IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Security Vulnerabilities in Edge Computing: A Comprehensive Review

Sahil Arora
Independent researcher
Staff Product Manager, Twilio Inc

Apoorva Tewari
Independent researcher
Senior Product Manager, Intuit Inc

Abstract—It is promising that edge computing has the ability to enhance cloud computing's functions. Keeping the internet safe from hackers and other security risks is crucial if people are going to keep using online services. Concerns about privacy and security have damaged the public's perception of the edge as a reliable paradigm. The goals that show how effectively a system can eliminate certain privacy and security concerns are known as security and privacy requirements. The purpose of this article is to provide readers with an overview of the many approaches used to tackle the privacy and security issues that arise in an edge computing setting. This research reviews the literature on the subject, illuminating the design, characteristics, and security concerns of edge computing along with potential solutions. Also, paper discussed the security vulnerabilities in edge computing and potential mitigation strategies. Furthermore, this study offers a comprehensive analysis of current research as well as future research prospects concerning edge computing's privacy and security concerns.

Keywords—Edge computing, Security vulnerabilities, edge computing architecture, security challenges, countermeasures

I. INTRODUCTION

The technology and applications of the IoT are permeating many parts of our lives, including smart homes, healthcare, and smart cities [1]. By 2020, experts anticipate that there will be 50 billion IoT devices, with tens of billions of goods already connected to the web [2][3]. The limited resources, such as processing power and storage, of IoT devices cause problems with privacy, security, reliability, and performance in IoT systems and applications. Connecting the IoT to the cloud improves several applications. Healthcare, smart homes[4], smart cities, smart meters, video surveillance, smart agriculture (like greenhouse environment-monitoring systems), smart transportation (like smart tourist destinations), and smart metering are a few examples of these uses. The IoT is able to get around its limited resources by utilising cloud computing.

In a cloud environment, data from IoT devices is continuously transferred from various applications to a central repository [5]. There are IoT applications that need real-time processing and minimal latency. Cloud computing is not a good fit for handling such needs [6]. Thus, in order to fulfil these demands using edge computing, it is crucial to deploy capabilities similar to cloud computing to the network's periphery [7].

One relatively new idea in computing is "edge computing," which refers to processing at the network's peripheral. The traditional model of cloud computing is changing. Moving processing closer to the point of data generation is the overarching goal [8]. Computing on the periphery of a network allows for the delivery of services and computations to be closer to the point of data generation. Edge computing seeks to relocate data processing, storage, and networking nodes away from central servers and towards the network's periphery. Offering intelligent services at the network edge may address critical IT sector demands in areas such as real-time business, data optimisation, application intelligence, security, privacy, low latency, and high bandwidth[9]. After make a recently-emerged IoT apps usable on the user's device, edge computing may be seen as a connection connecting IoTs to adjacent physical edge devices [10]. It is important to have a firm grasp of the technology, components, and their interplay (as seen in Figure 1) before delving into IoT edge computing designs.

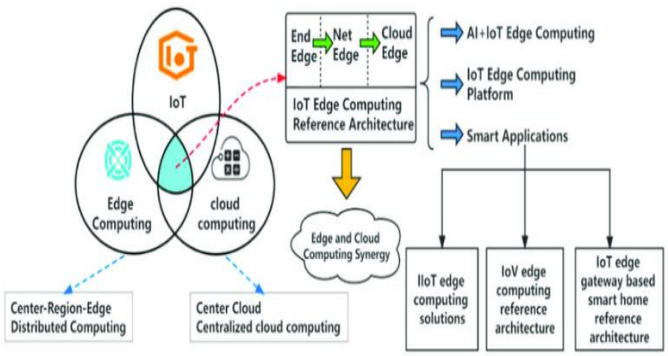

Figure 1: Edge Computing in IoT.

Despite its many advantages, edge computing is vulnerable to several privacy and security risks. One argument is that security concerns with cloud computing also affect edge computing since it is an outgrowth of cloud computing[11]. In contrast, an unique characteristics of edge computing, including its dispersed nature, heterogeneity, and low latency, provide additional obstacles to data privacy and security. Achieving secure data analytics requires the implementation of security measures. The usual security protocols suggested for cloud architecture are inapplicable to edge architecture owing to the limited resources of edge devices. It is critical to offer security solutions for this infrastructure to guarantee the dependability and effectiveness of IoT applications that depend on edge computing [12].

