DETECTION OF EXTERNAL INTERVENTIONS IN THE INTERNET OF THINGS

Namazov Asim TAHIR

Baku Higher Oil School, Azerbaijan, Baku

The importance of ensuring the security of Internet of Things (IoT) devices is just as crucial as accelerating the implementation process of IoT. Like other devices, IoT devices can be vulnerable to various types of attacks over the internet. To identify these attacks, attention should be paid to the system itself and the activity sequence of certain resources. This article discusses various types of security solutions for IoT devices. Additionally, a new solution is proposed to identify the potential impact of IoT devices. The experiments conducted using a Mikrotik router as a gateway have shown that it is possible to detect cyber attacks by monitoring the device's internal resources for various activities. Login attempts using different usernames recorded in the router's logs and the processor's jump activity were monitored to identify metrics indicating potential attacks based on increased sequential jumps. An algorithm was developed using these metrics, and a program was written in Python to detect cyber attack threats against the device.

Key words: *IoT*, gateway, attack, security

1. INTRODUCTION

The Internet of Things (IoT) refers to the management of everyday devices through various applications over the internet. As a result of connecting our daily-use items and household appliances to the global network, the terminology of the Internet of Things emerged. IoT is one of the fastest spreading and most current innovations in the world. This technology covers many application areas such as the automation of homes and various industrial fields, monitoring the environment, healthcare, etc. The expansion of this technology brings with it the benefit of easy access to the internet for everyone, as well as the use of limited numbers of special networks [1]. The main principle of IoT is to collect sensor data and transmit it to data centers over the internet. That is why special attention must be paid to security issues related to the Internet of Things.

By using global networks it is possible to transmit and receive information through devices over the internet. Many problems arise

regarding both control and management during the implementation of these processes. Several proposals have been made in various articles regarding these problems. Javier Carrillo-Mondejar and others [4] propose a module that checks the system for malicious software that has entered, configuration files, and symbols associated with them. With this module, it is possible to determine whether there have been any changes in symbols or files. Using this method, it is possible to detect the entry of malicious software into the system by comparing the current files with the original files. However, changes found in files using this module can result in the system being reverted back to its original configuration or reconfigured. This can cause the system to remain offline for a certain period during the recovery process. Additionally, if there is a delay during the comparison of files, the original files may also be damaged.

The volume of data generated by Internet of Things devices is significant. Big data and machine learning tools are used to analyze, protect, and manage this data. To facilitate these processes, prominent data centers have been established in various locations around the world. Examples of such data centers include Microsoft, Google, Amazon, and others. The architecture of the Internet of Internet of Things (IoT) devices generate a large volume of data, which requires the use of big data and machine learning tools to analyze, protect, and manage them. To accomplish this, data centers have been established in various parts of the world, such as Microsoft, Google, Amazon, etc., to ensure the security and storage of such data. The architecture of IoT consists of a large number of devices and various communication technologies that ensure the connection of these devices to provide services required by end-users. Users can manage their own information and household items by obtaining this information from data centers through special applications. Umar Ahsan and Abdul Bais [5] have divided the architecture of IoT into several layers. According to their research, each layer must be protected by different security protocols. The increasing amount of data collected by sensors and its storage in big data databases in upper layers emphasizes the need for implementing specific security protocols for each layer. It should be noted that many traditional security protocols, which were once considered secure, have lost their relevance and reliability. Therefore, currently reliable security protocols and encryption methods may become outdated in the future. Considering that encryption methods are applied between devices and data centers

when transmitting data, it can be concluded that implementing security measures in the latest technology and data centers is more appropriate.

The Internet of Things technology also finds its application in critical infrastructures. For instance, the automation of smart cities, smart villages, smart power grids, etc. utilizes the devices of the Internet of Things. Majid Moazzami, Mahdi Shaneh, and others [2] have discussed the concept of smart grids, especially smart power grids, and the existing security problems. Their proposed solution helps to reduce the risks that jeopardize the security of devices used in critical infrastructures. One of the systems proposed in the article is the immunology system, which can detect dangerous threats and pass them through filters. According to their idea, during a threat, this system can identify viruses in secure locations in advance. However, the crucial issue is that even a short time interval between the virus's entry into the system and its discovery can cause serious risks. There may be some movement during this interval, which can harm the system. Identifying and preventing viruses or other threats before they enter the system should be one of the main goals.

This article proposes possible solutions to prevent the harmful effects of the Internet of Things and attempts to prevent the interception of information.

2. INTERNET OF THINGS (IoT) NETWORK

The article examines the network of the Internet of Things and the gateway device that provides internet access to the devices connected to this network. Various examples have been taken from the experiment conducted on the device. As a result of these examples, the self-execution of some resources related to the structure of the Internet of Things during attacks has been discussed.

