www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 12 Issue 07 July 2023, Page No. 25769-25773
ISSN: 2319-7242 DOI: 10.18535/ijecs/v12i07.4744

Artificial Intelligence-Based Approach on Cybersecurity Challenges and Opportunities in the Internet of Things & Edge Computing Devices

Dr Mansoor Farooq [1*] Prof Mubashir Hassan Khan [2]

1* Assistant Professor, Department of Management Studies, University of Kashmir
2 Assistant Professor, Department of Computer Application, Cluster University Srinagar

Abstract
The Internet of Things (IoT) presents a wide range of issues and challenges. Security is a major concern for IoT technologies, applications, and networks. IoT's research progress is discussed in this paper, which focuses on this primary feature of IoT and describes various security issues and concerns. The Internet of Things and the concept of edge computing have enabled many new IoT applications, including smart homes, intelligent transportation, pioneering health, smart grids, and smart energy. It also introduces a slew of unanticipated challenges to data security. Cybersecurity, edge computing, the Internet of Things, and artificial intelligence all present exciting new research and development prospects. There are many new threats and opportunities and this paper will focus on them.

Keywords: Cybersecurity, Block Chain, AI, Machine Learning, IoT and Edge Computing

1. Introduction

The “Internet of Things” is a cutting-edge technology that will change the world. Enabling self-configuration capabilities, as well as self-identification, via dynamic global network infrastructure based on common protocol IoT, is a new platform (3D) that extends the current connection between humans and apps. Smart homes, smart transportation, inventive things, smart cities, smart health, and smart life are the Internet of Things' most significant breakthroughs. To this day, the Internet is still run by a single central authority, with a vast pool of processing and networking power and a large amount of data being transferred between them. It was able to cut prices, offer pay-as-you-go services, allow for scalable and elastic services, and enable substantial data analysis which is a major concern for LUCC because it is already evolving considerably towards the Internet of Things. After the IoT application's Installation, there will be significant security issues that will arise, affecting the Internet. The large deader of internet-connected devices connected to the Internet can cause a substantial impact on relevant fields. This trend would potentially change the flow of digital data. It is infeasible to acquire and process all the big data in remote data centres. The two main factors preventing the action are as follows. The data from IoT devices would effectively increase the amount of collected data, in which the acquisition of a local computer is unavoidable. The second factor is that many future IoT applications require low latency or fast response features. Virtual Reality, Augmented Reality, and autonomous cars are examples of technologies that make use of Artificial Intelligence (AI) to enhance the user experience.

With this outcome in mind, additional computing, storage, and networking means are predicted to arise on the network's periphery, closer to consumers and Internet of Things devices that generate data. This phenomenon is referred to as "fog computing" in several publications. Incorporating edge computing with the Internet of Things will drastically cut data traffic on the Internet while simultaneously improving data intelligence and enhancing reaction speed. This paradigm will benefit a lot of new Internet of Things applications, including smart homes, intelligent transportation, wise health, smart grids, and smart energy,

among others. The edge computing + Internet of Things development is posing cybersecurity issues and posing threats.

2. Cybersecurity Challenges

The essential attribute of an IoT system is security, which is related to distinct security aspects that are also required for a system to allow trust and privacy features(Jing et al, 2014). IoT can secure connected devices and also protect data and networks. Currently, there are many concerns related to IoT because of connected IoT devices (Pan et al, 2016).

2.1 Susceptible IoT Devices

A large number of people with a limited resource of IoT devices, due to inadequate computer, memory, and battery capabilities, may be much more exposed to all types of harmful attacks in the future IoT world, making them notably more prone in the face of any and all forms of attacks. Such flaws have the potential to result in large-scale security breaches as well as severe economic losses (Køien et al, 2014; Jing et al, 2014). When it comes to executing typical algorithms for encryption, authentication, and access control, IoT devices tend to be constrained in their capabilities.

