Security Implications of Edge Computing in Cloud Networks

Sina Ahmadi

Scientific Research Publishing

Journal of Computer and Communications, 2024, 12, 26-46
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Security Implications of Edge Computing in Cloud Networks

Sina Ahmadi

National Coalition of Independent Scholars (NCIS), Seattle, USA
Email: sina0@acm.org

How to cite this paper: Ahmadi, S. (2024) Security Implications of Edge Computing in Cloud Networks. *Journal of Computer and Communications*, **12**, 26-46.
https://doi.org/10.4236/jcc.2024.122003

Received: January 6, 2024
Accepted: February 6, 2024
Published: February 9, 2024

Abstract

Security issues in cloud networks and edge computing have become very common. This research focuses on analyzing such issues and developing the best solutions. A detailed literature review has been conducted in this regard. The findings have shown that many challenges are linked to edge computing, such as privacy concerns, security breaches, high costs, low efficiency, etc. Therefore, there is a need to implement proper security measures to overcome these issues. Using emerging trends, like machine learning, encryption, artificial intelligence, real-time monitoring, etc., can help mitigate security issues. They can also develop a secure and safe future in cloud computing. It was concluded that the security implications of edge computing can easily be covered with the help of new technologies and techniques.

Keywords

Edge Computing, Cloud Networks, Artificial Intelligence, Machine Learning, Cloud Security

1. Introduction

Edge computing is a distributed information technology architecture in which the client's data is processed at the network's periphery, which means the processing is done near the point where the data has been originally generated [1]. Data is considered one of the major assets of modern businesses that provide valuable insights and are also integral in making important decisions to run business operations smoothly. The rush of data can be controlled and managed with an appropriate system that ensures data is protected from unauthorized access and can be operated in real-time from different locations and connected devices. Managing the data flow by integrating a traditional cloud computing network is challenging. That's why there is a need for edge computing in cloud networks, so

a proper flow of information is ensured. The data processing and analysis process is completed at the point where the data is originally generated instead of transmitting the raw data to a central data center.

Security of data and resources is the most important thing to consider, no matter what field or industry it is. Similarly, edge computing also demands the security of shared data among all the connected devices and users. For this purpose, it is important to implement innovative and creative tools and techniques that ensure vulnerability management, intrusion detection, and prevention. Security must be extended to IoT devices and sensor devices, as every device connected to this cloud network can get hacked by unauthorized users. Other risks may be related to data storage, perimeter defense, authentication, physical attacks, malicious hardware/software injections, and many more. This research aims to conduct a literature review of past studies focusing on edge computing in cloud networks, so that the security implications can be understood deeply. Figure 1 shows how edge computing works.

2. Literature Review

2.1. Security in Traditional Cloud Environments

Traditional cloud networks face many security issues and threats. A study by [3] was also conducted in this regard. According to the researchers, cloud computing is becoming very common and has many benefits regarding remote access, improved IT infrastructure, cost efficiency, etc. However, there is a need to focus on the associated privacy and security issues in cloud environments. It was observed that clouds can suffer from different threats such as back doors, trojans,

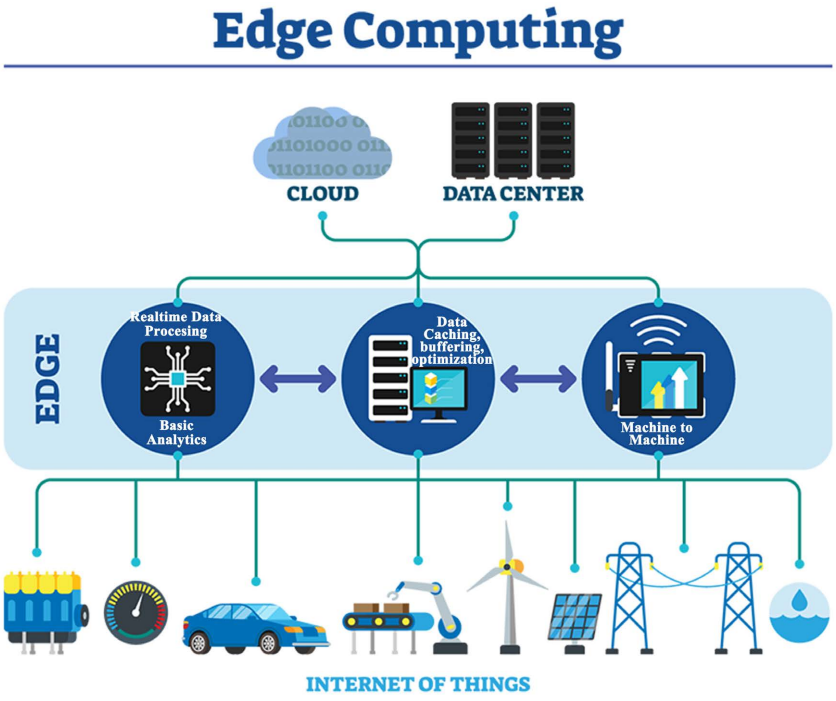

Figure 1. Edge computing [2].

viruses, etc. Tampering is another example of such a challenge in which the threat directly changes the whole system, such as XML positioning, which leads to complete system malfunction. Besides, in the case of repudiation, the authoring information of actions is modified by a malicious user. Moreover, a denial-of-service attack can occur in this case, where the hacker prevents authentic users from accessing the data. All such security issues must be overcome through proper security protocols and practices. Figure 2 shows the traditional cloud computing environment.

Research by [5] focused on analyzing the security protocols that can be used to overcome the challenges faced in a cloud environment. The research showed that companies can implement cloud computing deployment models to overcome such issues. The implementation of user-centric cloud accountability is equally important in this regard. An example of such a framework is Trust Cloud, which develops abstraction layers in the cloud. It acts as a detective to identify security threats in the cloud. Another important feature is Digital Identity Management, which helps limit access controls to authentic users. Data integrity can also be ensured by implementing the Zero-Knowledge Proofs mechanisms. Another method to ensure security is the implementation of auditability for cloud service providers. All these methods are highly effective in developing security practices in cloud environments.

2.2. Emergence of Edge Computing

Edge computing is a highly emerging computing paradigm related to various devices and networks near users. Edge is linked to processing data closer to where it is being produced, which helps in high-volume and speed processing. This further leads to greater action-based results. This concept was explained in detail by [6] through comprehensive research. The researchers stated that with

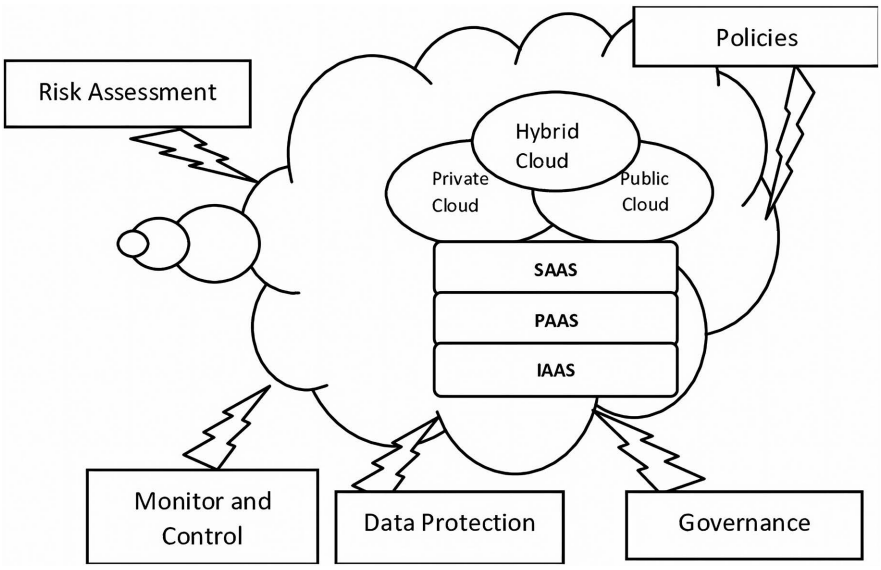

Figure 2. Traditional cloud computing environment [4].

the development of the Internet of Things, the number of smart devices linked to the Internet continuously increases. This leads to the development of large-scale data, which causes issues like poor privacy, bad security, slow response speed, bandwidth load, etc. In response to conventional cloud computing, a new concept of edge computing has emerged. This computing platform helps perform different calculations at the network's edge. It focuses on being closer to the source of the data. This is because, at this edge, it is lightweight for small-scale and local data processing and storage. **Figure 3** shows the emergence of edge computing in the computing paradigm.

