IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

An Analysis for the Use of Artificial Intelligence with Internet of Things in Cyber Security

Anu Sharma, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- er.anusharma18@gmail.com

ABSTRACT: ***The Internet of Things (IoT) has seen explosive growth in usage in recent years, and with that the, so have doubts about cyber-security. Artificial intelligence (AI) is at the center of cyber-security and can be used to create intricate algorithms that defend networks and systems, including IoT technologies. However, fraudsters have learned how to take benefit of this information and have even begun using aggressive AI to assault cyber-security. The adoption of block chain technology in smart cities is affected by security issues and challenges, which are thoroughly discussed in this study. In order to create a sustainable smart community, a number of critical factors for the fusion of AI technologies are discussed in great detail in this book. The essential ideas that can be applied to the creation of AI-based autonomous transportation systems are summarized in our discussion on AI security improvement solutions. We also talk about the unresolved problems and the direction of our additional investigation, which includes new previous research identified and standards for a long-term urban planning ecosystem.***

KEYWORDS: ***Attacks, Cyber Security, Internet of Things, Software, Artificial Intelligence, systems.***

1. INTRODUCTION

The Internet of Things (IoT) [1] was established in 2008, and ever since then, it has seen significant increase. Today, IoT is omnipresent and found in many homes and enterprises. IoT is difficult to explain even though it has changed and evolved since it was first conceived, but it is best defined as a networking of digital and analogue machinery and computer systems that have been given unique IDs and are capable of sending and receiving data without the intervention of a person [2]. Most often, this appears in the form of a person interacting with a centralized repository system or software, which is frequently a mobile application, before sending directions and information to one or more peripheral IoT devices. If necessary, the perimeter devices may carry out tasks and transmit information back to the gateway device or application so that a people can examine it.

The IoT concept has given the world a better level of accessibility, integrity, availability, scalability, secrecy, and interoperability in terms of device connection. IoTs are vulnerable to cyber-attacks because to their many potential weaknesses, lack of security standards and benchmarks, and newness [3]. Attackers may use a variety of cyber-attacks against IoTs, depending on the aspect of the system they are targeting and what they want to achieve from either the attack. As a consequence, a lot of research has been done on IoT cyber security. This entails using deep learning architectures to protect IoT devices from attackers, who often only appear as odd behaviours that would indicate an operation is underway. IoT devices must be protected from

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

a variety of threats, but attackers always have a chance since it only takes one security hole for them to succeed [4]. Because of this, cyberattacks are increasingly using AI to get around effective algorithms that spot odd behaviour and allow it to go unnoticed. With the development of intelligent technologies, AI has attracted considerable attention. AI has gotten a lot of attention as intelligent technology have developed.

With this development, AI techniques have been employed in IoT cyber security programs to be able to recognize dangers and probable assaults. These technologies include classification trees, regression models, machine learning, supported vector machines, and neural networks. Technological devices are compared in terms of integrity, privacy and confidentiality, data protection, privacy, access control, digital signatures, authorization, resilience, and self-organization by the novelists of, who also provide a comprehensive examination of the security dangers associated with IoT applications and possible future countermeasures the authors provide deep learning algorithms that provides excellent accuracy 96.17% or detecting DDoS attacks for IoT (Internet of Things) cyber-security using CICIDS2017 datasets [3]. In exchange for being able to identify inconsistencies in the data supplied from the edge devices, the study investigated Artificial-Neural-Networks (ANN) in a gateway device.

The study demonstrates that the proposed technique may enhance IoT system security. For the observation and estimate of cyber-attacks in corporate IoT systems as well as indemnification for them, the writers in provide an AI-based control scheme is proposed. The authors make a number of malicious examples and security protocols against IoT environments, as well as a reliable comprehensive detection method [4]. They also test our technique using datasets include MNIST, CIFAR-10, and SVHN. The writers investigate the different applications of the increasing integration of IoT devices in such systems has led researchers to examine the development of AI decision-making in cyber-physical systems and find that this evolution is basically really autonomous. Additionally, they draw the conclusion that this shift is likely to be unavoidable owing to the importance of AI decision-making due to its speed and efficiency in managing large volumes of data. [5].

