International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.065 ISSN: 2581-4621

A case study on conventional security practices v/s AI-powered approaches in Internet of Things

Cicy V Abraham[1], Indhuchoodan R[2] , Nikhil T. Das[3] , Cina Mathew[4]
[1,2,3] UG- Kristu Jyoti College of Management and Technology,Changanassery, Kerala
[4]Assistant Professor- Kristu Jyoti College of Management and Technology,Changanassery, Kerala

ABSTRACT

The internet of things (IoT) is an advancement that can change the way that we live, in regions going from transport to prosperity, from redirection to our associations with government. The usage of the IoT has extended decisively, and network insurance concerns have extended close by it. IoT systems might perhaps increase effectiveness, obligation, detectability, and efficiency. The extreme front line of organization assurance is Artificial Intelligence (AI), which is used to improve bewildering computations to shield associations and structures, including IoT systems. As to security, the IoT will be gone up against extra outrageous troubles. In this paper, we discuss the conventional security methods and the role of artificial intelligence in governing security in the Internet of things.

Keywords—Internet of things, AI, security

1. Introduction

A cyber threat is associated with identifying fraud, intended extortion, and loss of critical information such as family photographs. In today's interconnected culture, everybody profits from innovative data security strategies. Cyber threat relates to the body of techniques, procedures, and strategies designed to avoid malicious access to systems, computers, and software. In the course of business operations, companies transfer classified information through networks and to various machines and cyber safety encompasses the practice devoted to securing that data and the devices used to analyze and manage that content. When the frequency and complexity of cyber-threats increase, businesses, and organizations, particularly those dealing with data protection associated with nationwide protection, healthcare, or banking data, need to intervene to safeguard their classified company and personal records.

- **Methodology of message transferring in IOT**

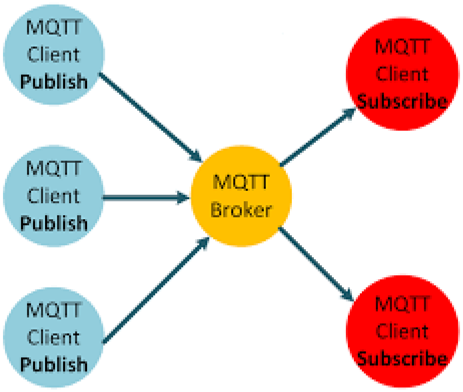

Fig 1. MQTT protocol in transferring messages

MQTT is the most commonly used messaging protocol for the Internet of Things (IoT). MQTT stands for MQ Telemetry Transport. The protocol is a set of rules that defines how IoT devices can publish and subscribe to data over the Internet. MQTT is used for messaging and data exchange between IoT and industrial IoT (IIoT) devices, such as embedded devices, sensors, industrial PLCs, etc. The connection between them is handled by the MQTT broker. The two important names in MQTT are the publisher and subscriber. Both publishers and subscribers are MQTT clients. The publisher and subscriber labels refer to whether the client is currently publishing messages or subscribed to receive messages (publish and subscribe functionality can also be implemented in the same MQTT client). An MQTT client is any device (from a microcontroller up to a full-fledged server) that runs an MQTT library and connects to an MQTT broker over a network. The client implementation of the MQTT protocol is very straightforward and streamlined. MQTT client libraries are available for a huge variety of programming languages.

2.Conventional security threats

2.1 Man in the middle attack

One of the most popular attacks on IoTs is Man-in-the-Middle (MITM) attack. With regards to computers in general, a MITM attack intercepts communication between two nodes and allows the attacker to take the role of a proxy. Attackers can perform MITM attacks between many different connections such as a computer and a router, two cell phones, and, most commonly, a server and a client.The most well-known casualties of MITM assaults are web assets that work with a lot of information: sites of monetary associations, SaaS assets, internet business locales, and different administrations that require online approval. The figure shows a basic example of a MITM attack between a client and a server. In regards to IoT, the attacker usually performs MITM attacks between an IoT device and the application with which it interfaces. There are two common modes of MITM attacks: cloud polling and direct connection. In cloud polling, the smart home device is in constant communication with the cloud, usually to look for firmware updates.

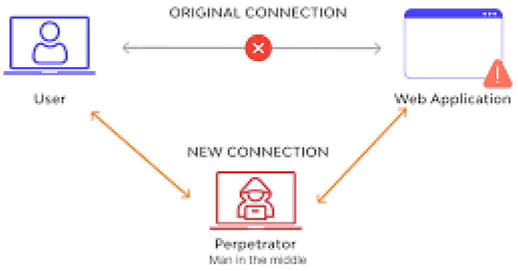

Fig. 2 Man in the middle attack

2.2 Denial of Service(DOS)

IoT devices may often carry out DoS attacks, but they themselves are susceptible to them as well. IoT devices are particularly susceptible to permanent denial of service (PDOS) attacks that render a device or system completely inoperable. This can be done by overloading the battery or power systems or, more popularly, firmware attacks. In a firmware attack, the attacker may use vulnerabilities to replace a device's basic software (usually its operating system) with a corrupted or defective version of the software, rendering it useless. The attacks on the device's power system, though less popular, are possibly even more devastating. One example of this type of attack is a USB device with malware loaded on it that, when plugged into a computer, overuses the device's power to the point that the hardware of the device is rendered completely ruined and needs to be replaced.DoS assaults can run in span and may target more than each site or framework in turn. An assault turns into a 'circulated disavowal of administration', alluded to as "DDoS", when it comes from numerous PCs (or vectors) rather than only one. This is the most well-known type of DoS assault on sites. One example of PDoS malware is known as BrickerBot. BrickerBot uses brute force dictionary attacks to gain access to IoT devices and, once logged in to the device, runs a series of commands that result in permanent damage to the device. This attack is devastating enough that it often requires reinstallation of hardware or complete replacement of the device. Interestingly enough, BrickerBot was designed to target the same devices the Mirai botnet targets and would employ as bots, and uses the same or a similar dictionary to make its brute force attacks. Due to the structure of IoT systems, there are multiple attack surfaces, but the most popular way of attacking IoT systems is through their connections as these tend to be the weakest links. In the future, it is advisable that IoT developers ensure that their products have strong protections against such attacks, and the introduction of IoT security standards would prevent users from unknowingly purchasing products that are insecure.

