e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

IOT THREATS & IMPLEMENTATION OF AI/ML TO ADDRESS EMERGING CYBER SECURITY ISSUES IN IOT WITH CLOUD COMPUTING

Avinash Ganne*1

*1Sr. SAP Basis Cloud Architect, Raley's, Sacramento, California, USA.

DOI : https://www.doi.org/10.56726/IRJMETS32866

ABSTRACT

The Internet of Things (IoT) has emerged as one of the most innovative and forward-thinking technologies, attracting interest from both the scientific community and the commercial community due to its financial allure. Artificial intelligence/machine learning (AI/ML) is required to deconstruct the data saved in the cloud framework in order to integrate various devices and associate gadgets with people. These IoT devices communicate with one another and exchange data utilizing the web and cloud-based network architecture by using their individual unique identities and the integrated sensor in each device. We are in a big data era where using AI/ML is essential to the cycle of swiftly and accurately analyzing the obtained cloud-based large data. IoT security issues include substantial challenges and risks, including hacking, data fraud, remote access, and cyberattacks. Despite the fact that AI is increasingly playing a larger role in the development of traditional cyber security, both cloud vulnerability and the networking of IoT devices pose serious risks. IoT devices that are not sufficiently protected run the danger of being used in DDoS (Distributed Denial of Service) attacks. These assaults reveal security flaws and interrupt services, which have a severe impact on customer satisfaction and economic output. Additionally, the great majority of IoT devices that are connected remotely and transported by a public entity are always in cyber danger. Because it is hard for humans to manage the network, AI and ML are advantageous and essential to our foreseeable networks. The above-mentioned issues in IoT security need the use of AI/ML as a security tool. The suggested approach to cloud network infrastructure security problems uses predictive analysis to foresee potential assaults. This research then develops the appropriate AI/ML application using 3GPP, MIMO, and datasets from CIADA and Packet. A more practical Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are the results of the use of AI components, which have been crucial and utilized.

Keywords: IoT, Cloud Computing, Artificial Intelligence.

I. INTRODUCTION

Cloud computing has been most popular research domain from past two decades[1, 2]. A cyber security event known as a data breach occurs when a hostile agent acquires unauthorized access to personal information. Data that is private and mostly secret is stolen as a result of this assault. Although data breach assaults can take many different forms and strategies, the end outcome is nearly always the same. Our data can be seen and, in most situations, stolen by individuals or groups that do not have access to it.[3, 4] It alludes to the methods, procedures, and technologies used to safeguard data assets from nefarious actors. Information security as we know it now has been upgraded by cybersecurity. Security is not seen by InfoSec as a consumer or national security issue but rather as a corporate one. Three fundamental components make up cybersecurity: people, procedure, and technology. Even though they are ostensibly the victims of a government corporation or institution, almost all cyberattacks target specific individuals. Hackers steal personal data or cause havoc in people's life. Therefore, individuals need to be informed of how they can lessen and prevent risks. Organizations must create procedures and rules that lessen risks. They must adjust to the evolving cybersecurity environment. Regulations fall within this umbrella. Data breach notification laws and the General Data Protection Regulation (GDPR) regulation both work to safeguard people and organizations from cyber-attacks.[5] Technologies that shield users and businesses against cyberattacks are needed. Defenders should employ technology in the same ways that attackers do, including firewalls, encryption, intrusion detection, and other tools. Industrial sensors are an example of an IoT device that is subject to numerous cyber risks, such as hackers who seize control of the device as part of a DDoS assault and obtain unauthorized access to the data the device collects. Due to their sheer quantity, widespread geographic dispersion, and sometimes out-of-date operating systems, IoT devices are the main target of malicious agents. A data breach is the intentional stealing

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

of information[6]. Data breaches can be caused by criminal activity (such as identity theft), malicious intent (like Edward Snowden or hacking DNCs), or espionage. Cybersecurity dangers include data breaches, spear phishing, and infrastructure infiltrations.

II. PREMIERS

This section will cover background information of data beach, spear phishing and other related issues.

Data Breach

There have been several widespread and highly disruptive data breaches in recent years. It destroys public trust in well-known brands and public institutions and threatens to harass millions of consumers, the victims of fraud. Data breach protection is improving, although much remains to protect data from unauthorized and unlawful security breaches.

Spear Phishing

One method of data source assault that does not involve an actual attack is through cyber threats. It resembles a strategy of assault. Currently, there are hundreds of millions of cyber dangers, which may be broken down into the following categories.

