Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 421–430
DOI : 10.47974/JDMSC-1898

Ensuring data confidentiality and integrity in edge computing environments : A security and privacy perspective

Rohini Suhas Kale [§]
Department of Polytechnic and Skill Development
Dr. Vishwanath D. Karad MIT world Peace University
Pune
Maharashtra
India

Jayashri Hase [†]
Department of Computer Science and Design
K. K. Wagh Institute of Engineering Education and Research
Nashik
Maharashtra
India

Shyam Deshmukh *
Department of Information Technology
Pune Institute of Computer Technology
Savitribai Phule Pune University
Pune
India

Samir N. Ajani [‡]
Department of Computer Science and Engineering (Data Science)
Shri Ramdeobaba College of Engineering and Management
Nagpur
Maharashtra
India

[§] *E-mail:* rohini.kale@mitwpu.edu.in
[†] *E-mail:* jshase@kkwagh.edu.in
* *E-mail:* dshyam100@yahoo.com (Corresponding Author)
[‡] *E-mail:* samir.ajani@gmail.com

Pratik K Agrawal [@]
Department of Computer Science & Engineering
Organization- Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Maharashtra
Pune
India

Chhaya Sunil Khandelwal [#]
Department of Electronics & Telecommunication
MGMU Jawaharlal Nehru Engineering College
Chhatrapati Shambhajinagar
Maharashtra
India

Abstract

This study examines, from a security and privacy standpoint, the significant obstacles to maintaining data integrity and confidentiality in edge computing contexts. Data security at the edge becomes critical as more and more edge devices proliferate and generate large volumes of sensitive data. The review of the literature looks at edge computing security problems that currently exist and discusses fixes to protect data integrity and confidentiality. The article explores various vulnerabilities, emphasizing the necessity for strong security systems, including data exposure risks and integrity concerns. It examines secure communication protocols, access control methods, and encryption techniques as crucial risk-reduction instruments. Anonymization and differential privacy are two privacy-preserving techniques that are investigated to find a middle ground between user privacy and data value. The article provides real-world insights through case studies and actual implementations, and it lays out metrics and evaluation criteria for determining how successful security measures are. Finally, the report highlights the need of addressing data security in changing edge computing settings and offers future directions and research difficulties.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Data confidentiality, Data security, Edge computing, Privacy preservation, Security.*

1. Introduction

The introduction of edge computing has completely changed how data is used and handled by moving processing closer to the point where the data is generated. The security and privacy issues that arise with edge

[@] *E-mail:* **pratik.agrawaal@gmail.com**
[#] *E-mail:* **ckhandelwal@mgmu.ac.in**

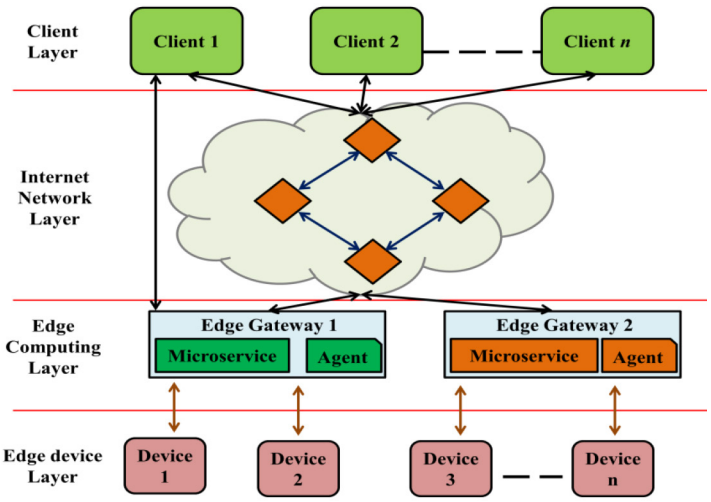

Figure 1

Overview Secure edge computing environment

devices are becoming more and more important to handle as they become a crucial part of our connected environment as shown in Figure 1. The important job of protecting data integrity and confidentiality in edge computing settings is the main topic of this article, which provides a thorough analysis from a security and privacy standpoint [1]. The spike in data generation at the edge of networks, where IoT sensors and smartphones process information locally, is driving the emergence of edge computing. Although this paradigm change improves real-time processing capabilities, it also adds new layers of vulnerability, hence a strong security framework is required.