A. Research Motivation

The growth of IoT is beyond our expectations. Researchers are utilising the scope of IoT in all areas of modern computing. Several applications have emerged on top of IoT. The integration of modern technologies over IoT opened a large-scale platform to accommodate novel applications. The traditional architecture of IoT has a cloud-dependent architecture. The centralised architecture of the cloud server is capable of fulfilling all the basic needs of small-scale IoT applications. But the real-time applications expect accurate as well as dynamic responses. The cloud server is not capable to serve such needs of modern IoT applications due to several known constraints. Placing an edge node nearer to the execution environment can accomplish all such computational needs. Edge computing offers a good platform to support heterogeneous real-time applications of IoT. Numerous security concerns arise with a widespread use of edge devices. The following key objectives of this paper as:

- This work provides a comprehensive breakdown of Edge Computing architecture, detailing roles and functions of the terminal, boundary (edge), and cloud layers.
- Identification of Security Threats: The study methodically identifies security risks that exist at several levels of the Edge Computing architecture, such as core infrastructure threats, edge network threats, access network threats, and edge device security.
- Mitigation Strategies for Security Vulnerabilities: It proposes detailed mitigation strategies to address the vulnerabilities found in edge computing, such as encryption for insecure data transmission, automated security patching, and multi-factor authentication for access control.
- The work highlights the role of ML and DL in securing edge computing environments.
- This research provides a comparative analysis between traditional security measures (e.g., encryption, user behaviour profiling, intrusion detection) and advanced AI-driven approaches.
- It demonstrates how AI techniques can enhance the ability to detect sophisticated security breaches in real-time, making it a valuable contribution to the future of edge computing security.

B. Organization of the paper

This essay continues as follows: Sections II and III provide a synopsis of the edge computing design, features, and security risk issues. Section IV covers countermeasures for edge computing assaults. Section V discusses edge computing security flaws and possible solutions. Section VI includes an assessment of the literature based on a variety of research articles and research gaps. The final section of this work discusses the work's conclusion and next steps.

II. EDGE COMPUTING ARCHITECTURE AND CHARACTERISTICS

The federated network design shown in Figure 2 is an example of an edge-computing architecture, which uses devices at the network's periphery to transport cloud services to endpoints rather than the central data centre. The architecture for cloud-edge cooperation consists of three layers: cloud, edge, and terminal resources. A high-level overview of the components and functions of an edge-computing architecture is presented here[9][13].

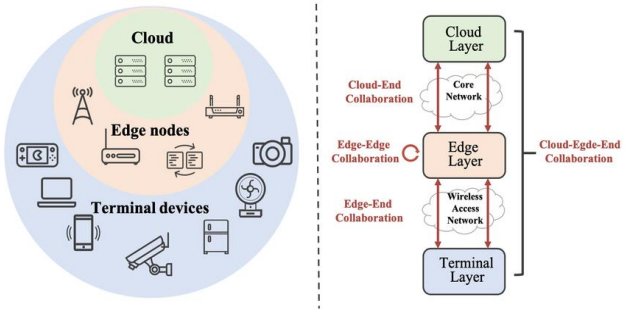

Figure 2: Architecture of Edge computing

- **Terminal Layer:**

The terminal layer encompasses all devices linked to the edge network, including mobile terminals and a wide range of IoT devices including sensors, phones, smart vehicles, cameras, and more. Both data consumption and data provisioning are carried out by the device at the terminal layer. Reduced terminal service latency is achieved not through increased processing power but by taking into consideration a perception of a different terminal devices.

- **Boundary Layer**

A middle layer supports a three-tier architecture. Periphery nodes, distributed throughout terminal devices and clouds, make up this layer of the network. Routing, switching, gateways, base stations, access points, etc. are common components. Edge computing and storage enables terminal devices downstream to access and process data uploaded by these devices.

- **Cloud Layer**

The cloud remains the most potent data processing hub for federated cloud-edge computing services. Applications that frequently analyse large amounts of data, like those involved in regular maintenance or supporting business decisions, might get an advantage from the numerous high-performance servers and storage devices found in the cloud computing layer.