Another research was conducted by [8] regarding this concept and its opportunities and issues. According to the research, the applications of service-based principles and virtualization in different emerging networking paradigms have developed a trend of network cloudification. This trend enables different network systems to be recognized based on cloud technologies. It also enables network services to be realized based on the cloud service model. Network cloudification and the crucial role of networking in edge computing platforms result in the convergence of edge computing and networking. This calls for a holistic view of all the areas of computing and networking that can develop the relevant technologies. The researchers also aimed to develop a big picture to depict the current status of research in edge computing. It was observed that edge computing

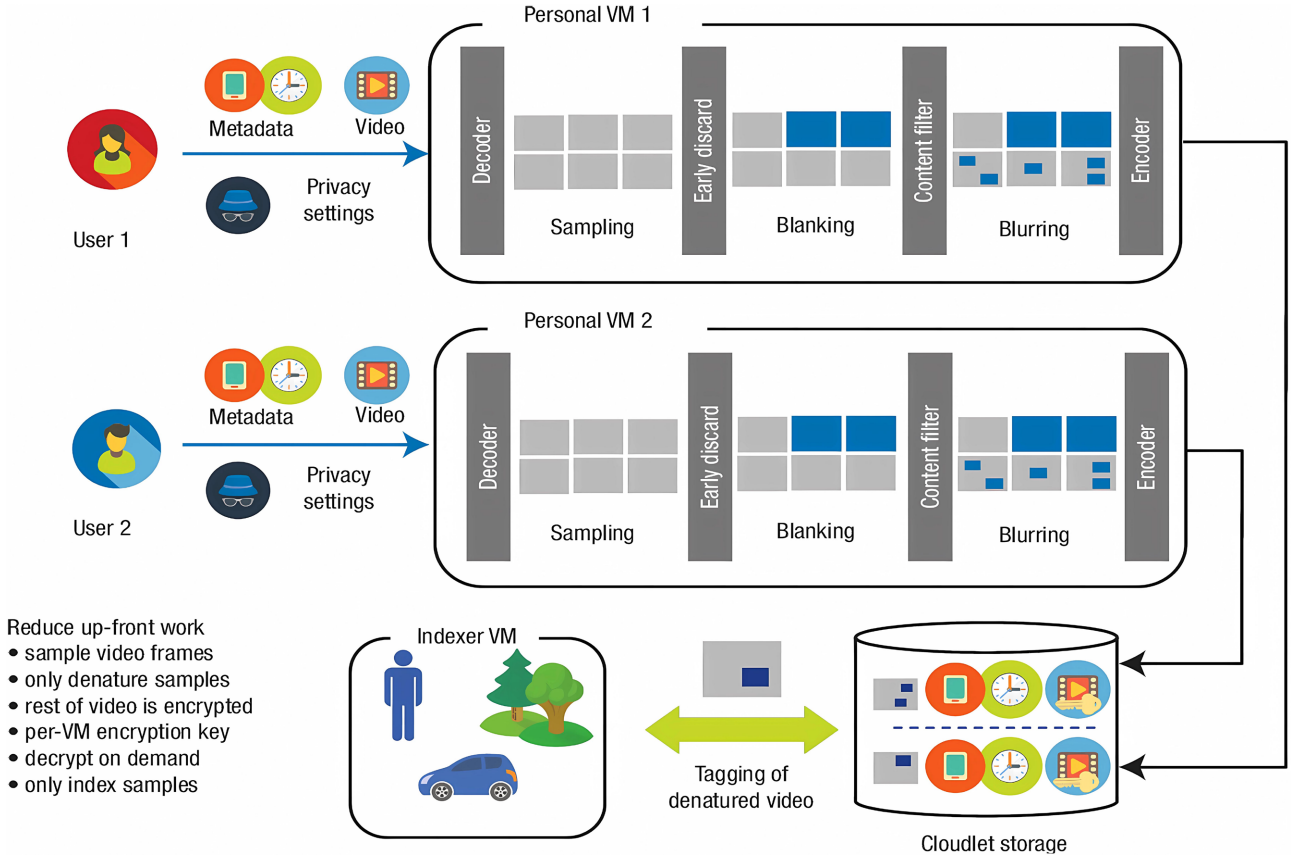

Figure 3. The emergence of edge computing [7].

could have many benefits in terms of speed, security, reliability, latency, cost, and performance.

2.3. Technological Enablers for Security

Different technologies can play a role in improving security in edge computing. Machine learning and artificial intelligence are becoming common in this regard. Research by [9] was conducted on the role of Machine Learning (ML) in this area. The research showed that many firms invest in cloud computing and its security. The use of ML techniques can help in detecting or preventing security gaps and attacks on the cloud. Different ML models, such as K-means, Random Forest, Linear Kernel, ANN, Bayes net, KNN, Decision Tree, etc., can be used in this regard. All of these models are effective in detecting different types of attacks. For instance, data mining techniques can help in identifying DDoS attacks. The CKNN model can help detect security risks by analyzing flow features. Figure 4 shows different machine learning models that help in detecting security gaps and attacks on the cloud.

Some other important techniques are cryptography and encryption. A detailed review of cryptography in edge computing was conducted by [11]. The researchers stated that cryptography is a protective approach to information from suspicious parties with the help of changing data into an unreadable format. The main purpose of this approach is to protect the data from unauthorized access. It involves encoding the main information, like textual media and content, to make it meaningless, non-understandable, and invisible. This technique thus helps to ensure the confidentiality and privacy of the data.

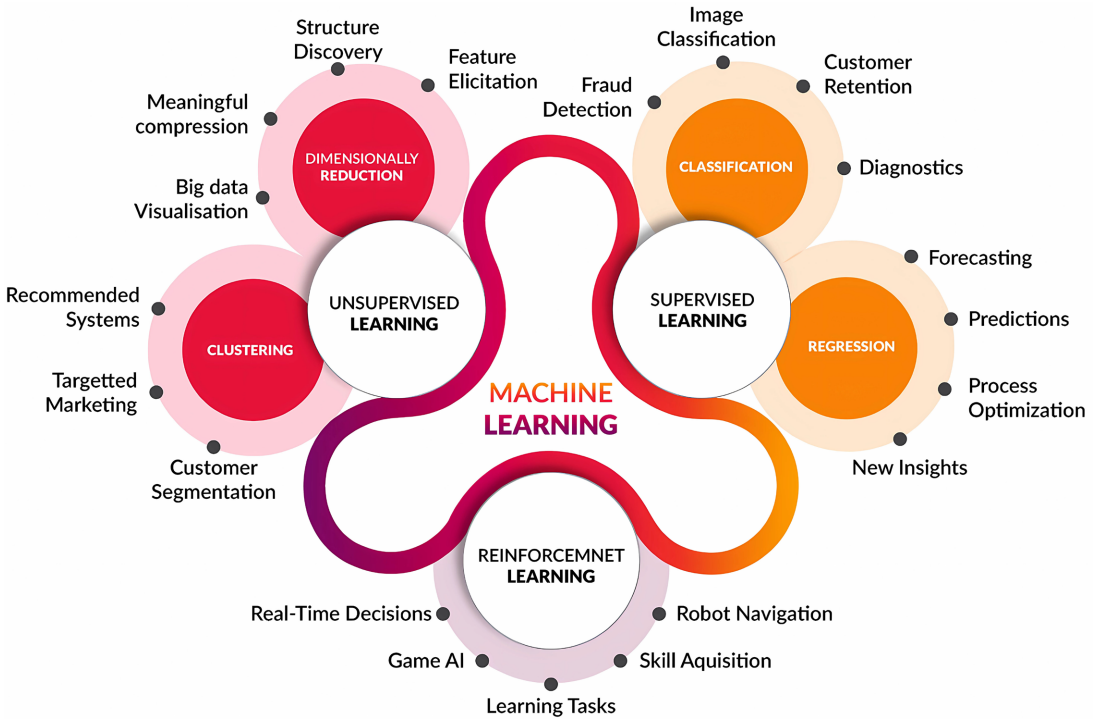

Figure 4. Machine learning models [10].