This paper seeks to give a comprehensive overview of the issues and offer practical solutions in light of the growing security and privacy concerns in the era of edge computing. The [2] literature review summarizes the current situation of edge computing security by outlining the problems that still need to be solved and reviewing earlier studies. The study examines encryption methods, access control systems, and secure communication protocols as essential elements of an all-encompassing security strategy, recognizing the importance of data confidentiality and integrity [3]. A careful balance between data utility and individual privacy is necessary, since the debate also touches on privacy-preserving techniques like anonymization and differential privacy. This paper connects theoretical frameworks with actual applications by exploring

case studies and real-world implementations, providing insights into the difficulties and accomplishments of implementing security measures in various edge computing settings [4]. The next sections will examine novel technologies and frameworks, address particular security and privacy issues, and suggest future paths to strengthen edge computing environments' security posture in a constantly changing digital context.

2. Method and Material

2.1 *Data Exposure Risks*

2.1.1. Edge devices vulnerabilities

From smart gadgets to sensors, edge devices frequently have limited resources and might not have the same strong security measures as standard computing systems. They are [5] vulnerable to exploits by hostile parties because of this inherent restriction. Unauthorized access, malware injection, and physical manipulation are common risks. Implementing security measures like device authentication, frequent software upgrades, and secure boot techniques to guarantee the integrity of the device's firmware are necessary to address these issues.

2.2 *Integrity Threats*

2.2.1 Tampering risks at the edge

Because edge [6] environments are physically accessible, there is a chance that unauthorized people will tamper with them and alter or

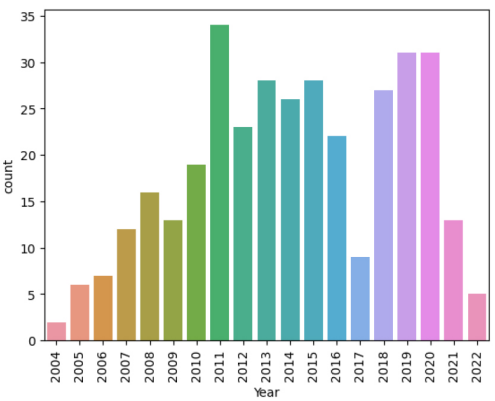

Figure 2

Data breach over the year

undermine the integrity of the data at the source. This can entail tampering with sensor readings or sending erroneous information into the edge system. Physical security measures combined with the use of tamper-resistant software and hardware techniques help reduce these threats. Furthermore, [7] the integrity and authenticity of the software operating on edge devices can be guaranteed using methods like code signing and integrity checks. Figure 2 shows the a amount of data breach cases found over the years.

3. Frameworks and Technologies for Data Security

3.1 *Encryption Techniques at the Edge*

3.1.1 Symmetric and asymmetric encryption

One of the most important components in ensuring data confidentiality is encryption. In order to ensure efficient processing, symmetric encryption uses a single secret key for both encryption and decryption [8]. It can be difficult to distribute and manage secret keys safely, though. This problem is solved by asymmetric encryption, which uses a pair of public and private keys. It needs more processing power even though it is more secure. The particular use case and available resources will determine whether type of encryption symmetric or asymmetric is used in edge computing.

a. Triple DES:

- **Key Generation:**
  Generate three 56-bit keys (K1, K2, K3) from a 168-bit key
- **Initial Permutation (IP):**
  Permute the 64-bit plaintext block according to the initial permutation table.
- **Encryption:**
  a. First Encryption (DES Round 1):
  - Apply the DES algorithm using Key K1.

$$L_o = Ppermuted\,[:32]$$

$$R_o = Ppermuted\,[32:]$$

and for each round

$$Li = Ri - 1$$

$$Ri = Li - 1 \oplus f(Ri - 1, Ki)$$

b. Decryption:

- Apply the DES algorithm in decryption mode using Key K2.

c. Second Encryption (DES Round 2):

- Apply the DES algorithm using Key K3.

- **Final Permutation (FP):**

  Permute the 64-bit ciphertext block according to the final permutation table.

$$Ciphertext = Ppermuted - 1\ (R16)$$

3.1.2 Homomorphic encryption for edge devices

Homomorphic encryption protects data privacy during processing by allowing computation on encrypted material without first decrypting it. When homomorphic encryption is used in edge devices, sensitive data can be processed securely without being vulnerable to outside threats [9]. While homomorphic encryption is computationally demanding, advances in cryptographic algorithms and technology make it more practical for edge devices with limited resources, improving their ability to carry out safe computations [10].