The Internet of Things devices mainly collect information through sensors. For example, security cameras capture images through motion sensors and transmit them to the central information system, and the heating or cooling system is regulated based on the information obtained by the temperature sensor about the condition of the room. The transmission and reception of information occurs over the network. It should be noted that these devices create connections with each other and share information through wired or wireless interfaces. Different types of cables are used to connect wired interfaces with each other. Short-

range radio waves are used for connecting wireless interfaces. This is one of the main factors for physically connecting devices to each other and exchanging information. Of course, it is necessary to use any software to create these connections. Through these programs, we can both configure and monitor devices. Based on all this information, the structure of the Internet of Things technology can be shown with the following (Figure 1) layers.

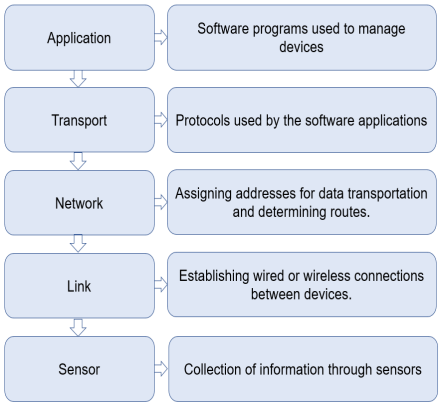

Fig. 1 Layers of Internet of Things network

3. THE REASON FOR BEING VULNERABLE TO ATTACKS IN THE INTERNET OF THINGS NETWORKS

When observing the integration methods and connections between devices, it can be seen that the devices are connected to the internet only through gateways. Internet gateways are used to transmit the collected data from devices to the global network. Each device's local connection with gateways implies that they have at least one IP (Internet Protocol) address. Based on the topology shown in Figure 2, it should be noted that gateways play a fundamental role for each device used in smart solutions.

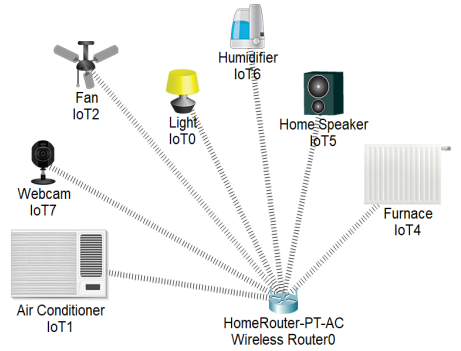

Fig.2 IoT connectivity scheme

From this, it can be seen that the main role of gateways is to transmit collected data over the internet or to gain access to devices over the internet. Therefore, it is possible to access and manage devices through gateways. For this reason, it is essential to control and monitor the external inputs of gateways.

Huichen Lin and Neil W. Bergmann have identified various vulnerabilities in security cameras through device search systems [3]. They have determined these

vulnerabilities by gaining access to security cameras through conventional protocols. To prevent such vulnerabilities, they emphasize the need for security measures to be taken for each layer of the Internet of Things architecture. They have also included a gateway architecture in their proposed architecture, especially highlighting the centralization of device registration and access through gateways. In the article, the gateway is not only considered as a means of establishing a connection between things and the internet, but also as a protective device. To act as a protective device, conventional secure protocols should be used through gateways. While it is possible to protect the network using these protocols, in some cases, attacks can still damage devices. The main purpose of the research in this article is to prevent successful or unsuccessful attempts to harm devices.

4. STATEMENT OF THE PROBLEM AND PROPOSED SOLUTION

As a result, the issue of detecting cyberattacks against the system based on the evaluation of the current activities of the Internet of Things has been raised. For simplicity, let's consider the issue in the context of a single object. Since the principles of operation of the Internet of Things are the same, the approach below can also be applied to the establishment of a protection system against cyber attacks for other objects.

Let's consider the Wi-Fi router, which is the main device responsible for connecting smart home devices to the internet, and plays the role of a gateway in the architecture of the connected home. We will take the Mikrotik router as an experimental object. The configuration, processor, and logs of the Mikrotik router have been analyzed.

For this purpose, let's first look at the performance indicators of the router during normal operation. As a rule, various jumps are observed at different time intervals on the graphics display of the router's processor. The jumps can increase or decrease depending on the traffic load, and such cases are evaluated as normal. Thus, the jumps observed with such sudden increases and decreases in the system's traffic load are considered normal activity according to the standard regulation and are not related to the device being under attack. Figure 3 shows

the processor indicators of the router during normal traffic load. It would be appropriate to rank and explain them over time.