Edge devices can also use identity and access management strategies to ensure security. Research on such strategies and their effectiveness was conducted by [12]. The authors stated that cloud computing involves using different technology resources by different users according to their needs. The main issue with this area is the issue of security. Since data are dispersed across different storage devices and machines, security issues are highly likely. In such a case, access control mechanisms are very important. According to the researchers, access control can be depicted as restricting access to a particular resource or place. These mechanisms are very important because of the dynamicity and heterogeneity of the cloud. They help ensure that all attempts of specific users to access the data are based on access controls provided by the system. In this way, privacy and security can be maintained.

2.4. Resource Constraints and Security Measures

In case of limited resources on edge devices, there is a need to implement proper security measures. Geo-resiliency is one such measure. When users consider cloud providers, they should always inquire about the resiliency and protection features they use. Research by [13] focused on developing solutions to such security issues. It is very important to be aware of different edge computing security considerations. Maintaining business functionality and data availability is very important in this regard.

Moreover, protecting data from unauthorized access is crucial to the security and privacy of data. Companies should also implement mitigation plans in case of security incidents. Proper measures should be implemented to detect the risk of security issues. Artificial intelligence, encryption, media sanitization, gateway technologies, etc., can be ensured to overcome these issues. **Figure 5** shows the security measures in edge computing.

Using lightweight security solutions and optimizations for resource-constrained environments is also becoming common today. Lightweight cryptographic algorithms for managing resource-limited cloud devices were also researched [15]. The research showed that the privacy and security of cloud services are the major issues. Such devices have very limited memory, power, and area resources. Therefore, securing resource-constrained devices in the cloud, wireless sensor networks and RFID tags has become difficult. Lightweight cryptographic algorithms are created to provide proper security in such devices. If these algorithms are implemented in the hardware, they cannot be read or modified easily by intruders. Thus, they provide a more physically secure adoption of security.

2.5. Interoperability Challenges and Solutions

Interoperability mainly relates to the ability of services and applications to be used on different platforms. This feature is crucial for companies that want to utilize various cloud service providers for diverse aspects of their applications. However, this feature also comes with many challenges regarding data portability.

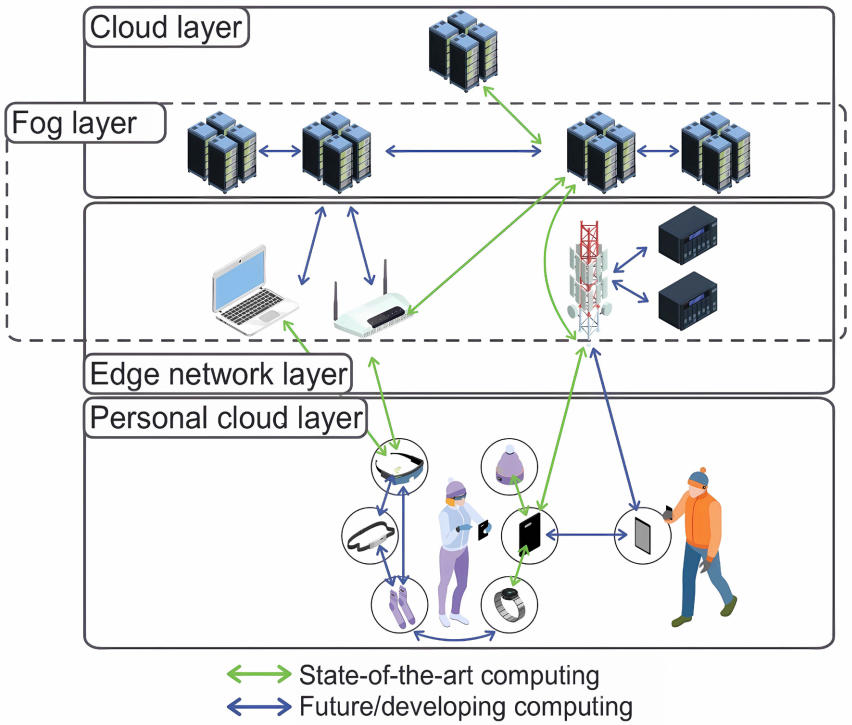

Figure 5. Components of edge security [14].

This issue of service interoperability is also focused by [16]. The research stated that client-centric interoperability helps migrate applications and data across clouds. It also provides users with enhanced control over their workloads. On the other hand, provider-centric interoperability helps the network providers to collaborate with users. Both of these perspectives can encounter serious issues related to security, scalability, and dependability.

The implementation of standardization efforts and industry-wide security protocols is needed in case of interoperability challenges. Research by [17] has also been conducted in this regard. The researchers focused on addressing semantics standards for cloud interoperability and portability. They stated that many proprietary application programming interfaces are available for collaboration and migration among cloud providers. However, they need the implementation of proper standardization efforts. These include Cloud SME, PSIF, STAGER, SCA, OSAIC, Open Swift, etc. The research also found that the semantics and migration of portability and interoperability cannot be attained together.

2.6. Future Trends and Research Directions

Research in the area of Edge Computing (EC) security is currently ongoing. Edge computing and sensor cloud are also focused on [18]. The researchers stated that sensor-cloud technology has developed from recent cloud computing applications and wireless sensor networks. The researchers analyzed the sensor-cloud-related literature to discover architectural challenges, effective management systems,

and security-enabled solutions. The researchers mainly focused on the perspectives of heterogeneity, transparency, sharing, and management. It was seen that sensor-cloud systems are transparent and related to the kinds of sensors used. Besides, the characteristic of heterogeneity can assist the sensor-cloud systems in processing real-time heterogeneous data to make important decisions. Moreover, multi-user data sharing can lessen the costs of communication and transmission and enhance working efficacy. Some of the emerging trends in edge computing are shown in Figure 6.

Many new trends are emerging in this field, such as machine learning and artificial intelligence integration. This trend is also focused by [20]. The researchers stated that there is a mutual benefit in the combination of AI and EC. The main reason behind this combination is that EC alone faces security, energy consumption, privacy, delay optimization, resource allocation, and task scheduling issues. The use of AI-based solutions helps in overcoming these problems by enhancing overall system efficiency. Future research is further needed regarding how the use of such solutions specifically enhances efficiency and overcomes security issues.