They are most at risk when a targeted attack on the Denial of Service (DoS) is introduced to them. For example, (Van, 2008) fraud and theft of information, codes, or keys; (Køien et al, 2014) counterfeit identity that endangers the integrity of the data; (Sundmaeker et al, 2010) listening to wireless channels; and (Bandyopadhyay & Sen, 2011) the use of bogus nodes to aggressively connect connections between IoT devices and edge nodes are all examples of IoT attacks. When it comes to providing Internet users with Things, linking security features, and even detecting and blocking malicious external attacks, a remote computer platform has the potential to play an important role. However, unlike conventional cloud computing, the peripheral computer paradigm is very young, and the various security implications of this paradigm are not yet fully understood.

2.2 Interaction between IoT and Edge Computing Devices

In the cloud era on the open edge (Higgins, 2016; La et al, 2016), tasks issued by IoT-enabled devices will become increasingly prevalent. for faster processing on a rich computer network of resources, which is one of the hallmarks of open cloud years. Internet of Things Devices can also collaborate to perform a variety of tasks, depending on the availability of the service and the incentive program available. In addition, downloads and communications of this program may raise concerns about new security risks. The first concerns the security of mobile applications. This includes writing and developing work codes that can be customized to work across a variety of systems, such as edge-computing and Internet of Things (IoT) devices (Farooq & Hassan, 2019). A sophisticated process that includes trusted APIs or links is needed for cross-platform code transfer and dynamic editing, among other things. Second, virtual machines (VMs) and other cloud-based services must be able to interface with mobile and wireless Internet of Things (IoT) devices. The horizontal cloud orchestrator must also provide the necessary resources from the cloud side edge. It is necessary to provide appropriate access control mechanisms to protect transmission codes between cloud clouds and IoT devices from malicious attacks.

Furthermore, wireless and mobile connections serve as the primary means of communication between Internet of Things devices and the edge-cloud. All of the security risks that are associated with wireless-mobile networks continue to exist in this environment. For any communications via these wireless channels, for example, it is required to use appropriate encryption software. However, because IoT devices are often low-resource, it is critical to develop authentication, encryption, and access control solutions that are both effective and light on the system's resources. The edge cloud, with its abundant resources, can aid in the promotion of various IoT protection activities.

2.3 Privacy and Data Security

Large amounts of data will be created at extremely fast speeds by a considerably greater number of Internet of Things devices that are linked to the Internet. Because it is impractical to store and process all of the information at centralised processing sites, such data would have to be stored and processed in a number of

decentralised edges computing nodes or edge clouds, as is the case with the existing cloud computing architecture. The way in which data privacy and protection are handled would also be distinct. For app users (such as those using medical IoT or health applications) who choose to own, store, and manage their data entirely instead of entrusting cloud service providers with it, who lack control over them and who can ensure that cloud service providers will not use their data or that data will be used in any way acceptable, this can be profitable. Alternatively, these decentralised edge clouds are far more prone to, and consequently less effectively secured against, different efforts to breach data, denial of service assaults, and even physical tampering, than centralised edge clouds. To protect privacy and data at all levels (including the vision layer, the transit layer, and the application layer) and in many ways (including physical security, information security, & executive security), more study needs to be done. In a highly separated computer setting, it is important to do so in order to keep data private and safe.

3. Opportunities to Overcome the Cyber Security Challenges

The alternatives or options that have been proposed as countermeasures to the Internet of Things security risks. With the rise of new technologies like Blockchain, AI, and ML, we can expect more chances to study and come up with new ideas in areas like privacy, edge computing, the Internet of Things, and processing. Wisdom will emerge.

3.1. Artificial Intelligence and Machine Learning

Over the past few years, AI innovation and machine learning (especially in-depth learning) have made great strides, especially since AlphaGo has done so well.