Identifying vulnerabilities

Software that performs harmful operations on a device or network, such as erasing data or controlling a system. A gadget has harmful software that is the virus. Once installed, a virus has the ability to have a variety of negative effects, such as system blockage, data theft, or even device hijacking for illegal activities like unauthorized digital currency extraction. "Crypto jacking, "as an illustration.[7]

Eavesdropping

A hacker obtains sufficient personal data (birthdate, SSN, and address) to determine your identity. A hacker may be able to establish credit card accounts on our behalf, steal money from a bank account, and do other things.

III. DIFFERENT ATTACKS IN IOT NETWORKS

A non-attack method of attacking a data source is through cyber threats. It resembles an offensive strategy. Cyber threats today number hundreds of millions and fall into the following groups.

Virus/Malware

An email attack deceives a receiver into clicking a link in a message and installing malicious software or giving sensitive information. As previously discussed, spear phishing is a more advanced type of assault. It entails an assailant impersonating a friend or coworker to identify oneself, often to share the account amount.[8]

Man in the Middle Attack

Attack by a Man in the Middle (MitM) Between the sender and the receiver of an email, an attacker can generate, intercept, and alter the location. Both the sender and the recipient think they are in direct communication. To perplex the opposition, the army might employ the MitM attack.

Trojan horses

Horses for hire The term "Trojan horse" comes from ancient Greek culture and refers to malware that infiltrates a target system, such as a common piece of software, but runs malicious code on the host machine. It is a cyber-attack that deceptively enters the intended target network. A hacker may, for instance, include a virus in a PDF file and email it to us as an attachment. When we open a PDF file while the document is open in Acrobat Reader, the malware file is added to our system.[9]

Ransomware

Ransomware Data on the target machine is encrypted during an attack, and the user is required to pay a ransom to regain access to the data. These assaults vary from small hiccups to significant events, such as the entire shutdown of municipal data in Atlanta in 2018. Our data is encrypted by a specific kind of virus, which demands that we pay a ransom in bitcoin to unlock it.

A hacker takes control of several (potentially thousands of) devices and uses them to access the target system's features, such as a website, and to crash it as a result of heavy demand.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

Advanced Continuous Threat (APT)

Possibly the most potent cyber danger is the advanced continuous threat. The result of national intelligence agencies is APT's. Our network is intended to be infiltrated covertly for months before being breached without our knowledge by an access point

sender and recipient. Until engaged, it glides horizontally and repeatedly latches onto various components of our system. The harm it may cause then is enormous.

IV. DESIGN FRAMEWORK OF AI & ML

Network intrusion detection and prevention

Using artificial intelligence and machine learning technologies, new and unexpected threats and intrusions can be detected that are undetectable by standard signature-based systems. This novel strategy entails To identify unusual behavior and categories of the sort of danger and keeping an eye on both inbound and outgoing network data. Malware detection in extensive corporate networks. By using Ethernet, wireless, SCADA, and software-defined networks, you may enable strong network security (SDN). [10]To recognize and categorize enterprise-wide network risks, such as botnet detection and domain formation algorithms, use ML-based anomaly detection capabilities (DGA). Utilize network traffic analysis enabled by ML. It can identify and cluster the assaults based on packet headers and data flow information, such as protocols, the number of bytes, speeds, and counters. It can do this using supervised and unsupervised learning methods. ML approaches being provided to customers help classify IP traffic.[11]

The CRQ and residual risk calculation solution's operational structure

For example, by lowering false alarms, unclassified samples and supervised learning algorithms are utilized to enhance classification performance. As an Intrusion Detection System (IDS) model, a mix of extreme learning machines and SVMs with a set of the k-means clustering is employed. In order to increase accuracy and decrease false alarms, use the KDD'99 dataset. The SVM least-squares sample is the foundation of IDS. A novel deep learning-based technique for detecting network intrusions is the Nonsymmetrical deep auto encoder (NDAE), which uses fuzzy logic, fuzzy-based semi-supervised learning, genetic algorithms (GA), and other techniques. To produce a digital signature for the network segment, gloss analysis is used. Additionally, it can detect anomalies and forecast the behavior of network traffic over time. A novel decision tree technique is called ant tree miner classification. To extract optical character recognition (OCR) fields from fixed points while digitizing documents using a conventional system, rule-based approaches must be used. These tried-and-true methods aren't necessarily the best ones.