3. Problem Definition

The use of cloud computing in completing business operations shows the advancement of this modern world. It shows how the data is getting transformed in different industries in different corners of the world. This innovation comes

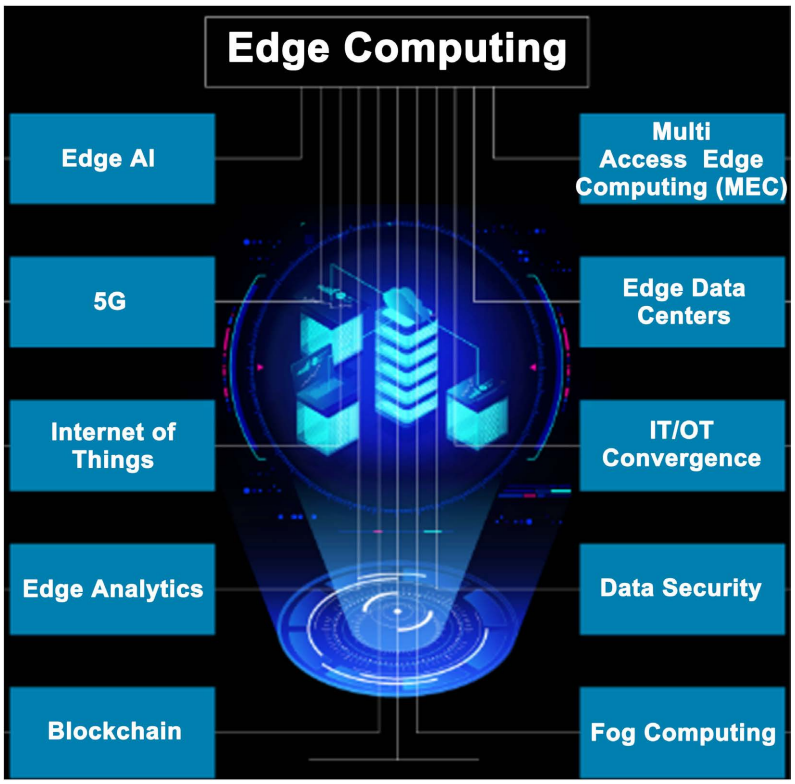

Figure 6. Edge computing trends [19].

with advantages and several challenges and issues, such as data security. The major problem revolves around understanding the importance of addressing security constraints and implications related to the integration of edge computing in cloud networks.

3.1. Decentralized Nature

One major challenge in the cloud network is the decentralized nature of edge computing [21]. Edge computing differs from traditional cloud computing regarding data processing in data centers. For instance, in the decentralized computing model, data processing occurs at different points spread out geographically, lowering latency and improving overall performance. It is advantageous for those applications where real-time data processing is important, such as IoT applications, video streaming and autonomous vehicles. Figure 7 shows decentralized edge computing architecture and how it is a challenge in cloud networks.

3.2. Increased Attack Surface

In edge computing, different factors lead to attack surface expansion, for example, Digital transformation ventures, which may include shifting towards a cloud platform [23]. As all the devices are connected in the cloud network, every switch or router that data encounters on its travel is a major point of compromise. Attackers could attack each of these devices to get unauthorized access to

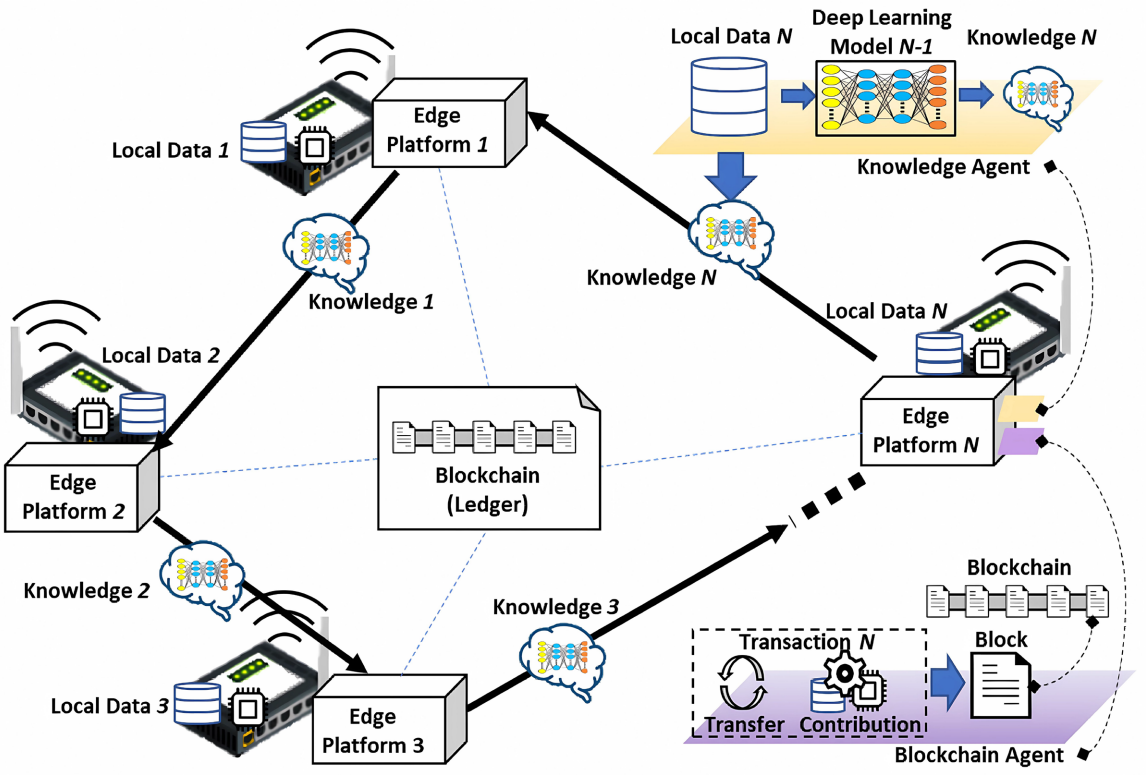

Figure 7. Decentralized edge computing architecture [22].

damage the personal data of an organization or network. Thus, limiting the number of access points is important to protect the data from unauthorized users. Edge computing introduces many devices where each device acts as a point of vulnerability. It leads to developing the problem in terms of developing and maintaining robust security measures that can adversely affect the overall computing network.

3.3. Network Latency and Bandwidth Concerns

Edge computing pays great attention to processing data closer to where it was generated to obtain fast responses. However, it becomes more work to maintain strong security and quick reactions simultaneously [24]. Undoubtedly, adding security measures may slow down the internal operation, affecting the real-time nature of edge computing. Thus, one of the most significant challenges is balancing low latency and strong security, which requires innovative solutions for enhancing the network's overall performance without compromising data security and safety.

3.4. Heterogeneous Environments

All edge networks are different from each other as different devices are connected with different features, capabilities, and operating systems [25]. This diversity results in making it difficult to develop security rules that are the best fit for all the devices. Edge devices differ from cloud devices because they require flexible security systems to handle different technologies effectively and efficiently. Creating such adaptable frameworks is one of the most significant challenges to ensure the safety and protection of the complete edge computing network.

3.5. Authentication and Authorization Complexity

In edge computing, it can be challenging to ensure the accuracy and authentication of all the connected devices and users and control what these devices and users do [26]. On the other hand, in traditional cloud computing, it is simple to check who is who and decide what the connected users can do in the central network. However, when edge computing is spread in different corners, it becomes challenging to set up strong systems that play an important role in checking and allowing data access. One of the major tasks is to follow creative ways to ensure authentic people are granted access. It means advanced tools must be used for this purpose, and organizations must also focus on extra security steps such as face recognition, fingerprint recognition, two-factor authentication, etc. Thus, the purpose of edge security is not just to keep things secure but to manage the data processing in a complicated and scattered network. **Figure 8** shows the importance of authentication in edge computing.

