ASIAN JOURNAL OF ELECTRICAL AND ELECTRONIC ENGINEERING
Vol. 4 No. 2 2024
E-ISSN: 2785-8189

Securing the IoT Edge Devices Using Advanced Digital Technologies

Abdul Manan Sheikh[1*], Md Rafiqul Islam[1], and Mohamed Hadi Habaebi[1],
Adnan Kabbani[2], Suriza Ahmad Zabidi[1], and Athaur Rahman bin Najeeb[1]
[1]*Dept. of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia*
[2]*Dept. of Electronics & Communication Engineering, A'Sharqiyah University, Ibra, Oman*

*Corresponding author: abdul.manan@asu.edu.om

(Received: 30 September 2024; Accepted: 2 October 2024)

Abstract— As the IoT ecosystem continues to grow, edge computing is becoming essential for handling and analyzing the vast amount of data generated by connected devices. Unlike traditional centralized data models, where information is sent to remote centers for processing, edge computing processes data closer to where it is generated. This decentralized approach helps reduce latency, optimizes bandwidth usage, and improves both privacy and security. However, the rise in IoT devices and the spread of edge computing also increase the potential for cyberattacks, demanding more robust security measures. With AI and machine learning being utilized to analyze IoT data, edge computing facilitates this analysis directly at the data source, pointing to a future where AI and ML applications are more prevalent on edge devices.

Keywords: *IoT, Edge computing, Cyberattacks, Artificial intelligence, Machine learning.*

1. INTRODUCTION

With the rapid development and acceptance of the Internet of Things (IoT), big data, and 5G network architecture, traditional cloud computing still needs to meet the ever-increasing data volume generated by network edge devices and the need for real-time services. The evolution of edge computing (EC) enables data processing near or at the network's edge, thus reducing the computational and communication overload. However, due to the exclusive benefits and characteristics of EC, such as heterogeneous distributed architecture, data processing, parallel computation, location awareness, and the need for mobility support, traditional data security and privacy mechanisms in cloud computing are not capable of the EC paradigm [1]. IoTs have upgraded conventional, passive devices into sensible ones, allowing them to transmit considerable volumes of relevant data over the internet. Data processing and analysis capabilities within an IoT framework enable these devices to function autonomously with minimal human intervention. Artificial intelligence (AI)--based algorithms are employed to analyze the substantial volumes of data generated within IoT networks, enabling the delivery of value-added public services [2]. IoT services are assembled on a foundation of miscellaneous technologies in hardware and software. These services leverage various network technologies and communication protocols, which include radio frequency identification (RFID), near-field communication (NFC), ZigBee, Bluetooth, electronic product code (EPC), low-energy wireless communication protocols, barcodes, long-term evolution (LTE) advanced, AI, and wireless sensor networks (WSNs) [3].

Projections indicate that the global IoT market will experience a compound annual growth rate (CAGR) of 10.53% from 2019 to 2025 [4]. Cisco estimates that in 2030, over 500 billion devices will be connected to the internet. In the present day, the impacts and applications of IoT are particularly notable in areas such as environmental sensing, healthcare monitoring systems, logistics supply chain management, real estate construction, energy management, drone-based applications, the manufacturing industry, and various other fields. Securing the IoT systems is crucial as they continue to grow and integrate further into our daily lives. Despite its numerous benefits, IoT also poses serious security concerns for enterprises and individual users. Any device that is connected to the internet could act as a doorway to an extensive network, including sensitive data.

DOI: https://doi.org/10.69955/ajoeee.2024.v4i2.69

Interconnected devices aggravate security concerns further by exposing more security flaws and vulnerabilities. In the absence of appropriate security and privacy measures, potential attacks and security threats may outweigh IoT benefits and applications.

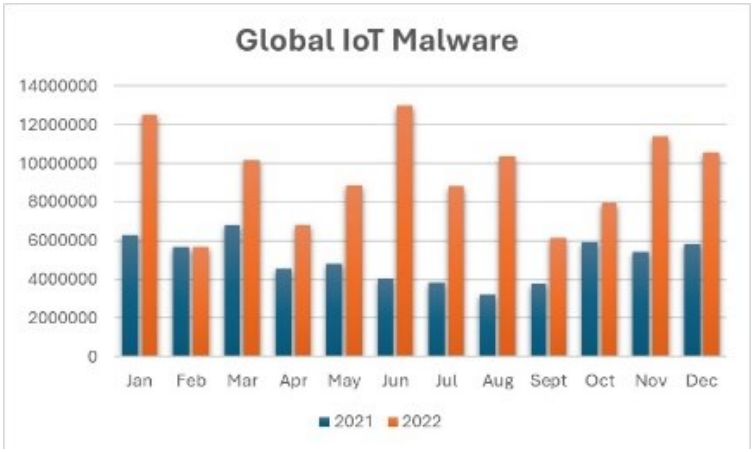

Fig. 1. Global IoT Malware during 2021 and 2022 [6]