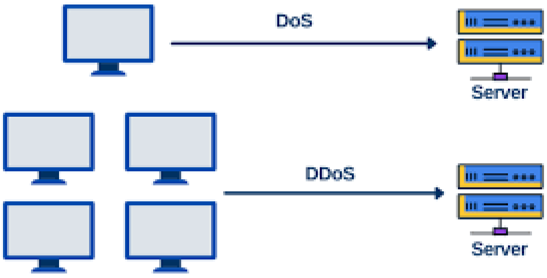

fig.3 Example of DOS attack

2.3 Brute force attack

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly. These attacks are done by 'brute force' meaning they use excessive forceful attempts to try and 'force' their way into your private account. This is an old attack method, but it's still effective and popular with hackers. Because depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years.

3.Methods of Artificial Intelligence application in Internet of Things

3.1 Dataset Description

Studies have tested systems using a wide range of dataset formats. The UNSW, Canberra, generated a number of datasets that were used for this investigation; the one we used in this experiment was a dataset called the BoT-IoT. This was created by building a protective system at the UNSW Canberra Cyber Center's Cyber Range Laboratory. Botnets and regular traffic were used to create the environment. Various file types, including original files with a.pcap extension and comma separated values (CSV) files, were supplied as data sources. Programs like Wireshark typically employ pcap files to store data packets on a network. This file is typically used to examine network data properties.

3.2 Convolutional neural network

Reduce the information parameters used in an artificial neural network using CNNs (ANN). A CNN has several hidden layers in addition to input and output layers.Through the use of equivariant representation, parameter sharing, and a trio of minimal exchanges. Increasing the training duration by reducing associations between the layers increases a CNN's scalability and degree of difficulty.

CONCLUSION

With the assistance of sensors, the IoT can gather, dissect and send a tremendous measure of information which thusly will be changed over into significant data and information that can be utilized to make new applications and administrations to work on our personal satisfaction. Security and protection are viewed as significant issues in the IoT framework.Giving a solid and protection saving IoT framework ought to be a mandatory errand to proceed with its fruitful improvements in our current circumstance.As the number and speed of assaults develop, specialists are going to AI for the purpose of safeguarding these frameworks shrewdly and continuously. Obviously, aggressors track down ways of foiling these AI and may try and utilize AI to go after frameworks.

References

1. Neha G. Relan and Prof. Dharmaraj R. Patil. "Implementation of Network Intrusion Detection System using Variant of Decision Tree Algorithm." In International Conference on Nascent Technologies in the Engineering Field (ICNTE), pp. 4799-7263. IEEE, 2015.

2. Murat Kuzlu, Corinne Fair and Ozgur Guler. "Role of Artifcial Intelligence in the Internet of Things (IoT) Cybersecurity"

3. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. "IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices". IEEE Internet Things J. 2019;6(5):8182–201

4. Radanliev P, De Roure DC, Nurse JR, Montalvo RM, Cannady S, Santos O, Burnap P, Maple C. "Future developments in standardisation of cyber risk in the Internet of Things (IoT)". SN Appl Sci. 2020;2(2):169.

5. Evans D. The Internet of Things: how the following advancement of the web is making a huge difference. Cisco Internet Business Solutions Group: Cisco; 2011.

6. Roopak M, Yun Tian G, Chambers J. Models profound learning, for digital protection in IoT organizations. In: IEEE ninth yearly figuring and communica-tion studio and meeting (CCWC), Las Vegas, NV, USA. 2019;2019:0452-7.

7. Vorakulpipat C, Rattanalerdnusorn E, Thaenkaew P, Hai HD. Late difficulties, patterns, and concerns connected with IoT security: aan transformative review. In: 2018 twentieth global gathering on cutting edge correspondence innovation (ICACT), Chuncheon-si Gangwon-do, Korea (South); 2018. p. 405-10.

8. Chuncheon-si Gangwon-do, Korea (South); 2018. p. 405-10.22. Atlam, H.F., Alenezi, A., Alharthi, A., Walters, R., Wills, G.B.: Integration of distributed computing with web of things: difficulties and open issues. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), no. June, pp. 670-675 (2017).

9. Atlam, H.F., Alenezi, A., Walters, R.J., Wills, G.B., Daniel, J.: Developing a versatile Risk-based admittance control model for the Internet of Things. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), no. June, pp. 655-661 (2017).

10. Shanbhag, R., Shankarmani, R.: Architecture for web of things to limit human between vention. In: 2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015, pp. 2348-2353 (2015).

12. Iqbal, M.A., Olaleye, O.G., Bayoumi, M.A.: A survey on web of things (IoT): security and protection prerequisites and the arrangement draws near. Worldwide J. Comput. Sci. Technol.: E Network, Web and Secur. 16(7) (2016).