3.6. Data Security and Privacy Concerns

Data security and privacy are some of the most important problems in edge

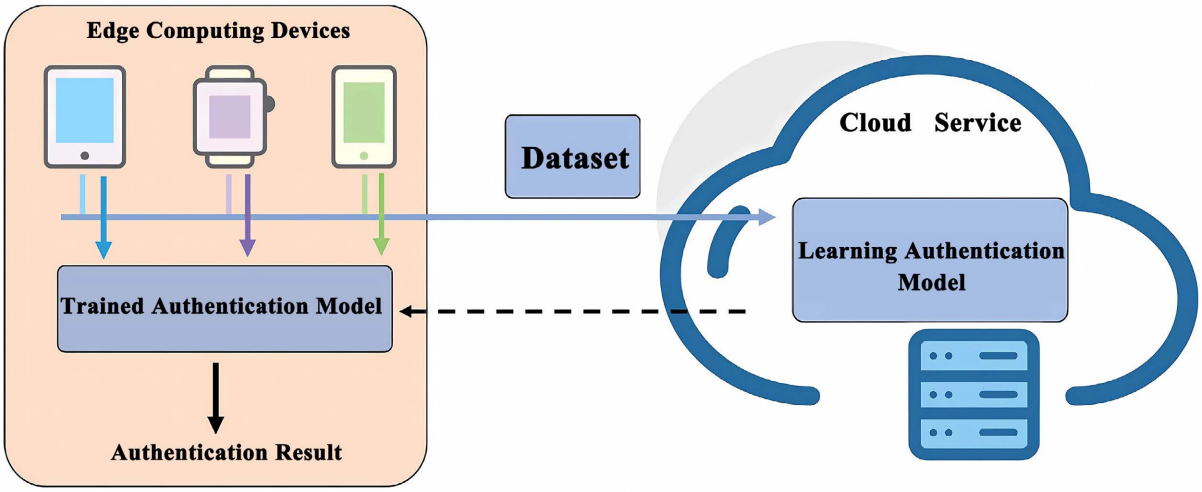

Figure 8. Accuracy and authentication in edge computing [27].

computing [28]. This is because when the data is shared between the cloud and the connected devices, it requires protection so that the sensitive data can be protected. Due to this, edge computing needs special care, and the best way to do this is to use end-to-end encryption. End-to-end encryption plays a vital role in ensuring the safety of sensitive data, whether sitting idle or roaming around the network. But it is about keeping the data safe and following some appropriate rules. Following data protection laws that become complex regarding a scattered setup is necessary. Moreover, it is not just to lock things up but to keep the data safe when it roams around. **Figure 9** shows the importance of data security and privacy concerns in edge computing.

3.7. Edge Device Security

Security challenges occur regarding the physical accessibility of the devices connected to edge computing networks [30]. These are the devices that are present in less controlled and diverse environments. It is important to provide physical security to the devices connected with the network so that unauthorized access can be prevented along with potential breaches. Moreover, updating these devices by integrating the latest and advanced technologies is important. It is important to remember that each device needs to be updated at different times. These devices must be updated by keeping the network secure, like updating a computer while keeping the house locked.

4. Methodology/Approach

4.1. Research Design

4.1.1 Approach

A qualitative research method, which is majorly focused on analyzing the existing literature, has been used for this research study. The purpose of using this approach is to explore different security aspects that are related to edge computing in cloud networks.

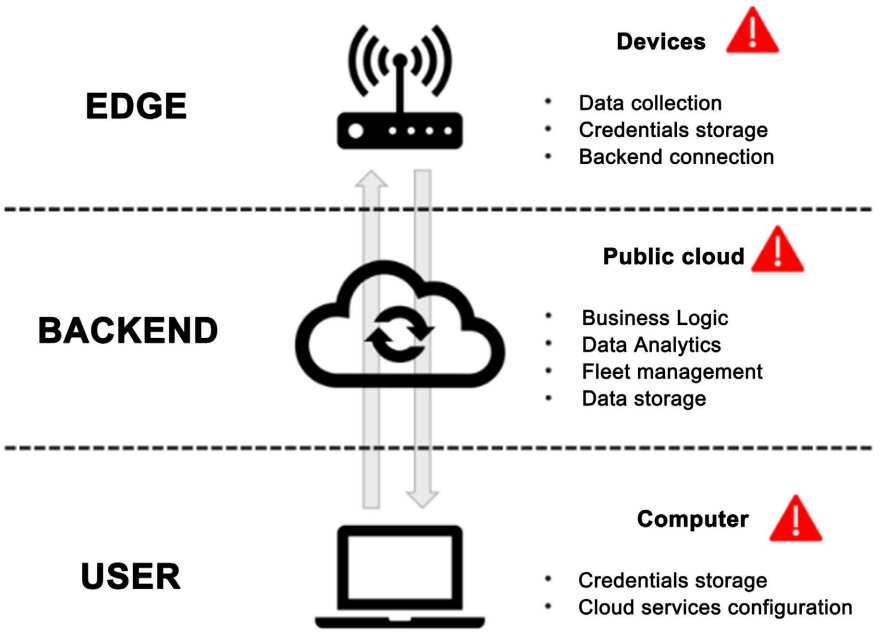

Figure 9. Confidentiality in edge computing [29].

4.1.2. Rationale

A qualitative research design is important in providing in-depth knowledge regarding a specific topic and insights into the literature. It is considered the best approach for understanding the role of edge computing in cloud networks and how security can be improvised in such networks. This is because it provides a detailed explanation of the role of edge computing in cloud networks. It also enables researchers to gather rich and context-specific data, so that valuable information can be explored regarding edge computing. Moreover, it provides human-centric insights as it involves interactions with individuals or organizations that are useful in decision-making processes and understanding the human factors.

4.2. Data Collection Methods

4.2.1. Inclusion Criteria

The data collection method included in this research study includes gathering important information from different sources like books, conference papers, and scholarly articles published from 2020 to 2023 [31]. This time frame ensures that all the gathered information is up-to-date, and this latest information shows the implications of security in edge computing in this modern and advanced world. These inclusion criteria play an important role in prioritizing the sources that address the security constraints in edge computing to ensure that the selected studies are according to the research objective of this conducted research study.

4.2.2. Search Strategy

The data collection process includes a systematic search strategy for managing databases such as ACM Digital Library and IEEE Xplore [32]. Moreover, some common keywords have also been used in this research study, such as cloud net-

work security, edge computing security, and many other related terms, which ensure that this research comes with a literature review of sources relevant to the research objectives.

4.2.3. Selection Process

The selection process includes the selection of specific abstracts, titles and relevant texts related to the research objectives. This study has prioritized relevance to ensure only the related studies that provide valuable and useful insights regarding security challenges and the things to be considered related to edge computing within cloud networks are included. This process aims to maintain the quality of the information mentioned in the research study's literature review, which contributes to a well-informed analysis of security implications in edge computing within a cloud network.

4.3. Data Analysis Techniques

4.3.1. Synthesis of Findings

Data analysis plays an integral role in this research study, including synthesizing key findings from all the selected literature studies. This includes summarizing the insights of each study, identifying the specific themes and categorizing the information of each research study related to the security implications of edge computing in cloud networks.

4.3.2. Thematic Analysis

Thematic analysis is the one in which the data is analyzed based on specific themes and defined patterns.

4.3.3. Gap Identification

All the data gathered from different sources has been critically evaluated so that the gaps in each study could be identified along with the areas that need to be focused on by future researchers. Identifying such gaps provides the basis for future exploration and insights into the present research on the security implications of edge computing within cloud networks. These gaps may include security gaps and attacks on the cloud.

4.3.4. Results and Discussion

The addition of edge computing in cloud network architecture leads to a new computing paradigm; this allows us to see how the work can be done by combining different machines. This new generation allows us to identify the hidden talents within each other. However, this transition has its security implications. Strict rules must be made to protect and arrange sensitive data. And the successful solutions to these challenges require more updates and experimentation. Embracing decentralized identity management is a foundational step in fortifying the authentication processes within edge environments, contributing to these decentralized computing architectures. **Figure 10** shows how edge computing works in cloud network architecture.