Standards for cyber security are automated

Intelligent automation of repetitive manual cybersecurity operations, such as cybersecurity controls and control functions, can be facilitated by AI capabilities, in particular RPA, ML, and NLP. This approach uses AI to increase the efficacy and efficiency of applying cyber controls, streamline processes, make controls more visible, and reduce audit costs. Cybersecurity control solutions that support AI & ML may automate cybersecurity controls and standardize automation controls for frameworks.[12]

Detailed analysis and eligibility

Teams working on the Internet can increase the efficacy and effectiveness of research and rehabilitation with the use of AI or ML. Every day, the platform analyses millions of records, filters the data and sends it to a human analyst, who lowers the number of warnings to around 100. The platform not only helps to significantly lower false positives but also raises the attack detection rate.

Identification, assessment, and protection of malware

Effective malware identification and analysis is made possible by an AI or ML solution. It can identify, examine, and stop newly developed malware strains. Malware like viruses, Trojan horses, worms, exploits, retroviruses, and ransomware are discovered. To find and understand malware, examine the accessible fields on the disc, the accessed APIs, the bandwidth used, the processing power used, the amount of data sent over the Internet, and the accessed hardware, such as keyboards and webcams. Use ML classifiers such as operational codes, KNN, and SVM to categorize malware. Using multi-layer restricted Boltzmann machines and automated encoding, and deep learning can identify intelligent malware. Novel machine learning method and rotation forest. To find

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

Android malware, combine ANN and the raw list of API models. For large-scale Android malware detection, the hybrid model relies on CNN and deep auto encoder. Malware detection, classifiers variable optimization using PSO or GA, and data enhancement utilizing bio-inspired techniques. [13]

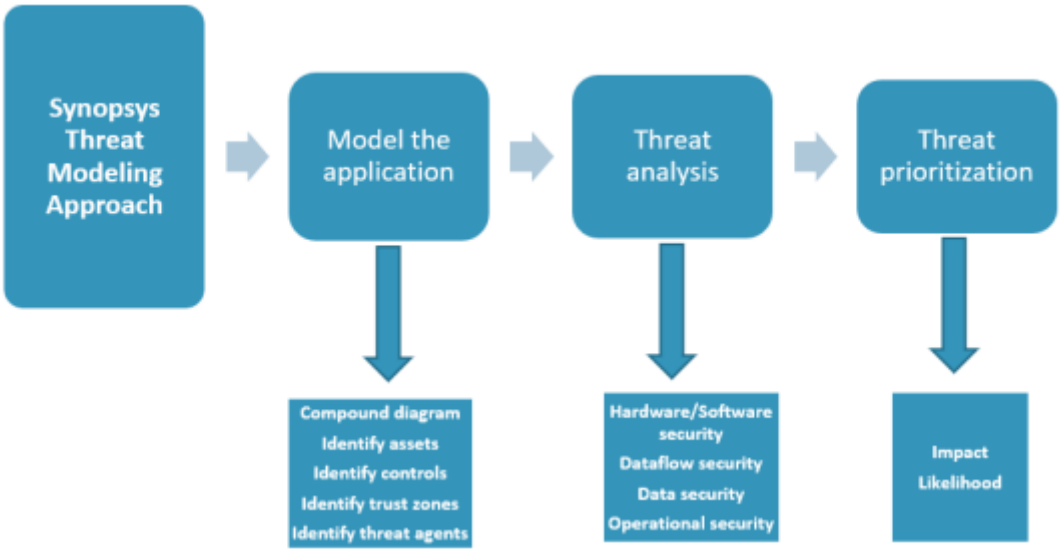

Figure 1: Threat Modeling Approach

Phishing, spam detection, and filtering

The most popular phishing websites are identified using various ML algorithms and functions by anti-phishing deception techniques. Use neural networks and reinforcement learning software to spot phishing websites. The ideas of risk mitigation and Monte Carlo algorithms are applied in these procedures. Using various categorization algorithms and NLP-based techniques, real-time anti-phishing systems. Using HTML and URL functions, stacking models identify phishing websites by combining XG Boost, gradient-boosted decision trees, and Light GBM. Spam filter systems are created by combining SVMS and Naive Bayes. Utilizing modified cuckoo search for spam categorization encourages random spam classification. SVM is utilized for classification, and the Cuckoo search technique is employed to extract functions. Features are chosen using the PSO method, and classification is done using decision tree SVMs.[14]

Combating sophisticated, persistent threats

APTs conceal their usage of sensitive data by employing clever techniques. Attackers using APT techniques frequently target lucrative targets, including governments or big corporations' security sections. The goal is frequently to steal long-term data. To counter APT assaults, AI or ML technologies are utilized[15].

