Enhancing Data Security and Privacy in Edge Computing: A Comprehensive Review of Key Technologies and Future Directions

[1]Rajesh Daruvuri, [2]Kiran Kumar Patibandla
[1] Google Inc, USA
[2]Visvesvaraya Technological University (VTU), India
Corresponding Author: [1]venkatrajesh.d@gmail.com, [2]Kirru.patibandla@gmail.com

Abstract: With the rapid development and widespread application of the Internet of Things (IoT), big data, and 5G networks, traditional cloud computing is increasingly unable to handle the massive amounts of data generated by network edge devices. In response, edge computing has emerged as a promising solution. However, due to its open nature, characterized by content awareness, real-time computing, and parallel processing, edge computing exacerbates the existing data security and privacy challenges already present in cloud environments. This paper outlines the research background of data security and privacy protection in edge computing and proposes a data-centric security framework. It provides a comprehensive review of the most recent advancements in key technologies related to data security, access control, identity authentication, and privacy protection that could be applicable to edge computing. The scalability and applicability of various approaches are analyzed and discussed in detail. Additionally, several practical instances of edge computing that are currently in use are introduced. Finally, the paper highlights key research directions and offers recommendations for future study.

Keywords: Edge computing, IoT, Data security, Access control, Identity authentication, Privacy protection.

I. INTRODUCTION

The rapid advancement of Internet of Things (IoT) technology and 5G networks has given rise to applications like intelligent transportation, smart cities, and mobile payments, driving an exponential increase in connected devices and data generation. Cisco's Global Cloud Index predicted global data center traffic would reach 15.3 zettabytes by 2020, alongside 50 billion IoT device connections. This explosion of data introduces challenges in processing, security, and bandwidth that traditional cloud computing models struggle to meet. To address these issues, edge computing has emerged as a complementary model. It processes data near its source on edge devices, reducing latency, alleviating bandwidth pressure, and enhancing data privacy. Edge computing platforms integrate network, computation, storage, and application capabilities, enabling real-time, intelligent services while preserving structural support for security. New paradigms like Mobile Cloud Computing (MCC), Fog Computing (FC), and Mobile Edge Computing (MEC) support task migration to the edge, improving efficiency and user experience. Despite similar goals, these paradigms differ in deployment and operational scope, influencing security and privacy mechanisms. For instance, MEC relies on telecom infrastructure, while FC and MCC are deployable on various devices, including user-owned nodes. The complexity and resource constraints of edge environments demand lightweight security and privacy mechanisms. Key challenges include: Lightweight encryption and fine-grained data sharing in multi-authority environments. Secure multi-source data control in distributed setups. Addressing security gaps in interconnected, resource-limited terminals. Meeting new privacy demands in diverse IoT services. This paper examines data security and privacy in edge computing, focusing on data encryption, identity authentication, access control, and privacy protection. It outlines current research, highlights challenges, and provides recommendations for scalable, context-specific solutions.

II. EDGE COMPUTING DATA SECURITY AND PRIVACY PROTECTION FRAMEWORK

2.1. Edge Computing Architecture and Security Challenges

In edge computing, the "edge" refers to any resource situated between data sources and cloud centers. This paradigm enables terminal devices to offload storage and computational tasks to nearby edge nodes, such as base stations (BS), wireless access points (WAP), or edge servers. This approach enhances terminal capabilities and reduces the data transmission load between devices and cloud servers. The architecture comprises four key layers:

1. Core Infrastructure: Serving as the backbone, this layer includes internet networks, mobile core

networks, centralized cloud services, and data centers. It supports large-scale computational offloading, enabling real-time services across geographically distributed users. Despite its critical role, the core infrastructure faces threats like data breaches, DoS attacks, and service manipulation, necessitating robust security measures.

2. Edge Data Centers: Positioned at the network's edge, these centers facilitate virtualization and multi-tenant services. They operate independently while collaborating with the cloud and other centers, enabling distributed, layered computing. However, they are vulnerable to physical attacks, data tampering, and privacy breaches, underscoring the need for secure sharing, access control, and privacy protection technologies.
3. Edge Networks: These networks connect IoT devices and sensors via diverse communication technologies, spanning wireless and mobile core networks. While they ensure interconnectivity, edge networks are susceptible to threats like DoS attacks, man-in-the-middle exploits, and forged gateways.
4. Mobile Terminals: Including mobile and IoT devices, terminals serve as both data consumers and providers in distributed infrastructures. Their vulnerabilities include privacy breaches, malware attacks, and communication security risks.