Security solutions are expected to be lightweight that can be hosted on devices with lesser memory, computational abilities, and cost. Although numerous security solutions are proposed for standalone constrained devices, they are unsuitable for integration into the IoT network. The edge devices' heterogeneous nature, diverse computational capabilities, and network complexity necessitate lightweight security solutions that adhere to global standards [5]. The rapid expansion of IoT devices has opened new opportunities for cybercriminals. Security experts are frequently uncovering new malware targeting poorly secured IoT devices.

In 2022, SonicWall Capture Labs recorded 112.3 million instances of IoT malware, marking an 87% rise compared to 2021 (as shown in Fig. 1). Cyber attackers exploit IoT devices and networks to steal sensitive user data, including financial information, card details, location data, and health records. In edge computing-based (EC) IoT networks, significant amounts of user data are processed at the network's edge, spanning various industries and applications. The connection between edge devices and EC nodes is typically established through wired or wireless links. In contrast, EC nodes communicate with the cloud or data centers via public or private networks [7]. There are numerous cyberattacks targeting IoT applications. For example, the 2016 Mirai attack compromised over 2.5 million IoT devices and launched distributed denial of service (DDoS) attacks. Subsequent attacks, like Hajime and Reaper, further emphasized the security threats facing IoT devices [8]. As a result, developing security standards and guidelines for IoT is crucial to building secure and resilient IoT services. Regulatory bodies globally have also recognized the importance of IoT security [9].

This article provides a detailed review of IoT systems' security and privacy challenges, addressing associated technologies and protocols. It evaluates the current IoT architecture, identifies the security risks and limitations of underlying technologies, and concludes by summarizing key points on ongoing IoT security challenges, offering potential solutions.

2. EDGE COMPUTING

EC leverages present techniques, which ensures the processing of sensitive data at the network edge itself, thus managing the downstream data to centrally located cloud services as well as upstream data for IoT services. The "network edge" implies any computing or network resource between the data sources and the centrally located cloud-based data centers. The primary functions of EC include offloading computing jobs, data storage and caching, processing collected information, distributing user requests, and delivering cloud-based services closer to the end user. Although cloud computing has proven to be efficient for data processing due to its superior computational abilities power, the networks' bandwidth could not match the speed of data processing, forming a bottleneck for cloud-based computing. The concept of EC was conceived to place computing closer to data sources, offering several advantages over the traditional cloud-based computing approach. A comparison is presented in Table 1 [10].

Table 1: Comparing IoTs, Edge and Cloud computing [11]

	IoT	*Edge*	*Cloud*
Implementation	*Distributed*	*Distributed*	*Centralized*
Nature of the devices	*Physical*	*Edge nodes*	*Virtual nodes*
Computing capacity	*Less*	*Less*	*Larger*
Memory availability	*Very limited*	*Limited*	*Unlimited*
Response time	*N.A.*	*Fast*	*Slow*
Big data	*Source*	*Process*	*Process*

2.1 Edge Computing Architecture

The general architecture of EC is depicted in Fig. 2, representing edge computing MEC servers closer to the end users as compared to cloud-based data centers. Despite lower computational abilities, EC servers can offer better quality of service (QoS) and lower latency than cloud servers. The generic architecture of EC can be divided into three layers: the front-end, near-end, and far-end. The characteristics of each layer in an EC architecture are discussed below [11].

2.1.1. Front End

The Front-End layer consists of end devices such as sensors and actuators that manage data flow between two networks, functioning primarily as gateways for data entry or exit. Edge devices in this layer handle tasks such as data transmission, routing, processing, monitoring, filtering, translation, and storage as user data moves between networks. Edge computing (EC) capitalizes on the computing power of nearby end devices to provide real-time services for specific applications. However, since end devices have limited processing capacity, they often rely on server resources to meet most service requirements.