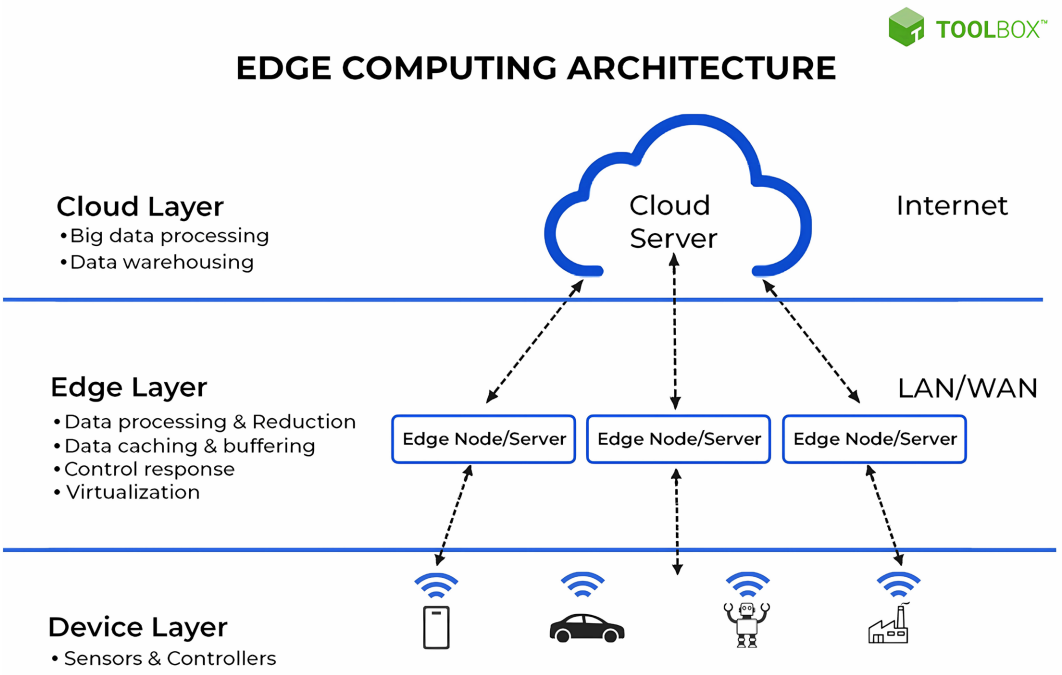

Figure 10. Edge computing in cloud network architecture [33].

4.3.5. Security Challenges

- **Edge Device Vulnerabilities**

Edge devices which work in long and different resource-constrained areas present a huge security challenge. These devices are helpless because of their limited resources, power, and security features, which leads to physical violation and attack [34]. This is due to their remote locations, and the difficulties of unauthorized access increase, making them helpless to intending actors. The combination of limited security and data privacy and integrity concerns are different. Solving these challenges requires a proactive approach that contains strong security features, encryption protocols, and continuous monitoring to increase the security position of these edge devices.

- **Data Transmission Security**

The separate nature of edge computing introduces the small data transfer from these edge devices to the cloud servers, combined into simple terms that how big data can be. The high data flow raises concerns about data privacy, security and eavesdropping during transmission. When the data is moved or transferred from edge devices to cloud devices, the risk increases because it becomes difficult to hide sensitive information [35]. In addition, increased frequency of transmission is also important to ensure data integrity. Strong encryption protocols, a secure communication framework, and good monitoring should be applied to face these challenges. Solving these data security issues is important to increase the efficiency of information exchange in edge computing.

- **Distributed Authentication and Authorization**

Traditional centralized authentication model faces many challenges due to the migration towards distributed edge environments [36]. The main challenge of

these models is security management. The use of edge devices in different locations and the decentralized nature of edge computing create problems in the authentication and authorization methods. This decentralized nature of edge devices makes it very difficult to adapt to traditional models. These challenges need to be tackled to strengthen security. Distributed authentication provides an emerging system to prevent unauthorized access. Implementing an efficient authentication method is the main goal. This ensures the avoidance of security protocols and overall network integrity.

- **Resource Management and Isolation**

Resource management is also very important in edge computing. It plays a vital role, but some challenges exist, such as workload isolation on shared edge resources [37]. At the same time, this increases the risk of data violation and affects the integrity of the entire network. Unauthorized access while sharing resources can damage data privacy and also affect the overall reliability of edge computing. To solve these problems, a strong isolation mechanism, such as containerization and virtualization, is required. This ensures that everything is done in a controlled and secure environment. Maintaining a secure, isolated environment and striking a balance is very important. Figure 11 shows how resource management works in edge computing.

- **Regulatory Compliance**

Regulatory compliance issues increase challenges in edge computing systems, where data is gathered from multiple locations [39]. It has to face different laws and regulations in different locations, which leads to more challenges. Meeting the requirements of data protection regulations such as GDPR is made difficult

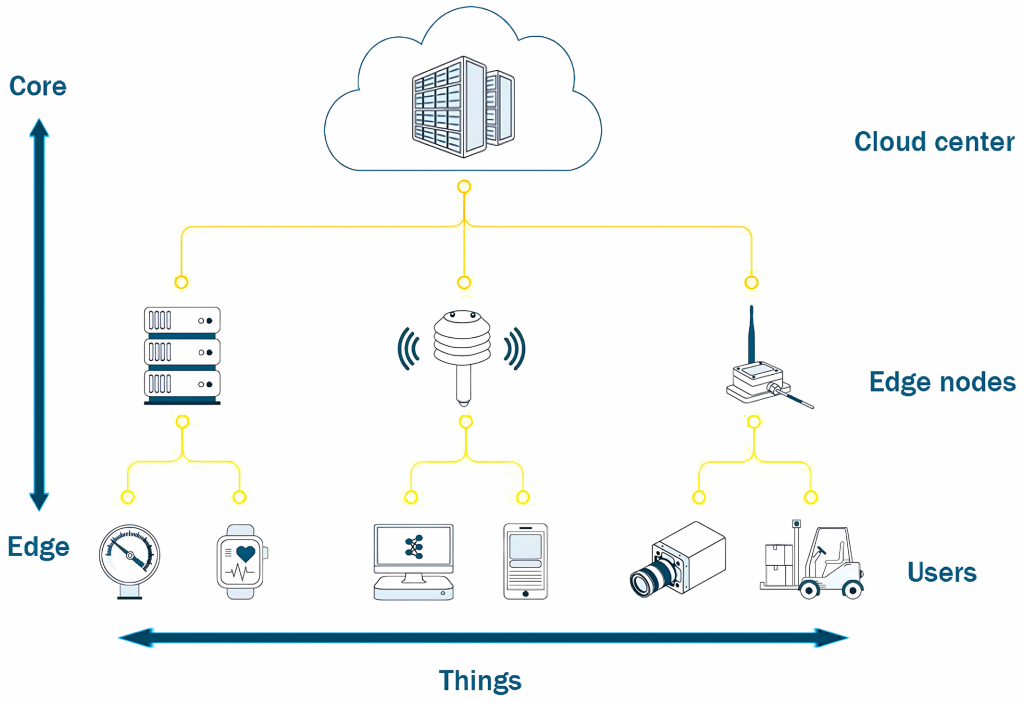

Figure 11. Resource management in edge computing [38].

by the decentralization of edge computing systems. Regulatory compliance requires attention to data release and processing policies so that the data can move through different regions and different laws. This is the best solution to challenge and agree on edge computing processes with data protection and regulatory frameworks. The organization that works in an edge computing system must create strong data protocols for its governance and compliance to transmit the data accurately through different locations. Expressive reasoning is important to organize technology development with a legal framework to secure user privacy and meet data protection law requirements.

4.3.6. Security Solutions

- **Edge Device Hardening Compliance**

It is very important to develop the security of edge devices. The overall condition of the security is based on the edge device hardening [40]. All the weaknesses can be tackled by applying strong security measures at the device level. These security measures include regular firmware updates, secure boot protocols, and devotion to stringent physical security protocols. The secure boot process plays an important role because it ensures that only authorized and reliable software mechanisms are executed during the device setup. This keeps away all the harmful attempts that try to compromise the system.