Applications for self-driving cars in circumstances when there is enough data to create models and optimise their parameters, these technologies work optimally and deliver the greatest predicted performance possible. Several scenarios in the current edge-computing plus IoT- environment can be predicted and intelligent decisions can be made to optimise a variety of different items, such as resource usage and access scheduling. AI and machine learning technology are able to predict and make intelligent decisions in a variety of contexts. The use of technological intelligence and learning in "edge computing + IoT" presents an important opportunity in the light of cybersecurity, as it will allow us to better understand the various online activities, determine possible risks and limitations to fix or exploit, and see cruelty. to attack. To give an example, in-depth learning technology can determine or foresee that a user's actions or inactions are indicative of an attack attempt against sensitive data, or that the user is the one actually attempting such an attack.. functions, based on relevant data collected and patterns obtained. The inclusion of such high-quality work may provide an additional layer of protection against any company from the identification of harmful attacks and the prevention of abuse.

Powered by artificial intelligence and machine learning systems, a dedicated automatic robot can also be deployed that secretly scans and reviews the enterprise's environment and activities to see any possible risks, weaknesses, or malicious activities. Any misuse will also be reported and detected and reminders sent out. They may also theoretically take timely measures on behalf of human administrators to respond to such particular threats. Once sufficient data is collected and a suitable model is developed, these robots will prove to be of great assistance in the field of cybersecurity.

3.2. IoT naming convention solitary and distinct IP

IP addresses are used by nearly all of the devices connected to the Internet today (IPv4 or IPv6). In terms of interconnectivity, this provides tremendous ease by letting devices communicate with one another as well as receive material and services from the internet. Administrators' lives are made considerably simpler as a result of this extensive interconnectivity, which allows for remote configuration and management. Its downside is that it exposes all devices, including important industrial control systems such as smart grids, to a potentially catastrophic media environment. The breach of any basic credentials, even those claiming to be authorised users, might provide potential hackers access to the leaked credentials. Conventional firewalls are capable of filtering some types of traffic. They do, however, frequently rely on a perimeter-based security scheme, with firewall filtering generally relying on random IP addresses as a starting point. It also does not

protect against assaults from the inside. To solve this security issue, a new unique identifier and a different wording scheme than IP can be used to identify IoT devices worldwide. Examples of this include using the Host Identification Protocol (HIP) [8] hosted IDs of IoT devices instead of IP addresses to provide them with a unique ID and an independent name scheme for an IP address. For that to identify overlay and configuration, IoT devices may need hosting IDs instead of IP addresses. Before two people may communicate with one another, Before they can safely share cryptographic keys with one another, they need to first bind themselves together. Important devices and systems connected to the Internet of Things will be protected against unauthorised access in this way. In a similar spirit, in the future of "edge computing + IoT," there will be a demand in particular for. The use of a secure, non-IP-based name and identification system has several benefits. for those resource-constrained Internet of Things devices that are part of critical systems that require extra protection. In this regard, we anticipate that there will be a significant number of research possibilities.

3.3 Cyber defence deployed on deceit

Wikipedia defines passive security as most traditional cyber defence measures like encryption, authentication, and access control, which do not actively pursue attackers but instead make it harder for them to gain access. Deception-based cyber security is one of the most effective ways to boost a company's cyber defences. This attack uses address hopping, honeypots, and network telescopes. Deception and unpredictable network settings may confuse attackers and attract them to pre-deployed honeypot traps[4]. As a result of the deception-based strategy, a large number of bogus credentials may be generated on a company's network, which allows them to more easily survive attacks on their networks' structures, which are composed of legitimate user identities. It is possible for security administrators to recognise and follow the perpetrators if they use these forged credentials. Once the attackers' actions have been registered and documented, the traces and archives of their actions may be examined in further depth to determine how they targeted the target device and the basic patterns they employed to do so. This data improves computer network security. Honeypot traps are generally virtual computers that, under tight supervision and tracking by security officials, become actual instruments for inquiry. They try to trick attackers into helping the defence or wasting time and money on wrong goals. However, attackers may try to avoid detection by acting suspiciously or normally. Industry analysts expect the deception-based cyber defence to make large-scale "edge computing + IoT" systems safer.