A. Edge computing characteristics

Edge Computing Characteristics Edge computing shares several similarities with cloud computing. On the other hand, here are some of the attributes that set edge computing apart:

1) Dense Geographical Distribution

Edge computing uses several computing platforms deployed on edge networks to deliver Cloud services closer to the customer. The following are some benefits of the infrastructure's widely dispersed geographic location:

- Administrators of the network may enable location-based mobility services without having to go across the whole wide area network;
- Improved speed and accuracy are possible with big data analytics;
- Large-scale, real-time analytics are made possible by the Edge systems. Environmental sensor networks and pipeline monitoring systems are two examples.

2) Mobility Support

With a proliferation of mobile devices, edge computing has evolved to accommodate mobility by enabling protocols like Locator ID Separation Protocol (LISP), which allow for direct communication with mobile devices. The LISP protocol decouples the host's identification from the location's name in order to set up a distributed directory system.

3) Location Awareness

Edge computing has a location-aware capability that allows users of mobile devices to utilise services provided by an Edge server that is located closest to them. Wireless access points, GPS, and cell phone infrastructure are just a few of the technologies that users can use to find electronic devices.

4) Proximity

Compute resources and services are made accessible close to users in edge computing, which enhances their experience. After making offloading and service consumption choices, users may take advantage of network context information based on the nearby computing resources and services.

5) Low Latency

In order to decrease latency, computing resources and services are moved closer to consumers using edge computing concepts. In order to run applications that are both resource-intensive and delay-sensitive, users may take use of the low latency offered by Edge computing. These Edge devices can be anything from routers and access points to base stations and dedicated servers [14]

III. SECURITY THREAT CHALLENGES IN EDGE COMPUTING

This section outlines the suggested controls and ranks the security hazards linked to EC for each functional layer. Whether intentional or accidental, the goal of a threat is to remove, change, or damage anything of value by exploiting a security hole. Security Risks in Edge Computing are shown in Figure 3.

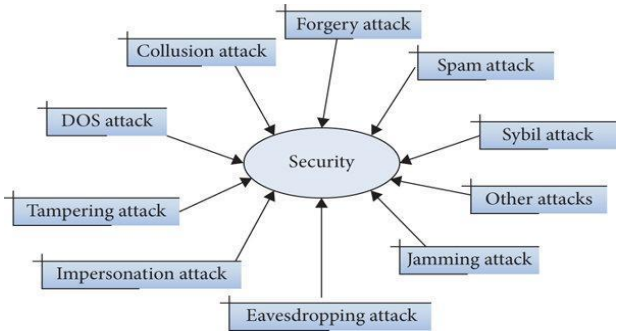

Figure 3: Security Threats in Edge Computing

A. Edge Device Security *Threats*

- **Information injection:** False information may be distributed when an attacker injects malicious data into a hacked device. The deliberate introduction of erroneous data into a system by opponents is known as poisoning. When malicious actors create misleading messages using fake data in an effort to steal sensitive information from unsuspecting nodes, this is known as outside forging. To illustrate the point, consider a scenario where an adversary in the smart manufacturing area deliberately delays valve activation by injecting false pressure readings, with the goal of damaging equipment.
- **Eavesdropping:** To get sensitive information, cybercriminals intercept communications using communication channels.
- **Side-channel attacks:** An objective is to get confidential and sensitive data by means of covert access to user equipment. This kind of attack targets location, email, login credentials, and passwords. A potential solution for virus detection in UEs with limited resources might be an IDS or IPS that uses ML techniques.

B. Access Network Security Threats

- **Denial of Service:** Attacks on digital networks may take several forms, including DDoS and wireless jamming. It is more likely that compromised VMs would coordinate in a large-scale assault, such as a DDoS, when Virtual Machines (VMs) coexist over several MEHs[15], [16].
- **Rogue gateway:** An adversary with ill intentions may theoretically construct and launch unauthorised gateways into the distributed MEC architecture, giving them access to sensitive data [17],[18]. The creation of backdoor access to sensitive resources may be a serious concern when unauthorised gateways gain access to network equipment, applications, and edge services.