Regular firmware updates are also important; their work is to tackle the known weakness of the device and enhance its flexibility against developing threats. Moreover, implementing physical security protocols works as an additional layer of safety that protects from unauthorized access. These physical security protocols include tamper-evident hardware and safe enclosures. In these constantly changing cybersecurity challenges, edge device hardening plays an important role. It protects the integrity of individual devices and helps in the flexibility of edge computing environments. Figure 12 shows the importance of edge device hardening.

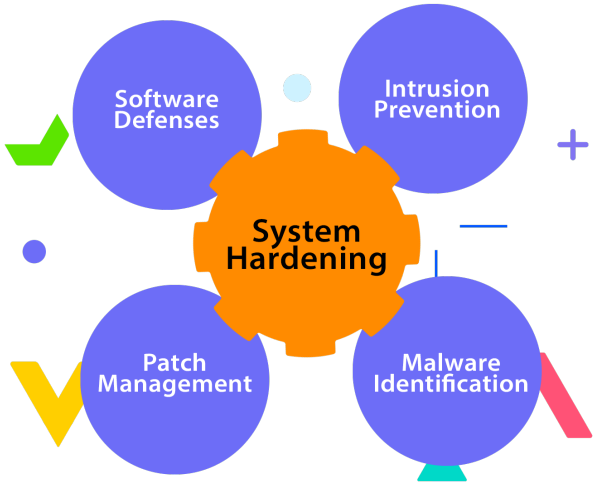

Figure 12. Edge device hardening [41].

- **Encrypted Communication Protocols**

The adoption of encrypted communication protocols is a pivotal measure in ensuring the security of data transmission within edge computing ecosystems [42]. By employing end-to-end encryption and robust communication protocols like Transport Layer Security (TLS), the confidentiality and integrity of data during transit between edge devices and cloud servers are fortified. End-to-end encryption ensures data remains encrypted throughout its journey, preventing unauthorized access or eavesdropping attempts. TLS, a widely accepted cryptographic protocol, further establishes a secure communication channel, safeguarding against potential man-in-the-middle attacks and unauthorized interception. Embracing such encrypted communication protocols not only shields sensitive information from external threats but also fosters trust in the secure exchange of data across the decentralized architecture of edge computing, contributing to the overall resilience of the network against evolving cyber threats.

- **Distributed Identity Management**

Deploying decentralized identity management solutions is pivotal for secure authentication and authorization in edge computing [43]. The unique challenges of edge environments necessitate adaptive identity frameworks and technologies such as blockchain offer compelling solutions. Blockchain provides a tamper-resistant and distributed ledger, augmenting the trustworthiness of identity information. By decentralizing identity management, the vulnerabilities associated with centralized approaches are mitigated, enhancing security. Utilizing blockchain in this context not only ensures the integrity of identity data, but also aligns with the dynamic and distributed nature of edge computing. Embracing decentralized identity management is a foundational step in fortifying the authentication processes within edge environments, contributing to these decentralized computing architectures.

5. Conclusion

In conclusion, edge computing security environments in cloud networks come with advantages, disadvantages, and challenges that organizations face. The nature of edge computing networks is decentralized, enhancing the overall data processing. The use of blockchain technology shows a need to identify adaptive security measures in edge environments due to their decentralized nature. It is important to focus on developing strategies that prioritize the privacy and security of the data, whether it is idle or traveling around the network from one device to another. The major reason is to overcome data privacy issues and resource limitations. This study focuses on introducing flexible security frameworks adapted to edge devices' dynamic properties and a zero-trust approach. Strong data security mechanisms, threat intelligence, and real-time monitoring are required to enhance edge computing. Integrating security solutions is becoming necessary to develop and enhance edge computing. It guarantees the robustness of edge environments and opens the door for safe, effective, and scalable distributed com-

puting in cloud networks. In this rapidly evolving and revolutionary industry, staying ahead of new security threats requires constant research and improvement.

6. Future Scope

The analysis of the security implications of edge computing in cloud networks shows how rapidly the world is advancing and the associated challenges. In the coming future, it is important to focus on developing security frameworks, specially designed according to the decentralized nature of edge computing. Comprehensive protocols and guidelines will be important to introduce, so that edge devices can deal with emerging vulnerabilities, difficulties, challenges, and threats. As new technologies are emerging in this modern world, such as 5G networks, it is important to comprehend their implication by considering security measures.

Additionally, the use of machine learning and artificial intelligence in edge computing will also rise, which will result in several remarkable innovative security solutions. Future researchers can focus on integrating these technologies and identify their associated challenges and risks to develop mitigation strategies. The scalability of edge computing networks provides a basis for future researchers to focus on security measures, so that the growing number of edge devices can be managed and data processing can be enhanced. Innovative strategies for error-free scalability must be investigated and analyzed without compromising the security of the data.

Organizations must refrain from ensuring robust data processing by implementing secure systems and security protocols; they must train their labor. For this purpose, future researchers may focus on employee training programs and user awareness programs to enhance overall security. The users must be provided with all the required information that could develop a sense of dealing with potential risks and introducing the best practices to create a human-centric security approach.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Al-Dulaimy, A., Sharma, Y., Khan, M.G. and Taheri, J. (2020) Introduction to Edge Computing. In: Taheri, J. and Deng, S.G., Eds., *Edge Computing*: *Models*, *Technologies and Applications*, Institution of Engineering and Technology, London, 3-25. https://doi.org/10.1049/PBPC033E_ch1

[2] Innovationatwork (2021) Real-Life Use Cases for Edge Computing. https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/

[3] Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020) A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions. *The Journal of Supercomputing*, **76**,

9493-9532. https://doi.org/10.1007/s11227-020-03213-1

[4] Sharma, A. (2020) Emerging Trends in Safety Issues in Cloud the Potentials of Threat Model. https://www.researchgate.net/figure/cloud-computing-environment-and-security-ii-cloud-security-and-privacy-some-of-the-key_fig1_347813709

[5] Abdulsalam, Y.S. and Hedabou, M. (2021) Security and Privacy in Cloud Computing: Technical Review. *Future Internet*, **14**, 11-15. https://doi.org/10.3390/fi14010011

[6] Cao, K., Liu, Y., Meng, G. and Sun, Q. (2020) An Overview on Edge Computing Research. *IEEE Access*, **8**, 85714-85728. https://doi.org/10.1109/ACCESS.2020.2991734

[7] Satyanarayanan, M. (2017) The Emergence of Edge Computing. *Computer*, **50**, 30-39. https://www.semanticscholar.org/paper/the-emergence-of-edge-computing-satyanarayanan/eca334591d85eab2ddf9d7b567a8363cb9b11f24

[8] Duan, Q., Wang, S. and Ansari, N. (2020) Convergence of Networking and Cloud/Edge Computing: Status, Challenges, and Opportunities. *IEEE Network*, **34**, 148-155. https://doi.org/10.1109/MNET.011.2000089

[9] Nassif, A.B., Talib, M.A., Nasir, Q., Albadani, H. and Dakalbab, F.M. (2021) Machine Learning for Cloud Security: A Systematic Review. *IEEE Access*, **9**, 20717-20735. https://doi.org/10.1109/ACCESS.2021.3054129

[10] Yadav, D. (2022) Different Machine Learning Models. https://medium.com/@yadavdeepika729/different-machine-learning-models-2387575e64cd

[11] Bhargav, A.J.S. and Manhar, A. (2020) A Review on Cryptography in Cloud Computing. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, **6**, 225-230. https://doi.org/10.32628/CSEIT206639

[12] El Sibai, R., Gemayel, N., Bou Abdo, J. and Demerjian, J. (2020) A Survey on Access Control Mechanisms for Cloud Computing. *Transactions on Emerging Telecommunications Technologies*, **31**, e3720. https://doi.org/10.1002/ett.3720

[13] Parast, F.K., Sindhav, C., Nikam, S., Yekta, H.I., Kent, K.B. and Hakak, S. (2022) Cloud Computing Security: A Survey of Service-Based Models. *Computers & Security*, **114**, Article ID: 102580. https://doi.org/10.1016/j.cose.2021.102580

