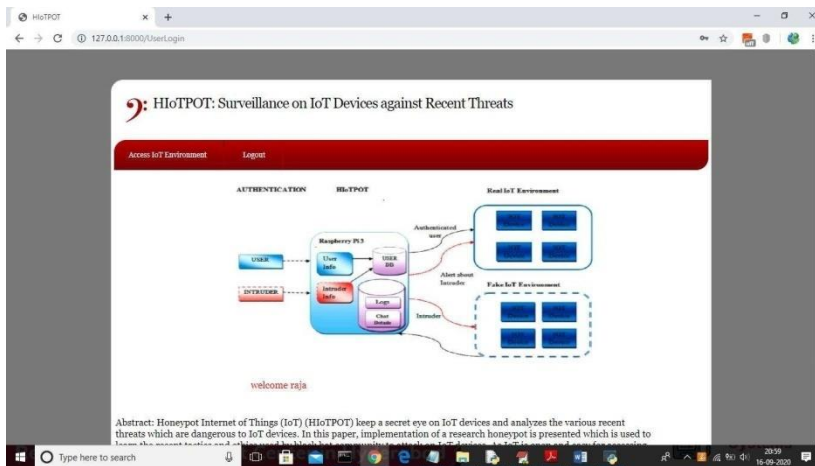

Figure15 Attacker in Honey pot Server to Access IoT Data

In above figure15 for attacker also Honey pot allow to access IoT data and now attacker can click on 'Access IoT Environment' link to access data.


Figure16 IoT ID Selected by Attacker

Pothumani.Parvathi   A Hybrid Honey Pot-As-A-Service Model To Secure The Network From Brute Force Attacks

In above figure16 attacker can select any device id and then press submit button to get dummy data.
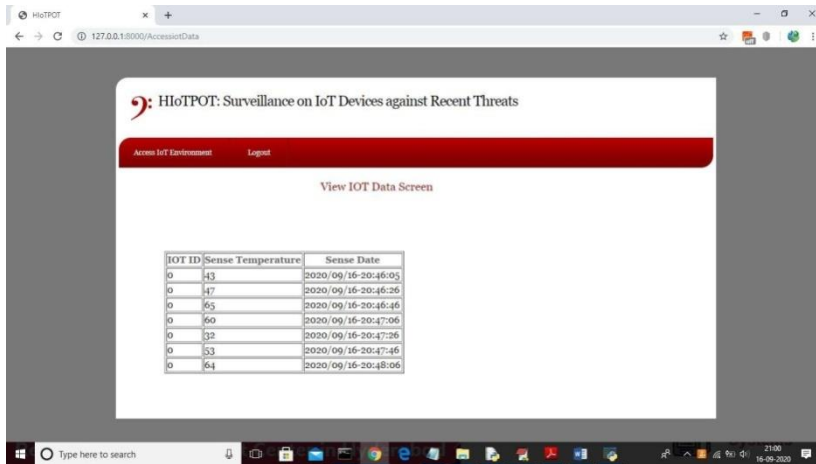
Figure17 IoT ID0 Accessed by Attacker

In above figure17 for IoTID0 attacker got temperatureas43 for first record and you can compare with genuine record in below screen.
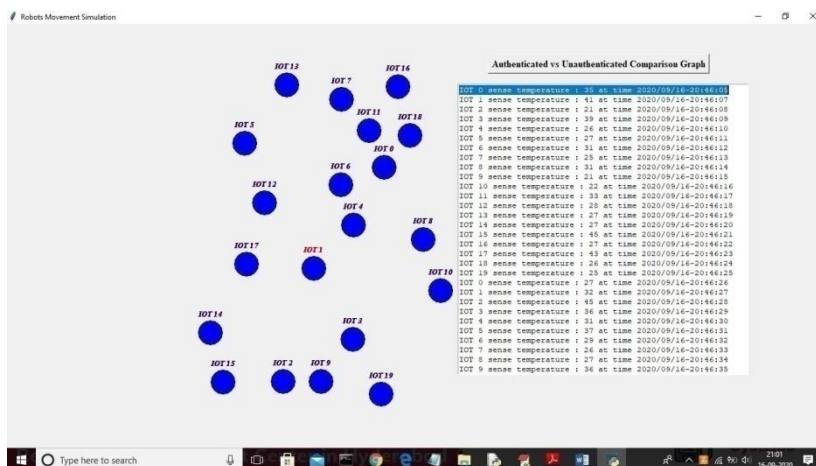

Figure18 IoT ID0 Data

In above figure18 IoT0 has 35 value in first record but Honey pot sent 43 to attacker and now see Honey pot log file again.