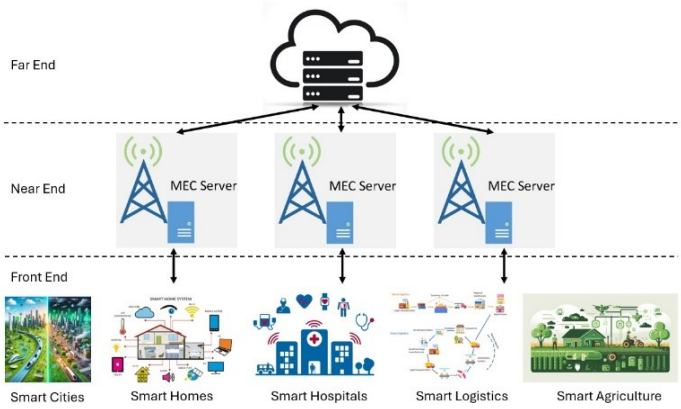

Fig. 2. Edge computing architecture.

2.1.2. Near End

The Multi-access Edge Computing (MEC) model and gateways in the near-end environment are designed to move technology resources closer to client devices and end users. Edge servers in this layer handle real-time data processing, data caching, and offloading computation tasks, offering computing and cloud-like services at the network edge. This reduces reliance on centralized cloud services for these processes.

2.1.3. Far End

The far end of the EC architecture consists of cloud data centers, including a centralized data hub and interconnected regional centers. These cloud data centers act as the ultimate repository for information. Since cloud servers are located far from the end devices, transmission latency becomes critical when delivering large-scale parallel data processing and storage services.

2.2 Edge computing benefits

According to the estimates published in Gartner report, about 75% of the network data produced at the business houses will be shifted out from the centrally located data centers for processing, a substantial increase from the 10% predicted in 2018. This trend demonstrates the growing adoption and acceptance of EC. By shifting computing resources and intelligence closer to the network's edge, EC offers numerous benefits, such as significantly lower latency, increased bandwidth, and enhanced privacy and security [12], [13]. These benefits of EC are further steering the adoption of various services such as IoT/M2M, 4K Ultra High Definition (UHD) video services, and mobile serious gaming. Also, MEC can offer application providers local context awareness, including Radio Access Network (RAN) analytics, traffic characteristics, and device location information [14]. Thus, EC solves latency-related challenges and supports users to optimize the benefits of cloud computing architectures. Forms of EC include local devices, localized data centers, and regional data centers. The benefits of EC can be summarized as,

Quicker data processing and analysis: EC minimizes the necessity for data transmission to centrally located cloud data centers, thus quicker response times and real-time processing. EC characteristics are leveraged in applications requiring rapid feedback, such as automatic driving, intelligent manufacturing, and video monitoring.

Security: EC processes the user data locally, mitigating the risk of data loss or leakage associated with data transmission to the cloud.

Lower energy consumption and bandwidth cost: EC minimizes the dependence on broad network bandwidth and energy consumption due to data processing locally.

2.3 Edge Computing Challenges

The edge-based servers provide distributed computing resources at a small-scale level; thus, EC-based IoT services are scalable and able to meet demands in large-scale applications like smart cities or autonomous driving. However, integrating EC with IoT poses unique challenges, and a seamless and efficient approach is needed to bridge the gap between these two technologies. The three important challenges in EC-based IoT systems are summarized below:

Heterogeneous IoT infrastructure: The edge devices/ sensors are deployed in diverse environments with unique purposes. Hence, various hardware devices and communication protocols are needed. Also, the deployment architecture of these devices in the EC environment varies with the application type. Thus, there is a need to explore a cooperation architecture involving hardware devices, communication protocols, and established industry standards to unify this diversity.

Coordination between communication and computing: Coordination between communication and computing is a bottleneck in the success of EC-driven IoT services. The limited power and computational capacity of edge devices and servers limit the amount of workload that can be transferred to the edge servers. Hence, an orchestration mechanism should be in place that allocates the workload between edge servers and IoT devices at optimal communication and computation costs.

Complicated security and privacy issues: Adversaries target IoT devices and edge servers to gain access to user data or disrupt the services. EC-based IoT systems' heterogeneity and constrained computing capability are the foremost challenges in ensuring security and privacy. Appropriate countermeasures like robust authentication and encryption techniques, secured communication protocols, regular updates to underlying software and firmware to patch vulnerabilities, and adherence to strict access control policies should be adopted and implemented to address these challenges.