3.2 *Access Control Mechanisms*

3.2.1 Role-based access control

RBAC is a popular access control mechanism that limits user access to the system according to their responsibilities. By ensuring that people have access privileges that are in line with their roles, RBAC implementation in edge environments reduces the possibility of unauthorized access. By lowering the attack surface and limiting rights to the absolute minimum required for each position, this streamlines access management and improves security [11].

3.2.2 Attribute-based access control for edge environments

Attribute-based access control (ABAC) offers a versatile solution for context-aware access control in dynamic edge environments. When

providing access, ABAC takes into account a number of factors, including user identification, device status, and ambient conditions. The overall security posture of edge computing systems is enhanced by the more adaptable and sophisticated access policies made possible by this fine-grained control [12].

4. Privacy-Preserving Approaches

4.1 *Anonymization Techniques*

4.1.1 Data anonymization at the edge

To preserve individual privacy, data anonymization is converting or eliminating personally identifying information (PII) from datasets. Handling sensitive data produced by devices requires the implementation of edge anonymization techniques. Techniques like differential privacy and k-anonymity help to mask certain information so that data can still be used for analysis without allowing for individual identification. This strategy is especially useful in edge contexts where data is frequently gathered from many sources.

4.2.2 Preserving user privacy in edge scenarios

In edge scenarios, user privacy protection goes beyond simple anonymization. It takes a comprehensive approach, taking user context and behavior into account in addition to data. Methods that help protect user privacy include pseudonymization, which substitutes pseudonyms for identifiable information. Furthermore, preserving privacy and building user confidence in edge computing systems depend on transparent data processing procedures and informed consent processes.

5. Discussion

Assess the system's resistance to various forms of attack, making sure it can tolerate malware, intrusion attempts, and denial-of-service attacks. Reduce the likelihood of unwanted access by double-checking authorization and authentication.

Analyze the level of data encryption while taking key management and assault resistance against cryptography into account. Assess the effectiveness of the processes for incident response and recovery, which are essential for handling security problems quickly. Make sure that regulations are followed in order to protect sensitive data and comply

Table 1

Result for DES and 3DES encryption on different set of data size

Data Size	Parameter	Latency (ms)	Processing speed (MB/S)
160	DES	5	100
160	3DES (EDE)	4.6	30
160	3DES (EEE)	4.1	25
220	DES	8	120
220	3DES (EDE)	5.23	55
220	3DES (EEE)	5.82	50
260	DES	10	256
260	3DES (EDE)	6.22	65
260	3DES (EEE)	6.45	62

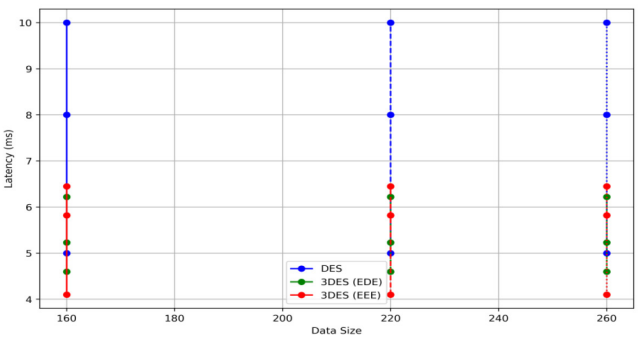

Figure 3

Latency Comparison between DES and 3DES

with legal obligations. The data that is supplied shows how varying data sizes affect processing speed and delay when using different encryption techniques. Comparing DES to its 3DES counterparts (EDE and EEE), with a 160-bit data size, DES shows reduced latency and faster processing speed, illustrating the trade-off between security and performance.

The speed difference grows as the data size reaches 220 and 260 bits, highlighting 3DES's computational overhead. These findings emphasize the necessity for cautious algorithm selection depending on the application's security requirements and computing limits, even though DES is still more efficient. This is especially true as data amounts and encryption demands increase. Table 1, Figure 3 and 4 shows the results of encryption on different datasets.