Hunting for cyber threats and breach testing

In order to uncover sophisticated threats that can get through existing defenses, duplicate networks are always searching for cyber threats. This management strategy applies to conventional risks such as firewalls, intrusion detection systems (IDS), 86 security information, and event management systems, which often need data analysis after a warning is delivered.

V. CONCLUSION

The implementation and processing of different computer engineering and networking devices have undergone significant modifications thanks to artificial intelligence and machine learning. AI consists of several networked devices and is a highly adaptive cyber-physical system. Therefore data flow and analyses take place in a complicated wide area network. A surge in cyberattacks is caused by new technology advancements and the global digitalization of everything. It also offers a solitary platform for developing fresh assaults, ranging from straightforward DDoS strikes to sophisticated WannaCry ransomware attempts. The IoT and its applications, cloud computing, artificial intelligence, and machine learning are all covered in detail in Phase 1 of this research. A proactive approach uses the mantra "never trust, always verify" to address new cybersecurity concerns. As risks increase and current skills are needed, advanced technologies like AI/ML, automation, cloud computing, and Agile development address them to access their data and operations. By utilizing these services,

a cybersecurity model that is more robust and flexible may be adopted, positioning itself to withstand fresh conflicts and profit from developing digital ecosystems. In the long run, it might lead to more secure IoT support and more profits. This study also uses cyber-attack detection, analysis, and learning to address security vulnerabilities. Our AI/ML solutions provide a history of assaults, the ability to predict attacks in the future, and layered defense against zero-day attacks.

VI. REFERENCES

[1] A. Ganne, "Cloud Computing And Security Model-A Brief Survey," International Research Journal of Modernization in Engineering Technology, vol. 4, no. 11, 2022.

[2] A. Ganne, "Emerging Business Trends in Cloud Computing," International Research Journal of Modernization in Engineering Technology, vol. 4, no. 12, 2022.

[3] Y. Alkali, I. Routray, and P. Whig, "Study of various methods for reliable, efficient and Secured IoT using Artificial Intelligence," Available at SSRN 4020364, 2022.

[4] A. Ganne, "Cloud Data Security Methods: Kubernetes vs Docker Swarm," International Research Journal of Modernization in Engineering Technology, vol. 4, no. 11.

[5] G. Dhayanidhi, "Research on IoT Threats & Implementation of AI/ML to Address Emerging Cybersecurity Issues in IoT with Cloud Computing," 2022.

[6] A. Ganne, "Cloud Computing And Security Model-A Brief Survey," International Research Journal of Modernization in Engineering Technology …, vol. 4, no. 11, 2022.

[7] T. G. Zewdie and A. Girma, "IOT SECURITY AND THE ROLE OF AI/ML TO COMBAT EMERGING CYBER THREATS IN CLOUD COMPUTING ENVIRONMENT," Issues in Information Systems, vol. 21, no. 4, 2020.

[8] K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, and T. Tran, "Grand challenge: applying artificial intelligence and machine learning to cybersecurity," Computer, vol. 52, no. 12, pp. 45-52, 2019.

[9] B. Geluvaraj, P. Satwik, and T. Ashok Kumar, "The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace," in International Conference on Computer Networks and Communication Technologies, 2019: Springer, pp. 739-747.

[10] P. Radanliev et al., "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," Cybersecurity, vol. 3, no. 1, pp. 1-21, 2020.

[11] P. Radanliev et al., "Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments–cyber risk in the colonisation of Mars," Safety in Extreme Environments, vol. 2, no. 3, pp. 219-230, 2020.

[12] M. Watney, "Artificial intelligence and its' legal risk to cybersecurity," in European conference on cyber warfare and security, 2020: Academic Conferences International Limited, pp. 398-405.

[13] S. Zhao, S. Li, L. Qi, and L. Da Xu, "Computational intelligence enabled cybersecurity for the internet of things," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 4, no. 5, pp. 666-674, 2020.

[14] B. Familiar and J. Barnes, "Sensors, Devices, and Gateways," in Business in Real-Time Using Azure IoT and Cortana Intelligence Suite: Springer, 2017, pp. 127-168.

[15] A. Ganne, "Applying Azure To Automate Dev Ops For Small ML Smart Sensors," International Research Journal of Modernization in Engineering Technology, vol. 4, no. 12, 2022.