3. DATA SECURITY AND PRIVACY CHALLENGES

EC requires outsourcing end-user private data to external service providers, such as cloud or edge data centers, leading to data ownership and control loss. This separation can result in data loss, leakage, unauthorized access, compromised confidentiality and data integrity. EC leverages various technologies, including offloading, virtualization, and outsourcing, that bring the computational tasks closer to data sources. Users' data privacy is an important driver for security, with the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) defining privacy as the right of individuals to manage the collection, processing, and storage of their personal data and control its access. The data privacy

requirement is often ensured through mechanisms like cryptography, which restricts access to authorized parties and inhibits unauthorized disclosure [1].

Several factors contribute to the increased attack surface in the EC model. Two primary concerns are hardware limitations and software heterogeneity. Devices and servers at the edge layer typically have less computing and storage capacity than cloud servers, making implementing robust security measures like firewalls challenging and leaving them more vulnerable to attacks. Additionally, the lack of standardization in protocols and operating systems across diverse edge deployments further increases the risk of security breaches. Security threats in edge computing (EC) are continuously evolving, mainly due to the frequent mobility of user devices. These security challenges stem from design flaws, misconfigurations, and implementation errors. Xiao et al. have categorized most EC security threats into four main types, as shown in Fig. 3: Distributed Denial of Service (DDoS) attacks, side-channel attacks, malware injection attacks, and authentication and authorization attacks. Corresponding mitigation strategies for these threats are detailed in Table II [17].

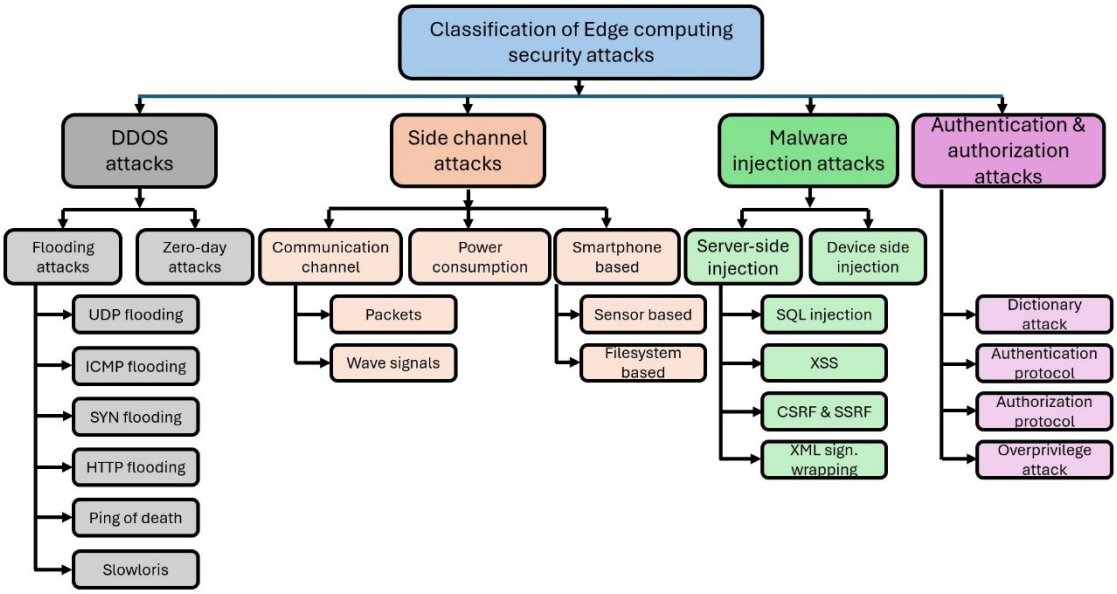

Fig. 3 Classification of EC security threats [15]

Distributed Denial of Service: DDoS attacks involve unauthorized server access through compromised edge devices. In these attacks, adversaries take control of edge devices and launch denial-of-service assaults on edge servers, effectively shutting down their services. Two common forms of DDoS attacks are zero-day attacks and flooding-based attacks. Flooding attacks overwhelm a server by bombarding it with many malicious network packets, such as UDP overflows, ICMP floods, SYN flash floods, HTTP flash floods, SYN flooding, ping of death, and delays, disrupting normal operations. Zero-day DDoS attacks are more advanced, relying on the attacker identifying an unknown vulnerability in the server's code. The attacker exploits this vulnerability, causing memory corruption and the eventual breakdown of the server's services. Flaws in communication network protocols primarily cause flooding attacks, while zero-day attacks exploit unaddressed vulnerabilities in server software [18].