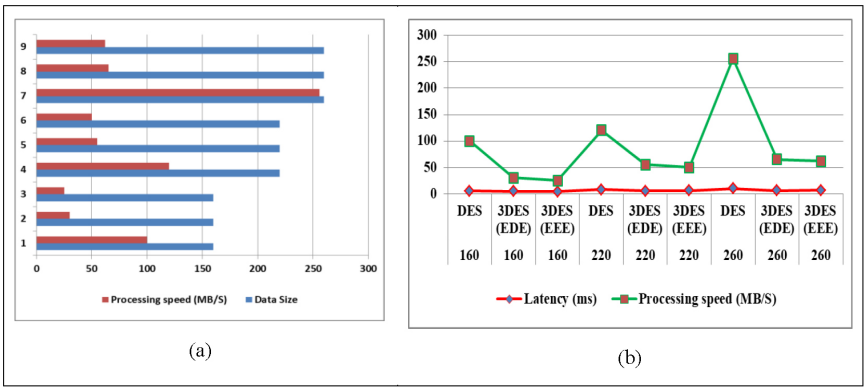

Figure 4

Performance parameter comparison for encryption model (a) Processing Speed (b) Latency and processing speed

6. Conclusion

Ensuring the secure and reliable functioning of decentralized systems in edge computing environments requires taking great care to protect data confidentiality and integrity. This article addresses issues specific to edge computing's dynamic nature by delving into the complex world of security and privacy considerations. A thorough security framework can be created by assessing factors including attack resistance, authentication precision, encryption strength, incident response effectiveness, and regulatory compliance. This architecture adjusts to new hazards in the dynamic edge environment in addition to providing protection against established threats. Metrics including data minimization, anonymity levels, consent management efficacy, and de-identification accuracy offer a detailed picture of privacy preservation initiatives. It is crucial to strike a balance between the practical applications of data analytics and privacy concerns. This calls for the cautious application of anonymization techniques and observance of user consent guidelines.

References

[1] Y. Hou, S. Garg, L. Hui, D. N. K. Jayakody, R. Jin and M. S. Hossain, "A Data Security Enhanced Access Control Mechanism in Mobile Edge Computing," in IEEE Access, vol. 8, pp. 136119-136130 (2020).

[2] Y. He, L. Chen, Y. Ni, Y. Wang, J. Li and Y. Li, "Privacy protection scheme for edge computing based on function encryption," 2021

International Conference on Networking and Network Applications (NaNA), Lijiang City, China, pp. 131-135 (2021).

[3] A. Sebbar and M. Boulmalf, "BCDS-SDN: Privacy and Trusted Data Sharing Using Blockchain Based on a Software-Defined Network's Edge Computing Architecture," ICC 2023 - IEEE International Conference on Communications, Rome, Italy, pp. 6578-6583 (2023).

[4] G. Simpson, Q. -A. Kester and L. Nana, "A Symmetric Encription Scheme for Electronic Data Exchange for Edge Medical Devices in a Dew-Fog Computing Environment," 2019 International Conference on Mechatronics, Remote Sensing, Information Systems and Industrial Information Technologies (ICMRSISIIT), Ghana, pp. 1-5 (2019).

[5] X. Guo, H. Lin, Z. Li and M. Peng, "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT", IEEE Internet Things J., vol. 7, no. 7, pp. 6242-6251, Jul. (2020).

[6] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu and T. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted Internet of Things", *IEEE Internet Things J*., vol. 7, no. 4, pp. 2679-2689, Apr. (2020).

[7] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for Resource Allocation of Grid Computing," in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.

[8] W. S. Shi, H. Sun, J. Cao, Q. Zhang and W. Liu, "Edge computing-an emerging computing model for the Internet of everything era", *J. Comput. Res. Develop*., vol. 54, no. 5, pp. 907-924, Feb. (2017).

[9] H. Li, G. Shou, Y. Hu and Z. Guo, "Mobile edge computing: Progress and challenges", Proc. 4th IEEE Int. Conf. Mobile Cloud Comput. Services Eng. (MobileCloud), pp. 83-84, Mar. (2016).

[10] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography,* 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

[11] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, G. Wang, T. Wang, M. M. Ahmed, et al., "Economic perspective analysis of protecting big data security and privacy", *Future Gener. Comput. Syst*., vol. 98, pp. 660-671, Mar. (2019).

[12] J. L. Zhang, Y. C. Zhao, B. Chen, F. Hu and K. Zhu, "Survey on data security and privacy-preserving for the research of edge computing", *J. Commun.*, vol. 39, no. 3, pp. 1-21, Mar. (2018).