Figure 19 Log File Data Mismatched

In above figure 19 log file for username raja Honey pot record data as login failed and extract ore information by receiving other commands also from attacker. In above screen we can see attacker has send command to access IoT 0 records.
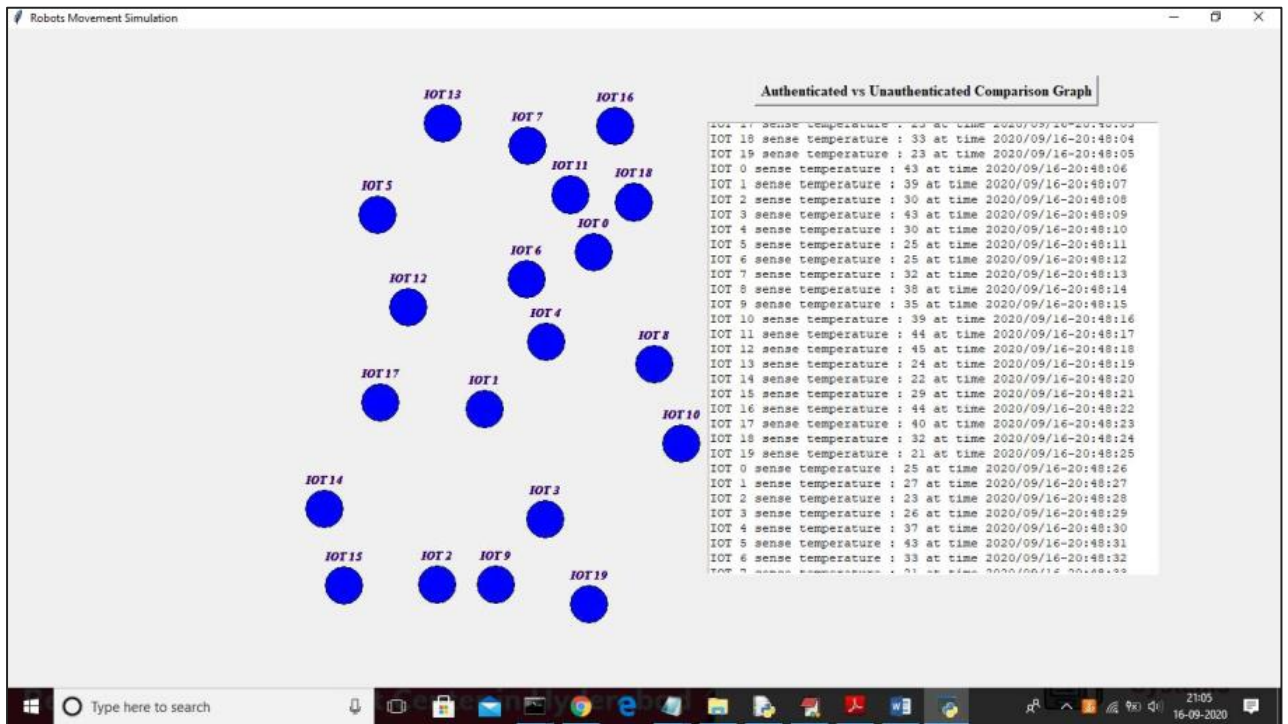
Figure 20 Attacker Send Commands to Access IoTID 0 Records

In above figure 20 similarly Honey pot monitors all users and then informs to IoT devices about normal users and attackers.

Conclusion

This paper presents a honey pot-as-a-service framework to defend the network against attackers. The system scans the network servers to detect anomalies. System scan the request and classify the request using Deep learning algorithm .If it finds any Brute force attacks are detected and the honey pot system is activated to mislead the attackers. If it detects multiple types of attack requests then system divert those to randomly selected honey pots, This helps securing the network from multiple types of attacks and by providing encryption algorithms like key management and AES algorithms then crypted data is securely stored in the servers. The proposed honey pot as a service can provide security to multiple servers at the same time.

Compliance to Ethical Standards

Hereby, we declare that no conflicts of interest among authors. Moreover, the current research does not involve any Human Participants and/or Animals. Hence, no need of informed consent

Reference

[1].   Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. "Survey of intrusion detection systems: techniques, datasets and challenges." *Cybersecurity* 2, no. 1 (2019): 1-22.

[2].   Shamshirb and, Shahab, Mahdis Fathi, Anthony T. Chrono poulos, Antonio Montieri, Fabio Palumbo, and Antonio Pescapè. "Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues." *Journal of Information Security and Applications* 55 (2020): 102582.