C. Edge Network Threats

- **Privilege escalation:** An attacker may escalate their privileges to control otherwise limited resources by taking advantage of a security hole in the system or an application's design, code, or configuration. The hostile user may install malware, carry out administrator commands, steal confidential data, and even seriously damage server applications with their newly acquired unauthorised rights.
- **Rogue data centre:** In comparison to more traditional cloud settings, the edge network lacks both manageability and security. Within this threat scenario, an adversary might potentially gain control of a whole edge network and affect interactions with external systems through methods such as privilege escalation or the introduction of malicious infrastructure that imitates an edge network device. The enemy would be situated between the UE and a data centre in the core.

D. Core Infrastructure Security Threats

- **ICT attacks:** An ICT attack occurs when an intruder tries to gain unauthorised access to a system or device in order to steal data or take over the hardware it runs on. Included in this category are assaults such as eavesdropping, identity theft, Sybil, tampering with data, background knowledge, cooperation, and outside forgeries.
- **Rogue infrastructure:** Consistent with the results shown for rogue infrastructure in the V-C edge network, this danger might allow attackers to take control of applications and services hosted on EC nodes if they manage to target certain parts of the core infrastructure[19][20]

IV. SECURITY VULNERABILITIES IN EDGE COMPUTING WITH MITIGATION STRATEGIES

Here is Table 1 summarising the security vulnerabilities in edge computing and potential mitigation strategies:

Table 1: Security Vulnerabilities in Edge Computing and Potential Mitigation Strategies

Vulnerability	Description	Mitigation Strategies
Limited Physical Security	Edge devices deployed in insecure locations are vulnerable to tampering or theft.	Implement physical security measures, tamper detection, and encryption of data stored on the device.
Insecure Data Transmission	Data transmitted between edge devices and central systems is susceptible to attacks.	Use strong encryption (TLS/SSL) and secure communication protocols for all data transfers.
Resource Constraints	Edge devices have limited resources for security mechanisms like encryption or firewalls.	Utilise lightweight security frameworks and prioritise essential security measures, like encryption and IDS.
Distributed Nature	Each edge device increases the attack surface due to decentralised architecture.	Apply a zero-trust architecture and implement endpoint protection and monitoring.
Inadequate Security Updates	Difficulty in applying regular security patches, leading to outdated software.	Implement automated or remote update mechanisms to ensure timely security patches.
Authentication and Access Control	Weak or insufficient authentication can lead to unauthorised access.	Use multi-factor authentication, role-based access control (RBAC), and strong identity management.
Malicious Code Execution	Edge devices are vulnerable to malware and ransomware.	Deploy antivirus solutions, endpoint detection and response (EDR), and use containerisation to isolate processes.
Insider Threats	Physical access by malicious insiders increases risk.	Implement strict access control, monitoring, and logging of device activities, and use tamper-proof hardware.
Lack of Standardization	Lack of unified security standards across edge devices.	Adopt industry-wide security standards and best practices specific to edge computing environments.
Data Privacy and Compliance	Sensitive data processed at the edge may lead to privacy breaches.	Ensure compliance with data protection regulations and use data anonymisation and encryption.
Denial of Service (DoS) Attacks	Edge devices can be overwhelmed by excessive requests due to limited resources.	Use rate limiting, traffic filtering, and distributing load across multiple devices to mitigate DoS attacks.

V. COUNTERMEASURE FOR ATTACKS IN EGDE COMPUTING

The security protocols employed by cloud computing providers are incompatible with the distinctive features of the edge computing concept. Therefore, below are a few solutions that tackle the distinct features of edge computing:

A. Non-AI Solutions

For complete security in EC-IoT settings, traditional countermeasures are crucial. An effective defence framework is formed by these strategies.