Side-channel attacks exploit publicly accessible information about a target, known as side-channel data, rather than directly accessing sensitive information. Attackers use the correlations between the gathered public data and private information to infer the protected data. These attacks can occur at any point in the edge computing (EC) network, as public information can often be linked to sensitive data. For example, attackers may capture communication signals (such as packets or wave signals) to expose private user data or monitor the power consumption of edge devices to reveal usage patterns. Power analysis is a common technique for extracting side-channel data from EC networks. Power analysis-based attacks are categorized into two types: simple power analysis and differential power analysis. Simple power analysis involves closely examining individual power waveforms to extract valuable information. On the other hand, differential power analysis (DPA) consists of recording a series of power consumption readings while the

device processes specific data, such as a secret encryption key. These readings are then compared to known power models to deduce parts of the secret key [19].

Table 2: Mitigation strategies against EC cybersecurity threats [15]

Station	*System Type*
DDoS attack	*Detect and filter technique is adopted. Individual packets are inspected to identify and remove the malicious content from the network. Machine learning and packet entropy can also help identify malicious packets. Countermeasures against zero-day attacks are difficult as the source codes are buried deep in the firmware.*
Side-channel attacks	*Data perturbation and differential privacy techniques. K-anonymity is the commonly used data perturbation technique that alters the identifier information before publishing sensitive attributes along with the data.*
Malware injection attacks	*The detection-and-filter technique has emerged as effective against server-side injection attacks. Defense strategies normally rely on static analysis to detect malicious code and implement a fine-grained access control mechanism.*
Authentication and authorization attacks	*Two common methods are improving the security of communication protocols and reinforcing cryptographic implementations to counter attacks on authentication protocols. To prevent over-privileged attacks, the most effective strategy is to enhance the permission models of operating systems on edge devices.*

A malware injection attack is a data security threat where attackers insert malicious code into a legitimate software application running on an edge server. This compromised software may lose functionality and potentially gain access to users' sensitive data. Such attacks exploit software vulnerabilities, allowing the attacker to run arbitrary code and take control of the targeted system for malicious purposes [20]. Due to the resource limitations of edge devices, they often lack robust firewalls, making them vulnerable to cybersecurity threats. Attackers can covertly install malicious software on an edge device or server. Server-side attacks are typically classified into four categories: SQL injection, cross-site scripting (XSS), XML signature wrapping, and Cross-Site Request Forgery (CSRF) or Server-Side Request Forgery (SSRF). Device-side attacks, on the other hand, commonly target the firmware of edge devices.

Authentication and Authorization attacks: Authentication is the process of confirming the identity of a user requesting access to services, while authorization defines the access rights and privileges of that user. In EC, authentication commonly occurs between edge devices and servers but can also happen between devices or servers in a decentralized system. Authorization involves the edge server granting access permissions to a particular device or its applications. Both processes in EC are susceptible to several types of attacks, which can be categorized into four main groups: dictionary attacks, attacks on authentication mechanism vulnerabilities, exploitation of authorization protocol flaws, and over-privileged attacks. [17]. Dictionary attacks use a list of access keys to bypass authentication systems. Authentication vulnerabilities are often exploited through weaknesses in security protocols like WPA/WPA2. Authorization attacks take advantage of poorly designed authorization protocols running in EC systems. In over-privileged attacks, attackers deceive the system to gain excessive access rights, allowing them to perform malicious actions within the EC network.

4. EDGE AI

Big data processing requires more powerful methods, such as AI technologies, to extract insights that enable better decisions and strategic business moves. Edge artificial intelligence, or edge AI, is the deployment of AI algorithms and models on edge devices like sensors or IoT devices. Edge AI facilitates real-time data processing and analysis without dependence on cloud computing infrastructure. Edge AI combines EC and AI technologies to execute machine learning (ML) algorithms on edge devices. Technologies such as self-driving cars, wearable devices,

security cameras, and smart home appliances leverage edge AI capabilities to promptly provide users with real-time information. ML can control shared resources at the edge smartly and adaptively [21]. Edge AI offers several benefits. Firstly, it decentralizes the data required for refining algorithms. Secondly, it enables analysis and decision-making to be conducted close to the data source. From a security and privacy standpoint, edge AI can mitigate attack vectors by minimizing or eliminating data transfer between edge devices and their data centers. Training and execution of AI models on edge devices are confronted by several challenges and roadblocks discussed below [22].