[3].   Meijaard, Yoram J., Bram CM Cappers, Josh GM Mengerink, and Nicola Zannone. "Predictive Analytics to Prevent Voice over IP International Revenue Sharing Fraud." In *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 241-260. Springer, Cham, 2020.

[4].   Fouad, Maria A., and Amr Talaat Abdel-Hamid. "On Detecting IoT Power Signature Anomalies using Hidden Markov Model (HMM)." In *2019 31st International Conference on Microelectronics (ICM)*, pp. 108-112. IEEE, 2019.

[5].   Erlacher, Felix, and Falko Dressler. "On high-speed flow-based intrusion detection using snort-compatible signatures." *IEEE Transactions on Dependable and Secure Computing* (2020).

[6].   Fan, Wenjun, Zhihui Du, Max Smith-Creasey, and David Fernandez. "Honey DOC: an efficient honey pot architecture enabling all-round design." *IEEE Journal on Selected Areas in Communications* 37, no. 3 (2019): 683-697.

[7]. Sharma, Sparsh, and Ajay Kaul. "A survey on Intrusion Detection Systems and Honey pot based proactive security mechanisms in VANETs and VANET Cloud." *Vehicular communications* 12 (2018): 138-164.

[8]. Babash, Alexander V., Valery A. Sizov, and A. A. Mikryukov. "Security Evaluation of a Brute-force Attack on a Cipher using a Statistical Criterion for Plaintext." *Automatic Control and Computer Sciences* 53, no. 1 (2019): 39-44.

[9]. Nursetyo, Arif, Eko Hari Rachmawanto, and Christy Atika Sari. "Website and network security techniques against brute force attacks using honey pot." In *2019 Fourth International Conference on Informatics and Computing (ICIC)*, pp. 1-6. IEEE, 2019.

[10]. Vetterl, Alexander. "Honey pots in the age of universal attacks and the Internet of Things." PhD diss., University of Cambridge, 2020.

[11]. Kapil, Gayatri, Alka Agrawal, Abdulaziz Attaallah, Abdullah Algarni, Rajeev Kumar, and Raees Ahmad Khan. "Attribute based honey encryption algorithm for securing big data: Hadoop distributed file system perspective." *PeerJ Computer Science* 6 (2020): e259.

[12]. Baddar, Sherenaz Al-Haj, Alessio Merlo, and Mauro Migliardi. "Behavioural-anomaly detection in forensics analysis." *IEEE Security & Privacy* 17, no. 1 (2019): 55-62.

[13]. Pliatsios, Dimitrios, PanagIo Tis Sarigiannidis, Thanasis Liatifis, Konstantinos Rompolos, and Ilias Siniosoglou. "A novel and interactive industrial control system honey pot for critical smart grid infrastructure." In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp. 1-6. IEEE, 2019.

[14]. Pahl, Marc-Oliver, Alexandre Kabil, Edwin Bourget, Matthieu Gay, and Paul-Emmanuel Brun. "A Mixed-Interaction Critical Infrastructure Honey pot." *European Cyber Week CAESAR* (2020).

[15]. Nursetyo, Arif, Eko Hari Rachmawanto, and Christy Atika Sari. "Website and network security techniques against brute force attacks using honey pot." In *2019 Fourth International Conference on Informatics and Computing (ICIC)*, pp. 1-6. IEEE, 2019.

[16]. Kviesis, Armands, Vitalijs Komasilovs, Olvija Komasilova, and Aleksejs Zacepins. "Application of fuzzy logic for honey bee colony state detection based on temperature data." *Biosystems Engineering* 193 (2020): 90-100.

[17]. Udhani, Shreya, Alexander Withers, and Masooda Bashir. "Human vs bots: Detecting human attacks in a honey pot environment." In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-6. IEEE, 2019.

[18]. Karabulut, Berkcan, Muhammed Ali Aydin, and Abdul Halim Zaim. "An Application on Honey pot-Based Hybrid Deployment System: in the Turkish Software Industry." *BSEU Journal of Engineering Research and Technology* 1, no. 1 (2020): 24-30.

[19]. ParvathiP , Anuradha Chinta , S.R.Chandra Murthy Patnala,"Literature Survey for Efficient Method to Protect Honetpot Enabled IOT", The International Journal of Analytical and Experimental Modal Analysis, Volume XII, Issue 1,January 2020.

[20]. P.Parvathi, Anuradhachinta, Dr.P.S.R. Murthy" A Honey pot Implementation for security Enhancement in IOT system using AES and Keymanagement" ,Turkish Journal of Computer and Mathematis Education, Volume 12,April 2021.