2. DISCUSSION

The author discusses about advanced solutions for pre-determined categories that making use of AI and machine learning, especially in IoT networks seen in industrial settings. Finally, in order to standardise such processes and increase the efficacy of risk detection and protection, analyses approaches for collecting and analysing network security risks to IoT devices. This article explores a variety of topics relating to cyber-security, the Internet of Things (IoT), artificial intelligence (AI), and how much they all relate to one another in three survey-style parts. Along with offering a complete study of cyberattacks on IoT devices, it also recommends AI-based defences [8]. The main goal of this article is to serve as a resource for anyone researching these current challenges by summarising and linking key works that cover different angles of all these subjects.

2.1. Attacking IoT Devices:

Because many IoT devices lack proper security, cybercriminals have developed a variety of strategies to target IoT devices from a variety of attack surfaces [9]. The hardware and software of the IoT device itself, the networks to which it may connect, and the application in which it interacts

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

are the three attack interfaces that are most often used. These three elements work together to form the core parts of an IoT system. Figure 1 depicts a basic overview of a multiple IoT system. The bulk of attacks similar to those mentioned in this study occur at access point and data storage server connections since these are virtually always the weakest spots in IoT security. [6].

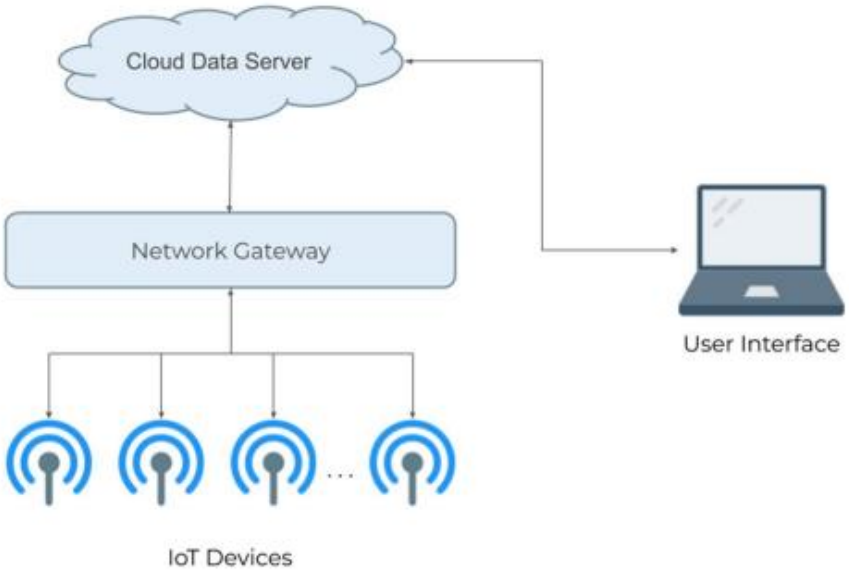

Figure 1: Illustrates that the IoT gadget interface with the cloud [Google].

1.1. Initial-Reconnaissance:

Before attempting to hack an IoT device, IoT attackers often analyse their targets to identify issues. This is often done by first buying a similar IoT device off the market. Then they use reverse engineering to build a test attack in order to look at each device's outputs and attack possibilities [11]. Some examples of this include disassembling the gadget and investigating the hardware and software, such as the micros card, to learn more about the programme, and playing with the electronics to uncover private information or cause unexpected behaviour. For IoT devices to be protected against reverse engineering, hardware-based security is necessary. The implementation processor, which cause potential, actuators, a battery charger, and connection, will have to be installed in a setting that is impenetrable to tampering. Hardware-based encryption may also be used for authentication mechanism, enabling the device to verify its authenticity to the server with which it is associated [7].