- **Edge Node Security:** To provide appropriate safety procedures, each node in the edge network must adhere to the same stringent security measures. An attacker with access to higher-level security measures might compromise the system by exploiting a vulnerable node with an inadequate security algorithm.
- **Full-time Monitoring:** To keep malicious users out of the network, network security necessitates constant edge node monitoring and giving users interactive interface access to the network.
- **Proper Encryption:** The development of more sophisticated and difficult-to-decipher encryption algorithms is a direct result of the rapid pace at which technology is progressing. In order for these algorithms to work, the secret key must be securely stored and exchanged only between the authorised sender and recipient.
- **Intrusion Detection System:** This system is designed to alert a user in the event that it identifies any suspicious behaviour or attempts to gain unauthorised access.
- **User Behavior Profiling:** The phrase "user behaviour profiling" describes the process of keeping track of users' typical actions so that any deviation from the norm may be used to identify potentially harmful people.
- **Cryptographic Techniques:** In response to security breaches caused by hackers and other attackers, cryptographic methods are being considered. Most of these methods rely on an encrypted key that can only be known by the sender and the recipient.
- **Data Confidentiality:** To solve the various privacy issues brought on by network attackers' illegal data activities, data loss, manipulation, breach, etc., a number of encryption-based data confidentiality solutions have been proposed[21]

B. AI solutions

Securing EC-IoT environments has also undergone a radical change due to the AI age. AI techniques, in particular ML and DL, provide sophisticated solutions for recognising and thwarting a variety of security risks by seeing minute patterns and abnormalities that conventional techniques would overlook.

- **Machine Learning:** ML approaches provide strong mechanisms for detecting and mitigating diverse threats, which is crucial for EC-IoT system security. SVMs are employed for assaults that target the network level. Attacks that target applications often make use of decision trees and naive Bayes classifiers. PCA and KNN are used for assaults on the data level.
- **Deep Learning:** Due to their advanced mechanisms for detecting and mitigating different kinds of assaults, DL techniques are essential in improving the security of EC-IoT systems. Network traffic patterns are analysed using CNNs, which are used to spot abnormalities suggestive of network-level assaults. Time-series analysis of network traffic using RNNs, such as LSTMs, is useful for identifying temporal irregularities.

VI. LITERATURE REVIEW

This section provides the existing work in the field of secure data management with edge computing.

This paper, Jin et al., (2020) suggests using secure edge computing to manage people, data, devices, and other services. This is accomplished by installing separate microservices providers on edge gateways and combining them with security gateways. The suggested edge gateway combines client support with security measures to make it easier for clients to

communicate with IoT devices, which in turn allows users to access and visualise secure edge services[22].

This paper, Fan et al., (2018) offers a safe method for data sharing between domains using the edge computing model; in this architecture, each domain consists of a computational node and controlled edge equipment; and with the cloud connecting all of these domains, the authentication issue across domains is easily solved. Data confidentiality and one-to-many sharing are maintained via an use of CP-ABE and the RSA method. At last, the results of the analysis prove that our plan is safe[23].

This research, Pepito and Dutta, (2021) draw attention to a 5G security testbed that was created to examine the security of edge computing and is open-source. Testbed findings show that QoS, packet loss, packet corruption, delay distribution, and edge/central cloud server interface management are possible. Additionally, these simulations are compared with one another. This section discusses the essential background research as well as current work on edge computing security challenges and mitigating approaches[24].

The paper, Yahuza et al., (2020) delves into the existing research and draws attention to the following: how edge computing security and privacy requirements are classified, the most recent methods utilised to combat these threats, the trends in the technical methods used by these methods, the metrics used to measure how well these methods worked, the types of attacks that impact edge networks, the techniques used to mitigate these attacks, and potential avenues for future research in this area[25].

This research, Caprolu et al., (2019) gives a rundown of primary technologies supporting an Edge paradigm, assesses the existing state of affairs, gives relevant scenarios, and finally examines the advantages and disadvantages of the several solutions put up to address these issues. Finally, we address the present security concerns in the new environment and try to sketch out potential future research directions for security and technological advancement in different Edge/Fog situations[26].

This paper, Tesei et al., (2021) examines the MEC system's privacy and security measures. They have provided an extensive analysis of threat vectors in the ETSI-standardized MEC design. They also provide possible security solutions to address the weaknesses that led to the detected attack vectors. Also discussed are the privacy concerns with MEC, and concrete goals for protecting personal information are laid forth. Lastly, they lay forth plans for the future that will strengthen the privacy and security of MEC services[27].

Table 2 shows the Related work summary for secure edge computing based on methodology, performance and limitation/future work.