Limited hardware capabilities: Edge devices are usually constrained by several factors, such as processing capability, data storage requirements, and network bandwidth, that limit the hosting of complex AI algorithms on edge devices.

Power constraints Mostly, edge devices support mobility, are battery-operated, and have low power, limiting their ability to perform intensive AI tasks.

Scalability issues Unlike cloud resources, the resources at the edge layer need to be more flexible to scale, and the heterogeneous nature of these resources can degrade service quality.

Collaboration challenges Coordination and cooperation between heterogeneous edge devices can be challenging, resulting in poor efficiency and effectiveness of AI models.

Data privacy concerns: Using original private data for model optimization on edge devices raises privacy concerns, and limited communication resources can restrict the distribution of computation to devices.

4.1 Hardware for Edge Devices

The algorithm and hardware selected for running a model on an edge device are crucial. Optimal hardware choice should consider accuracy, energy consumption, data throughput, and cost metrics. Edge devices designed for AI model execution can typically be categorized into four types based on their technical architecture [23].

Application-Specific Integrated Circuit (ASICs) Chip: ASICs are the best possible option for specific applications rather than general functions. Their smaller footprint, lesser power consumption, more robust security and performance make them ideal for meeting the demands of edge computing patterns for AI algorithms. On the other hand, Edge Tensor Processing Units (TPUs) are Google's custom-designed chips used to accelerate Machine Learning workloads.

Graphics Processing Unit (GPUs): GPUs leverage the inherent data parallelism of mining programs to enhance throughput, achieving higher speeds compared to central processing units (CPUs). These GPUs' characteristics make them suitable for implementing AI algorithms, thus making them an ideal choice for designing and implementing edge devices. For example, NVIDIA's Jetson TX1, TX2, and DRIVE PX2 are embedded AI computing devices equipped with GPUs. These devices offer a small form factor, lower latency, and low power requirements.

Field-Programmable Gate Array (FPGA): FPGAs are highly flexible, programmable hardware with lower energy requirements, parallel computing resources, and high security. Developers familiar with hardware description languages can quickly implement AI algorithms on FPGAs. However, FPGAs have poorer compatibility and more limited programming capabilities compared to GPUs. Leading FPGA manufacturers include AMD-owned Xilinx and Intel Altera.

Brain-Inspired Chip: Brain-inspired chips are constructed on a neuromorphic architecture, featuring programmable neurons on a silicon chip that process tasks akin to the human brain using synapses. These chips enable significantly accelerated processing of neural network applications in real-time, with extremely low power needs. Examples of neuromorphic processor chips include IBM True North and Intel Loihi, which are well-suited for complex AI algorithms.

5. CONCLUSION

Edge computing offers numerous benefits but also poses challenges that must be tackled. Security and privacy are foremost cause of concern as the user-sensitive data is processed and analyzed near edge devices. Implementing robust encryption, data protection, and secure communication protocols is crucial to mitigate these risks. Managing and scaling distributed edge infrastructure can also be complex, requiring seamless integration, network connectivity, and device management as edge device numbers increase. Standardization and interoperability

across various edge computing solutions are essential for creating a cohesive and scalable ecosystem. Deploying machine learning on IoT devices reduces network congestion by enabling computations near data sources, ensuring data privacy, and lowering power consumption compared to continuous wireless transmission to central servers. The integration of specialized hardware into edge devices enhances computing efficiency in physical environments and improves responsiveness. Neuromorphic processors and sensors are also emerging, offering real-time intelligence and continuous onboard learning at the edge, even with a tight power budget, enabling complex AI computation at the network's edge.

REFERENCES

[1] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," IEEE Access, vol. 6, pp. 18209-18237, 2018. https://doi.org/10.1109/ACCESS.2018.2820162

[2] M. A. Albreem, A. M. Sheikh, M. H. Alsharif, M. Jusoh, and M. N. Mohd Yasin, "Green Internet of things (giot): Applications, practices, awareness, and challenges," IEEE Access, vol. 9, pp. 38833-38858, 2021. https://doi.org/10.1109/ACCESS.2021.3061697