1.2. Physical Attack:

Violent attacks, where the hardware of something like the target device is leveraged in some fashion to the attacker's advantage, are also an often low-tech sort of attack subcategory. Different types of physical attacks exist. This would include attacks like service disruptions, in which the devices' connection toward the network is cut off to start interfering with their operations; severe trauma, in which the equipment or their parts are harmed to help stop proper functionality; malicious payload injection, in which the attacker needs to be plugged a USB comprising a malicious software into the victim machine; and object jamming, inside which signal jammers are

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

accustomed inhibit or interfere with the transmissions the targets' devices emit. Physical operations may be used to carry out continuous dissent of service attacks, which have been covered late inside this work. For instance, if an IoT device is linked to something like a high voltage electricity source, its electricity supply could get overburdened and need to be changed [8].

1.3. Man-in-the-Middle:

Man-in-the-Middle attacks are some of the most common IoT cyberattacks. In terms of computers in principle, an MITM attack enables that attacker to act as a proxy by eavesdropping interactions between different nodes. Attackers have access to many different communications, including those here between computer and just a router, two handheld platforms, and, most often, a servers and a client [9]. When it connected via the Internet of Things, the attacker often undertakes MITM assaults between an Electronic gateway and the application it connects with. Because they lack the common implementations to mitigate against the assaults, IoT devices throughout particular likely to be more exposed to MITM attacks. MITM problems usually use either cloud polling or direct line. The smart home equipment constantly communicates with the internet while cloud polling, often to monitor for custom firmware. Figure 2 illustrated client server connection.

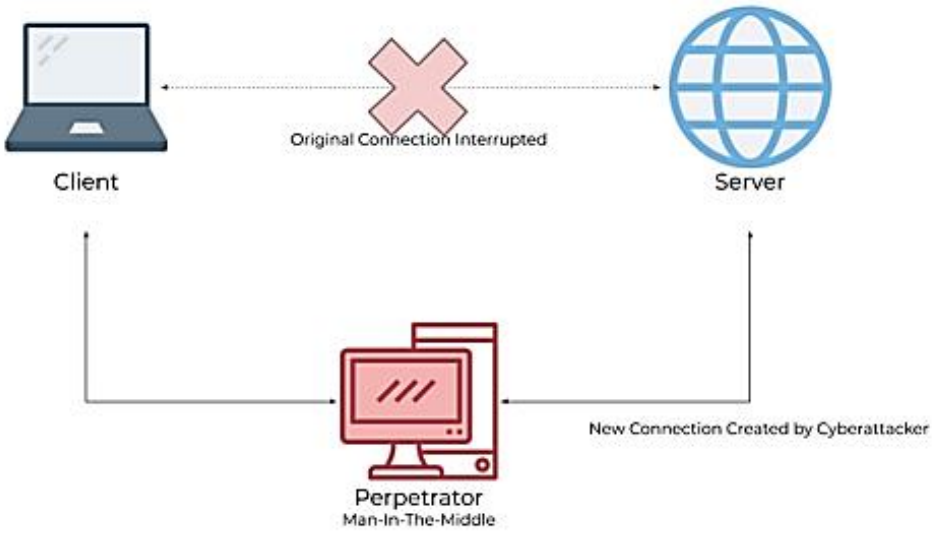

Figure 2: Illustrated client server connection [Google].

Attackers have the potential to reroute traffic on the network using the ARP (Address Resolution Protocol) poisoning techniques or by modifying DNS (Domain Name System) configurations. Using techniques like the Secure Sockets Layer (SSL) SSL strip or self-signed accreditations, they may also eavesdrop on HTTPS communication. [10]. The self-signed certificate approach is particularly successful since many connected devices do not check the validity or sense of confidence of certificates. Obvious connections allow for communication systems and a hub or applications on the same network. This allows smartphone apps to search every Internet address on the local network for that same port in order to identify new devices. The same procedure could be used by an attacker to find network devices. An example of an MITM IoT attack is a smart refrigerator that may display the user's Google calendar. And though it looks like a good notion,

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

attackers revealed that the software did not verify SSL certificates, which gives an opportunity to launch an MITM attack and obtain the participant's Google username and password.