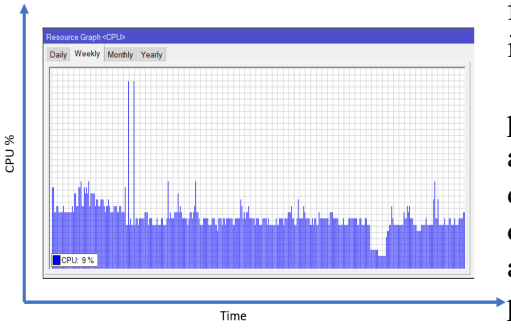

Fig. 3 Mikrotik Router Processor Metric

During the analysis of the log files, the observation of normal procedures and combinations was also carried out (Figure 4). It can be seen from here that the device has not been subjected to any external attacks.

Fig. 4 Mikrotik router's log file indicating no attempted attacks.

Based on the indicators presented in Figures 3 and 4, it can be determined that there is no threat of attack observed on the device. This can be explained by the absence of any attempts to access the device from outside and the consecutive increase in processor load.

To investigate the process of a potential attack, a simulation of an attack process was carried out on the device. Different patterns were observed in the logs and processor activity during the simulated attack process. The log information for the attack simulation is provided in Figure 5. From the logs, it is clear that there were login attempts under user names such as "admin" and "supervisor" at intervals of 1 or 2 seconds.

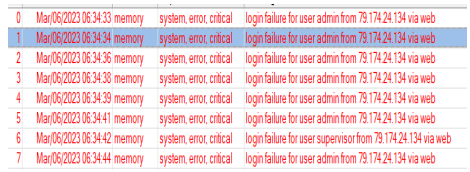

Fig. 5 Log indicators of attack attempts on the Mikrotik router

Based on the observed activity, the management system can suspect the possibility of a threat and take various measures to protect the device. In the case being examined, the main resource is considered to be the processor, since the processor's overload can cause other processes to slow down or stop. At the same time, based on the processor's load spikes, it is possible to determine the

extent to which the attack is continuous and dangerous.

As mentioned earlier, even during normal traffic loads, there can be various spikes. The first spike can be explained by normal traffic load. However, the consecutive second spike can be considered as a possibility of an attack. But the spikes that continue with increasing frequency, starting from the third spike, should be interpreted as a significant threat of an attack. As a result of the conducted experiment, the spikes observed in the processor due to the simple attacks performed on the MikroTik router are provided below (Figure 6).

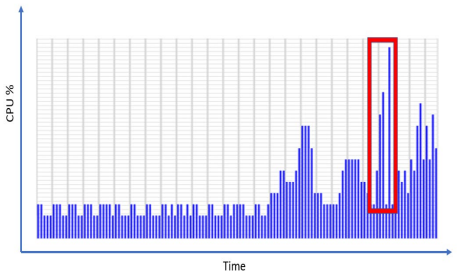

Fig. 6 Processor Load during Attack on MikroTik Router

As seen from Figure 6, during the attack, there is a short-term sequence of increasing spikes in processor activity. These spikes represent, for example, 11% at the 1st second, 13% at the 2nd second, 17% at the 3rd second, and 25% at the 4th second of the attack. For clarity, the graph of the dynamics of the changing indicators depending on time can be constructed as shown in the following Figure 7.

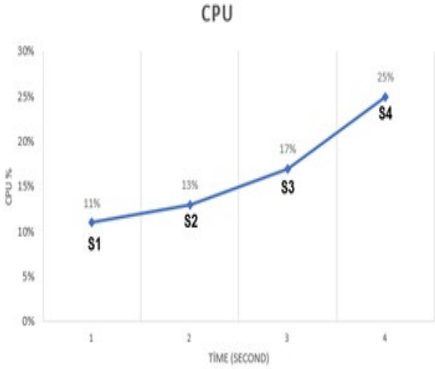

Fig. 7 Graphical representation of the device's processor load during the attack

Based on the above information, let's formalize the measure for detecting a hacking attempt based on processor usage data.

Let's denote the maximum value of the monitored indicator in normal operation as S_o. For the purpose of determining a hacking attempt, let's consider the moments of recording the indicator during the monitoring process as $t_i, i = 1, 2, 3, \ldots$ and let S_i represent the value of the indicator at time t_i. It is evident that if an attempt has occurred at a certain t_i, then the condition $S_i > S_0$ must be satisfied. However, as mentioned above, this condition can also occur due to random fluctuations. To identify a ongoing hacking event, the values of S_i at observation moments $t_{i+k}, k = 1, 2, 3, \ldots$ which are not too

far apart in time, should be analyzed. For this purpose, at certain time intervals, the values of S_{i_k} at t_{i_k} $t_{i_k}, k = 1,2,3,4$ should be examined in such a way that the following conditions (1) and (2) are met:

$$S_{i_k} > S_0\,, \tag{1}$$

$$t_{i_4} - t_{i_1} < 8\,. \tag{2}$$

Based on numerous experiments, it has been shown that the difference between $S_{i_{k+1}} - S_{i_k}$ for $k = 1,2,3$ increases monotonically with a certain proportionality factor α. If we denote the proportionality factor by α, the indicator for a potential attack can be formulated as follows:

$$S_{i_{k+1}} - S_{i_k} \geq \alpha \cdot \left(S_{i_k} - S_{i_{k-1}}\right), \tag{3}$$