[3] M. A. Albreem, A. M. Sheikh, M. J. Bashir, and A. A. El-Saleh, "Towards green internet of things (IoT) for a sustainable future in Gulf cooperation council countries: Current practices, challenges and future prospective," Wireless Networks, vol. 29, no. 2, pp. 539-567, 2023. https://doi.org/10.1007/s11276-022-03133-3

[4] M. A. M. Albreem, A. M. Sheikh, and A. A. El-Saleh, "Towards a sustainable environment with a green IoT: An overview," in 2022 International Conference on Computer Technologies (ICCTech), pp. 52-63, 2022. https://doi.org/10.1109/ICCTech55650.2022.00017

[5] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: a survey," Wireless Personal Communications, vol. 115, no. 2, pp. 1667-1693, 2020. https://doi.org/10.1007/s11277-020-07649-9

[6] SonicWall, "2023 SonicWall cyber threat report." https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf/, 2023. accessed:2024-04-26.

[7] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing assisted internet of things," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4004-4022, 2020. https://doi.org/10.1109/JIOT.2020.3015432

[8] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82721-82743, 2019. https://doi.org/10.1109/ACCESS.2019.2924045

[9] L. Jose, "Exploring IoT security issues and solutions." https://www.deviceauthority.com/blog/exploring-iot-security-issues-and-solutions/, 2023. accessed:2024-04-27.

[10] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, 2016. https://doi.org/10.1109/JIOT.2016.2579198

[11] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of things," IEEE Access, vol. 6, pp. 6900-6919, 2017. https://doi.org/10.1109/ACCESS.2017.2778504

[12] G. Singh, "Edge computing: Benefits and challenges." https://www.synopsys.com/blogs/chip-design/edge-computing-benefits-and-challenges.html, 2022. accessed:2024-04-27.

[13] A. Pradeep, "Exploring the future of edge computing: Advantages, limitations, and opportunities," in International Conference on Advanced Communication and Intelligent Systems, pp. 196-209, Springer, 2023. https://doi.org/10.1007/978-3-031-45124-9_15

[14] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5g network edge cloud architecture and orchestration,"

IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1657-1681, 2017. https://doi.org/10.1109/COMST.2017.2705720

[15] M. S. Ansari, S. H. Alsamhi, Y. Qiao, Y. Ye, and B. Lee, "Security of distributed intelligence in edge computing: Threats and countermeasures," The Cloud-to-Thing Continuum: Opportunities and Challenges in Cloud, Fog and Edge Computing, pp. 95-122, 2020. https://doi.org/10.1007/978-3-030-41110-7_6

[16] S. A. Bhat, I. B. Sofi, and C.-Y. Chi, "Edge computing and its convergence with blockchain in 5g and beyond: Security, challenges, and opportunities," IEEE Access, vol. 8, pp. 205340-205373, 2020. https://doi.org/10.1109/ACCESS.2020.3037108

[17] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," Proceedings of the IEEE, vol. 107, no. 8, pp. 1608-1631, 2019. https://doi.org/10.1109/JPROC.2019.2918437

[18] S. Nirenjena and D. Baskaran, "An investigation on distributed denial of service attack in edge computing," in 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 668-675, 2023. https://doi.org/10.1109/ICSSIT55814.2023.10061128

[19] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advances in Cryptology-CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15-19, 1999, Proceedings 19, pp. 388-397, Springer, 1999. https://doi.org/10.1007/3-540-48405-1_25

[20] K. Alsubhi, "A secured intrusion detection system for mobile edge computing," Applied Sciences, vol. 14, no. 4, p. 1432, 2024. https://doi.org/10.3390/app14041432

[21] T. Sipola, J. Alatalo, T. Kokkonen, and M. Rantonen, "Artificial intelligence in the iot era: A review of edge ai hardware and software," in 2022 31st Conference of Open Innovations Association (FRUCT), pp. 320-331, IEEE, 2022. https://doi.org/10.23919/FRUCT54823.2022.9770931

[22] C. Surianarayanan, J. J. Lawrence, P. R. Chelliah, E. Prakash, and C. Hewage, "A survey on optimization techniques for edge artificial intelligence (ai)," Sensors, vol. 23, no. 3, p. 1279, 2023. https://doi.org/10.3390/s23031279

[23] Z. Chang, S. Liu, X. Xiong, Z. Cai, and G. Tu, "A survey of recent advances in edge-computing-powered artificial intelligence of things," IEEE Internet of Things Journal, vol. 8, no. 18, pp. 13849-13875, 2021. https://doi.org/10.1109/JIOT.2021.3088875