Table 2: Related work summary for secure edge computing

Reference	Methodology	Performance	Limitations & Future Work
[22]	Secure edge computing using independent microservices providers and a security gateway on an edge gateway to manage devices, data, and users.	Enabled secure communication between IoT clients and devices for secure services, including access and visualisation.	May require robust infrastructure to support microservices; scalability and real-time processing challenges. Future work could explore optimisations in edge gateway design, microservice scaling, and real-time processing solutions.
[23]	Secure data sharing across domains via edge computing model, using RSA and CP-ABE for confidentiality and one-to-many data sharing.	Provides secure data sharing among different domains and ensures confidentiality with RSA and CP-ABE encryption.	High computational cost due to RSA and CP-ABE, and potential bottlenecks in multi-domain authentication. Future work could focus on developing lightweight encryption schemes and improving authentication efficiency.
[24]	Open-source 5G security testbed developed for edge computing security research, with video streaming as proof-of-concept.	Displays command over latency, packet loss, and quality of service for interfaces with both central and edge cloud servers.	Limited scope of testing, focusing mainly on latency and packet quality without covering other security aspects. Future work could expand scenarios to include diverse applications and explore more security challenges in 5G edge environments.
[25]	Review of security and privacy requirements in edge computing, classification of attacks and techniques, and analysis of current technological trends.	Finding critical parameters for assessment, this article examines the current level of edge computing security and privacy.	Primarily theoretical analysis with a lack of empirical validation. Future work should develop empirical studies to validate findings and explore real-world applications of security/privacy techniques.
[26]	Survey of key technologies supporting edge computing, including scenarios, benefits, caveats, and security issues.	Provides a detailed discussion of existing security solutions and outlines future research directions.	Generalised discussion without specific security solution focus or validation through case studies. Future work could include case studies or simulations to assess the effectiveness of proposed solutions in real-world scenarios.
[27]	Examination of potential privacy and security risks in MEC systems, with a focus on the architecture that has been standardised by ETSI.	Provides an in-depth analysis of MEC vulnerabilities and proposes potential security solutions.	Does not fully explore privacy implications or scalability of proposed solutions. Future work could investigate scalability and develop privacy-preserving techniques for MEC systems.

VII. CONCLUSION AND FUTURE WORK

An exciting new paradigm, edge computing seeks to do away with almost all of cloud computing's negative aspects. Many people are hesitant to use it because of concerns about security and privacy. This study discusses various aspects of edge computing that provide insights into its architecture, unique security challenges and potential solutions. Data integrity and privacy must be guaranteed in dispersed networks via strong security frameworks, as this paper emphasises the consequences of decentralisation, resource restrictions, and device heterogeneity. The increased dispersion and volatility of the edge computing environment compared to the static cloud makes data security and privacy assurance a more formidable challenge. Future research should focus on addressing the existing limitations and exploring new opportunities for blockchain in cybersecurity. This includes developing more sophisticated cryptographic techniques and key management systems to mitigate risks associated with private key theft. It will also be critical to investigate potential regulatory frameworks and create scalable systems to deal with the ever-increasing data and transaction volumes.

REFERENCES

[1] M. Aazam, S. Zeadally, and K. A. Harras, "Fog Computing Architecture, Evaluation, and Future Research Directions," *IEEE Commun. Mag.*, 2018, doi: 10.1109/MCOM.2018.1700707.

[2] S. Talwar, D. Choudhury, K. Dimou, E. Aryafar, B. Bangerter, and K. Stewart, "Enabling technologies and architectures for 5G wireless," in *IEEE MTT-S International Microwave Symposium Digest*, 2014. doi: 10.1109/MWSYM.2014.6848639.

[3] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[4] S. Y. Chen, C. F. Lai, Y. M. Huang, and Y. L. Jeng, "Intelligent home-appliance recognition over IoT cloud network," in *2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013*, 2013. doi: 10.1109/IWCMC.2013.6583632.

[5] S. Almajali, H. B. Salameh, M. Ayyash, and H. Elgala, "A framework for efficient and secured mobility of IoT devices in mobile edge computing," in *2018 3rd International Conference on Fog and Mobile Edge Computing, FMEC 2018*, 2018. doi: 10.1109/FMEC.2018.8364045.