The goal of this review is to explore the viability of deploying the unstaffed offline retail style. We do this by proposing any intelligent IoT-based and AI-based retail shop design. Based on a data set of 11, 000 pictures in various configurations that include 10 different types of stock keeping unit (SKU), an end-to-end classifications model trained using the MASK-RCNN technique is created for SKU counting and categorization. The approach we recommended does away with character segmentation, which eliminates the inaccuracy that character segmentation produces. This technique provides exceptional counting precision and good recognition accuracy on the test dataset, according to the experiment findings throughout this paper. We will concentrate on strengthening algorithm effectiveness and recognizing rate, lowering number of false positives, and setting up a greater picture data set for more SKU in our forthcoming work.

3. CONCLUSION

There are frequent attacks against IoT systems since of their multiple attack surfaces, and as IoT has become more and more widespread, more has been found. Systems must always be shielded from these attackers as effectively as feasible. As the amount and frequency of attacks rise, experts are turning to AI as a way to protect these systems logically and in real-time. Of course, hackers also used to undermine these AI and might use AI to attack systems. This article describes common methods was using to try to infiltrate or disrupt IoT it gives a general explanation of how these assaults are carried out. Illustrations are also given when required to further explain these arguments. The applications of a range of AI algorithms in cyber security are then investigated. These models are quite often in the process of being developed or are still challenging to execute, making them unique since they are not yet widely used in commercial products. Furthermore, the models shown motivated to participate and might rapidly spread to other threat detection systems. In the context of IoT systems, procedures of countering AI threat and countering AI attacker are also considered. As IoT systems expand, these cyber-attack will become an emerging concern, especially as humongous networks like smart cities laboratory activity with them. Not only are humongous networks more difficult to guarantee since they have so many attack surfaces, AI should be more or less fault-tolerant, yet everyday life and safety rely on them. The issues raised in this article are then reiterated in a chart along with traditional or recommended defenses against further attacks.

REFERENCES:

[1] A. Deshpande, P. Pitale, and S. Sanap, “Industrial Automation using Internet of Things (IOT),” *Int. J. Adv. Res. Comput. Eng. Technol.*, 2016.

[2] H. K. and D. D., “Industrial Automation using IoT with Raspberry Pi,” *Int. J. Comput. Appl.*, 2017, doi: 10.5120/ijca2017914277.

[3] M. Chiang and T. Zhang, “Fog and IoT: An Overview of Research Opportunities,” *IEEE Internet of Things Journal*. 2016. doi: 10.1109/JIOT.2016.2584538.

[4] P. R. Newswire, “Global Internet of Things (IoT) Industry,” *LON-REPORTBUYER*. 2016.

[5] F. Alam, R. Mehmood, I. Katib, and A. Albeshri, “Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT),” in *Procedia Computer Science*, 2016. doi: 10.1016/j.procs.2016.09.068.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 5, May 2022

[6] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," in *2016 14th Annual Conference on Privacy, Security and Trust, PST 2016*, 2016. doi: 10.1109/PST.2016.7906930.

[7] T. Foradis and K. Thramboulidis, "From Mechatronic Components to Industrial Automation Things: An IoT Model for Cyber-Physical Manufacturing Systems," *J. Softw. Eng. Appl.*, 2017, doi: 10.4236/jsea.2017.108040.

[8] F. Christoulakis and K. Thramboulidis, "IoT-based integration of IEC 61131 industrial automation systems: The case of UML4IoT," in *IEEE International Symposium on Industrial Electronics*, 2016. doi: 10.1109/ISIE.2016.7744911.

[9] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Communications Surveys and Tutorials*. 2016. doi: 10.1109/COMST.2016.2548426.

[10] Z. Dong, R. Espejo, Y. Wan, and W. Zhuang, "Detecting and locating man-in-the-middle attacks in fixed wireless networks," *J. Comput. Inf. Technol.*, 2015, doi: 10.2498/cit.1002530.