[14] Appviewx (2020) Edge Security. https://www.appviewx.com/education-center/edge-security/

[15] Singh, P., Acharya, B. and Chaurasiya, R.K. (2021) Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices and Sensor Networks. In: Sharma, S.K., *et al.*, Eds., *Security and Privacy Issues in IoT Devices and Sensor Networks*, Elsevier, Amsterdam, 153-185. https://doi.org/10.1016/B978-0-12-821255-4.00008-0

[16] Bouzerzour, N.E.H., Ghazouani, S. and Slimani, Y. (2020) A Survey on the Service Interoperability in Cloud Computing: Client-Centric and Provider-Centric Perspectives. *Software: Practice and Experience*, **50**, 1025-1060. https://doi.org/10.1002/spe.2794

[17] Ramalingam, C. and Mohan, P. (2021) Addressing Semantics Standards for Cloud Portability and Interoperability in a Multi-Cloud Environment. *Symmetry*, **13**, Article 317. https://doi.org/10.3390/sym13020317

[18] Wang, T., Liang, Y., Shen, X., Zheng, X., Mahmood, A. and Sheng, Q.Z. (2023) Edge Computing and Sensor-Cloud: Overview, Solutions, and Directions. *ACM Computing Surveys*, **55**, Article No. 281. https://doi.org/10.1145/3582270

[19] Prat, M.K. (2024) 8 Edge Computing Trends to Watch in 2024 and Beyond. https://www.techtarget.com/searchcio/tip/Top-edge-computing-trends-to-watch-in-2020

[20] Hua, H., Li, Y., Wang, T., Dong, N., Li, W. and Cao, J. (2023) Edge Computing with Artificial Intelligence: A Machine Learning Perspective. *ACM Computing Surveys*, **55**, Article No. 184. https://doi.org/10.1145/3555802

[21] Atieh, A.T. (2021) The Next Generation Cloud Technologies: A Review on Distributed Cloud, Fog and Edge Computing and Their Opportunities and Challenges. *ResearchBerg Review of Science and Technology*, **1**, 1-15.

[22] Jin, W., Xu, Y., Dai, Y. and Xu, Y. (2023) Blockchain-Based Continuous Knowledge Transfer in Decentralized Edge Computing Architecture. *Electronics*, **12**, Article 1154. https://www.mdpi.com/2079-9292/12/5/1154 https://doi.org/10.3390/electronics12051154

[23] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J. and Lv, W. (2019) Edge Computing Security: State of the Art and Challenges. *Proceedings of the IEEE*, **107**, 1608-1631. https://doi.org/10.1109/JPROC.2019.2918437

[24] Wang, S. (2019) Edge Computing: Applications, State-of-the-Art and Challenges. *Advances in Networks*, **7**, 8-15. https://doi.org/10.11648/j.net.20190701.12

[25] Ning, H., Li, Y., Shi, F. and Yang, L.T. (2020) Heterogeneous Edge Computing Open Platforms and Tools for the Internet of Things. *Future Generation Computer Systems*, **106**, 67-76. https://doi.org/10.1016/j.future.2019.12.036

[26] Liu, D., Yan, Z., Ding, W. and Atiquzzaman, M. (2019) A Survey on Secure Data Analytics in Edge Computing. *IEEE Internet of Things Journal*, **6**, 4946-4967. https://doi.org/10.1109/JIOT.2019.2897619

[27] Zeng, X., Zhang, X., Yang, S., Shi, Z. and Chi, C. (2021) Gait-Based Implicit Authentication Using Edge Computing and Deep Learning for Mobile Devices. *Sensors*, **21**, Article 4592. https://www.mdpi.com/1424-8220/21/13/4592 https://doi.org/10.3390/s21134592

[28] Alwarafy, A., Al-Thelaya, K.A., Abdallah, M., Schneider, J. and Hamdi, M. (2020) A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. *IEEE Internet of Things Journal*, **8**, 4004-4022. https://doi.org/10.1109/JIOT.2020.3015432

[29] Sun, Y., Zhang, J., Xiong, Y. and Zhu, G. (2014) Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*, **10**, Article ID: 190903. https://www.semanticscholar.org/paper/data-security-and-privacy-in-cloud-computing-sun-zhang/82121318f0945ca6444586c3e13c172531085387

[30] Sha, K., Yang, T.A., Wei, W. and Davari, S. (2020) A Survey of Edge Computing-Based Designs for IoT Security. *Digital Communications and Networks*, **6**, 195-202. https://doi.org/10.1016/j.dcan.2019.08.006

[31] Mishra, S.B. and Alok, S. (2022) Handbook of Research Methodology. Educreation publishing, Delhi.

[32] Mourão, E., Pimentel, J.F., Murta, L., Kalinowski, M., Mendes, E. and Wohlin, C. (2020) On the Performance of Hybrid Search Strategies for Systematic Literature Reviews in Software Engineering. *Information and Software Technology*, **123**, Article ID: 106294. https://doi.org/10.1016/j.infsof.2020.106294

[33] Mohanan, R. (2022) What Is Edge Computing? Components, Examples, and Best Practices. https://www.spiceworks.com/tech/edge-computing/articles/what-is-edge-computing/

[34] Sun, Y., Lo, F.P.W. and Lo, B. (2019) Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access*, **7**, 183339-183355. https://doi.org/10.1109/ACCESS.2019.2960617

[35] He, Z., Zhang, T. and Lee, R.B. (2020) Attacking and Protecting Data Privacy in Edge-Cloud Collaborative Inference Systems. *IEEE Internet of Things Journal*, **8**, 9706-9716. https://doi.org/10.1109/JIOT.2020.3022358

[36] Puthal, D., Ranjan, R., Nanda, A., Nanda, P., Jayaraman, P.P. and Zomaya, A.Y. (2019) Secure Authentication and Load Balancing of Distributed Edge Datacenters. *Journal of Parallel and Distributed Computing*, **124**, 60-69. https://doi.org/10.1016/j.jpdc.2018.10.007

[37] Luo, Q., Hu, S., Li, C., Li, G. and Shi, W. (2021) Resource Scheduling in Edge Computing: A Survey. *IEEE Communications Surveys & Tutorials*, **23**, 2131-2165. https://doi.org/10.1109/COMST.2021.3106401

[38] Liu, H., Li, S. and Sun, W. (2020) Resource Allocation for Edge Computing without Using Cloud Center in Smart Home Environment: A Pricing Approach. *Sensors*, **20**, Article 6545. https://www.mdpi.com/1424-8220/20/22/6545 https://doi.org/10.3390/s20226545

[39] Hartmann, M., Hashmi, U.S. and Imran, A. (2022) Edge Computing in Smart Health Care Systems: Review, Challenges, and Research Directions. *Transactions on Emerging Telecommunications Technologies*, **33**, e3710.

[40] Coppolino, L., D'Antonio, S., Mazzeo, G. and Romano, L. (2019) A Comprehensive Survey of Hardware-Assisted Security: From the Edge to the Cloud. *Internet of Things*, **6**, Article ID: 100055. https://doi.org/10.1016/j.iot.2019.100055

[41] Benjamin, A. (2022) What Is System Hardening? Standards and Best Practices. https://www.chef.io/blog/system-hardening-with-chef-for-a-secure-it-infrastructure

[42] Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M. and Wu, D.O. (2020) Edge Computing in the Industrial Internet of Things: Architecture, Advances and Challenges. *IEEE Communications Surveys & Tutorials*, **22**, 2462-2488. https://doi.org/10.1109/COMST.2020.3009103

[43] Ren, Y., Zhu, F., Qi, J., Wang, J. and Sangaiah, A.K. (2019) Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things. *Applied Sciences*, **9**, Article 2058. https://doi.org/10.3390/app9102058