[6] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet Things J.*, 2016, doi: 10.1109/JIOT.2016.2579198.

[7] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-computing architectures for internet of things applications: A survey," *Sensors (Switzerland)*. 2020. doi: 10.3390/s20226441.

[8] M. Satyanarayanan, "The emergence of edge computing," *Computer (Long. Beach. Calif).*, 2017, doi: 10.1109/MC.2017.9.

[9] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An Overview on Edge Computing Research," *IEEE Access*. 2020. doi: 10.1109/ACCESS.2020.2991734.

[10] M. Talebkhah, A. Sali, M. Marjani, M. Gordan, S. J. Hashim, and F. Z. Rokhani, "Edge computing: Architecture, Applications and Future Perspectives," in *IEEE International Conference on Artificial Intelligence in Engineering and Technology, IICAIET 2020*, 2020. doi: 10.1109/IICAIET49801.2020.9257824.

[11] S. G. Priya Pathak, Akansha Shrivastava, "A survey on various security issues in delay tolerant networks," *J Adv Shell Program.*, vol. 2, no. 2, pp. 12–18, 2015.

[12] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, 2019, doi: 10.1109/JIOT.2019.2897619.

[13] R. P. Vamsi Krishna Yarlagadda, "Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity," *Eng. Int.*, vol. 6, no. 2, pp. 211–222, 2018.

[14] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2019.02.050.

[15] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Communications Surveys and Tutorials*. 2020. doi: 10.1109/COMST.2019.2933899.

[16] V. K. Y. Nicholas Richardson, Rajani Pydipalli, Sai Sirisha Maddula, Sunil Kumar Reddy Anumandla, "Role-Based Access Control in SAS Programming: Enhancing Security and Authorization," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 6, no. 1, pp. 31–42, 2019.

[17] J. Okwuibe, M. Liyanage, I. Ahmad, and M. Ylianttila, "Cloud and MEC security," in *A Comprehensive Guide to 5G Security*, 2018. doi: 10.1002/9781119293071.ch16.

[18] H. Ge, D. Yue, X. Xie, S. Deng, and C. Dou, "A unified modeling of muti-sources cyber-attacks with uncertainties for CPS security control," *J. Franklin Inst.*, 2021, doi: 10.1016/j.jfranklin.2019.01.006.

[19] A. Shaik, R. Borgaonkar, S. Park, and J. P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols : Exposing device capabilities," in *WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks*, 2019. doi: 10.1145/3317549.3319728.

[20] B. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," *IEEE Access*. 2021. doi: 10.1109/ACCESS.2021.3053233.

[21] A. M. Alwakeel, "An overview of fog computing and edge computing security and privacy issues," *Sensors*, 2021, doi: 10.3390/s21248226.

[22] W. Jin, R. Xu, T. You, Y. G. Hong, and D. Kim, "Secure edge computing management based on independent microservices providers for gateway-centric IoT networks," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3030297.

[23] K. Fan, Q. Pan, J. Wang, T. Liu, H. Li, and Y. Yang, "Cross-domain based data sharing scheme in cooperative edge computing," in *Proceedings - 2018 IEEE International Conference on Edge Computing, EDGE 2018 - Part of the 2018 IEEE World Congress on Services*, 2018. doi: 10.1109/EDGE.2018.00019.

[24] R. Pepito and A. Dutta, "Open Source 5G Security Testbed for Edge Computing," in *Proceedings - 2021 IEEE 4th 5G World Forum, 5GWF 2021*, 2021. doi: 10.1109/5GWF52925.2021.00075.

[25] M. Yahuza *et al.*, "Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2989456.

[26] M. Caprolu, R. Di Pietro, F. Lombardi, and S. Raponi, "Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues," in *Proceedings - 2019 IEEE International Conference on Edge Computing, EDGE 2019 - Part of the 2019 IEEE World Congress on Services*, 2019. doi: 10.1109/EDGE.2019.00035.

[27] A. Tesei, M. Luise, P. Pagano, and J. Ferreira, "Secure Multi-access Edge Computing Assisted Maneuver Control for Autonomous Vehicles," in *IEEE Vehicular Technology Conference*, 2021. doi: 10.1109/VTC2021-Spring51267.2021.9449087.