3.4 Blockchain

Recently, blockchain technology has piqued the curiosity of many in the business world as well as the academic community. It is seen as a powerful technology to change not only the way people spend money (Bitcoin or other cryptocurrencies), but also the way people interact with individuals, companies, and institutions that they do not trust when conducting all sorts of transactions. Blockchain is made up of a distributed ledger shared by all users. All of the transactions that other blockchain participants may make, trade, and verify over a dispersed network of computers are recorded in the ledger and are accessible to anybody who has access to the blockchain. The transactions are extremely transparent and accessible to all of the people involved. Because of the Blockchain's structure, it is nearly impossible for transactions to have been intentionally changed after they have been reported.

Blockchain technology may enhance user identification, identity, and access control management, as well as transaction recording and email. DARPA has solicited ideas for a blockchain-based battle-field communications system (Sundmaeker et al., 2010). Private blockchains, Edge Computing, and the Internet of Things may empower smart contractors to reimagine commercial transactions without trust ties. Zero-trust protection is possible with the Blockchain's trust less environment. Previous security models employed perimeter-based protection to defend organisations inside their networks from internal threats. which puts them at risk of internal attacks. The zero-trust framework (Sucuri, 2016) is characterized by the fact that participants do not automatically trust each other and always verify each other's identities before proceeding. An intruder who has compromised internal content will not be able to move away from confidential data or content to the target when using such a method. Additionally, it will ensure that data access and use of the app are both secure and readable. Access regulations may also be strictly enforced in some cases. Zero-trust-

based blockchain-based structures could be instrumental in building a more secure "edge computing + IoT" ecosystem, according to the authors.

4 Conclusion

Many IoT applications may reap significant advantages from the shift to the Internet of Things and the rise of edge computing. It also poses some very fundamental problems for network security. Three possible cybersecurity risks and four potential cybersecurity opportunities were identified and mitigated as part of the strategy's execution. The synergy between edge computing, IoT platforms, and emerging blockchain and AI technologies has led to a number of successful outcomes.

References

1. Bandyopadhyay, D., Sen, J. (2011). "Internet of Things: Applications and Challenges in Technology and Standardization". Wireless Pers Commun Vol 58, pp. 49–69.
2. Higgins, Stan. (2016), "DARPA Seeks Blockchain Messaging System for Battlefield Use", available at:https://www.coindesk.com/darpa-seeks-blockchain-messaging-system- for-battlefield- back-office- use/.
3. Køien, Geir & Abomhara, Mohamed., (2014), Security and privacy in the Internet of Things: Current status and open issues. 10.1109/PRISMS.2014.6970594.
4. La., Duy, Quang., Quek, QS, Tony., Lee, Jemin., Lee, Shi. and Zhu.,Hongbo. (2016), "Deceptive attack and defense game in honeypot-enabled networks for the internet of things", IEEE Internet of Things Journal, Vol.3 No.6 pp. 1025–1035.
5. Farooq, M. (2022). Supervised Learning Techniques for Intrusion Detection System based on Multi-layer Classification Approach. International Journal of Advanced Computer Science and Applications, 13(3).
6. Pan, Jianli & Ma, Lin & Ravindran, Ravi & Talebifard, Peyman. (2016). Home Cloud: An edge cloud framework and testbed for new application delivery. 1-6. 10.1109/ICT.2016.7500391.
7. Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu & Dechao Qiu.,(2014), "Security of the Internet of Things: perspectives and challenges", Wireless Networks, Vol. 20 No.8 pp. 2481–2501. https://doi.org/10.1007/s11276-014-0761-7
8. Farooq, M. and Hassan, M (2021), IoT Smart Homes Security Challenges and Solution, International Journal of Security and Networks, Vol. 16, No. 4, pp. 235-243
9. Sucuri. (2016), "Large CCTV Botnet Leveraged in DDoS Attacks", available at: https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos- attacks.html
10. Sundmaeker, H., Guillemin, P., Friess, P. and Woelffie, S. (2010), Vision and Challenges for Realising the Internet of Things. EUR-OP, Brussels
11. Van Kranenburg, Rob. The Internet of Things (2008) : A Critique of Ambient Technology and the All-Seeing network of RFID. Amsterdam Netherlands: Institute of Network Cultures.