The note states that conducted experiments show that the difference values increase twice during an attack, in other words,

$$\alpha \approx 2. \tag{4}$$

Thus, to determine the attack risk based on the processor's loading activity, the following rules can be given in accordance with relations (1)-(4).

Rule 1 - If there are 1 or 2 jumps in the processor per 1 second interval, this should be considered as a normal jump.

Rule 2 - If there are 3 jumps in a 1 second interval, these jumps should be considered suspicious, and the occurrence of the 4th jump should be monitored with probability.

Rule 3 - If 4 jumps occur in a 1 second interval, this should be evaluated as an attack risk and calculations should be performed to determine whether there has been an intensive increase between the jumps.

Rule 4 - If the difference between the 4th jump and the 3rd jump is twice as large as the difference between the 3rd and the 2nd jump, and the difference between the 3rd and the 2nd jump is twice as large as the difference between the 2nd and the 1st jump, then it is verified that an attack has occurred on the device.

Based on these rules, a program has been developed in the Python programming language, tested with appropriate tests, and yielded positive results. Below is an example of the program code:

```
import psutil
import time
# Define function to check for CPU spikes
def check_cpu_spike():
    # Get CPU usage for first second
    cpu_usage1 = psutil.cpu_percent(interval=1)
    # Get CPU usage for second second
    cpu_usage2 = psutil.cpu_percent(interval=1)
    # Get CPU usage for third second
    cpu_usage3 = psutil.cpu_percent(interval=1)
    # Get CPU usage for fourth second
    cpu_usage4 = psutil.cpu_percent(interval=1)
    # Check if there was a spike between first and second seconds
    spike1 = cpu_usage2 - cpu_usage1
    # Check if there was a spike between second and third seconds
    spike2 = cpu_usage3 - cpu_usage2
    # Check if there was a spike between second and fourth seconds
    spike3 = cpu_usage4 - cpu_usage3
    # If the second spike is twice as large as the first spike, print "there
was a change"
    if spike2 >= 2*spike1:
        print("there was a change")
    # If the third spike is twice as large as the second spike, print "there
an attack"
    if spike3 >= 2*spike2:
        print("there was an attack")
# Call function to check for CPU spikes
check_cpu_spike()
```

5. CONCLUSION

As a result of experiments conducted with a Mikrotik router acting as a gateway, it has been determined that it is possible to detect a cyber attack by monitoring the device's internal resources for various activities. To this end, login attempts with various user names identified in the Mikrotik router's logs, as well as the processor's jump activity, have been monitored. Metrics indicating when increasing sequential jumps are related to attempted attacks have been identified based on the observed indicators. An algorithm has been developed based on these metrics, and a program has been written in

the Python programming language and tested to detect cyber attack threats against the device.

REFERENCES

[1] R.M. Əliquliyev, R.Ş. Mahmudov. 2011, №2(4). *Əşyaların İnterneti: mahiyyəti, imkanları və problemləri, İnformasiya cəmiyyəti problemləri,* s.29-40.

[2] Majid Moazzami, Mahdi Shaneh, Zahra Davoody-Beni, Hossein Shahinzadeh, Niloufar Sheini-Shahvand, Gevork B. Gharehpetian. 18-19 December 2019. *"Application of IoT in Smart Grid: Challenges and Solutions"* 5th Conference on Signal Processing and Intelligent Systems, , Shahrood University of Technology.

[3] H. Lin and N. Bergmann. 2016. *"IoT privacy and security challenges for smart home environments*," Information, vol. 7, no. 3, p. 44.

[4] Javier Carrillo-Mondejar , Juan Manuel Castelo Gomez, Carlos Nu´ñez-Go´mez, Jose Rolda´n Go´mez, and Jose´ Luis Martı´nez. 2020. *"Automatic Analysis Architecture of IoT Malware Samples"* Security and Communication Networks Volume, Article ID 8810708.

[5] Umar Ahsan, Abdul Bais. 2016. *"A Review on Big Data Analysis and Internet of Things"* IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems. p. 325-330.