2.2. Data Security and Privacy Protection Research Framework

This article categorizes the research framework for data security and privacy protection in edge computing into four key areas: data security, identity authentication, privacy protection, and access control, as shown in Figure 3.

1. Data Security: This foundational aspect ensures the confidentiality and integrity of data, addressing challenges like ownership-control separation, data loss, leaks, and unauthorized operations. Key measures include data confidentiality and secure sharing, integrity auditing, and searchable encryption, enabling secure user interactions with outsourced data.
2. Identity Authentication: In edge computing's distributed, multi-trust domain environment, robust identity verification is crucial. Research focuses on single-domain, cross-domain, and handover authentication to ensure secure interactions across entities while mitigating risks from semi-trusted participants.
3. Privacy Protection: Given the open connectivity of edge systems, protecting users' identity, location, and sensitive information is critical.
4. Access Control: Vital for system security and user privacy, popular schemes like attribute-based and role-based access control enable fine-grained data sharing, with attribute-based methods being especially suited for distributed architectures.

The article highlights advancements in cryptography-driven data security, authentication, and privacy protection, emphasizing the need for adaptable solutions tailored to edge computing. Research remains in its early stages, with potential to leverage security techniques from related fields. For instance, Roman et al. analyzed mobile edge paradigms, proposing a collaborative security framework, offering valuable insights for edge computing security research.

III. DATA SECURITY

In cloud and edge computing, users often outsource sensitive data to third-party data centers, leading to separation of data ownership and control, as well as storage randomization. These factors make data vulnerable to loss, leakage, and unauthorized operations, compromising confidentiality and integrity. Ensuring outsourced data security is a fundamental challenge in edge computing. Current research on edge computing data security remains exploratory, with most insights derived from related paradigms like cloud, mobile cloud, and fog computing. A key research focus is adapting these security solutions to the edge computing framework, accounting for its unique characteristics, such as distributed architecture, resource constraints, edge big data processing, and dynamic environments. This involves creating lightweight, distributed data security systems. This section reviews three core areas of data security: confidentiality and secure sharing, integrity auditing, and searchable encryption, emphasizing key findings from other paradigms and proposing directions for advancing edge computing security.

3.1. Data Confidentiality and Secure Data Sharing

Current data confidentiality and secure data sharing solutions typically employ encryption techniques. The conventional process involves the data owner pre-encrypting the outsourced data before uploading it, allowing data users to decrypt it as needed. Traditional encryption algorithms include symmetric encryption (e.g., DES, 3DES, AES) and asymmetric encryption (e.g., RSA, Diffie-Hellman, ECC). However, traditional encryption algorithms often result in low operability of encrypted data, posing significant challenges for subsequent data processing. Commonly used data encryption algorithms today include Attribute-Based Encryption (ABE), Proxy Re-Encryption (PRE), and Fully Homomorphic Encryption (FHE).

3.1.1. Attribute-Based Encryption Algorithms

Attribute-Based Encryption (ABE) is a cryptographic technique enabling decryption based on user attributes meeting predefined access policies, represented as logical expressions or tree structures. In threshold-based policies, decryption is possible only if the user's attribute set intersects with the ciphertext attribute set at or above a specified threshold. ABE is divided into Key-Policy ABE (KP-ABE), where the receiver defines access policies, and Ciphertext-Policy ABE (CP-ABE), where the sender specifies them. CP-ABE is widely used for secure data storage and sharing in cloud computing. Traditional CP-ABE employs a monotonic access tree structure embedded in ciphertext, granting access only when a user’s attributes satisfy the tree's threshold. However, this approach struggles with multi-level data sharing. To overcome this, Wang et al. proposed a hierarchical encryption scheme that integrates multi-layer file access structures into a single access policy, enhancing fine-grained data sharing and storage security. Although ABE supports scalable storage and fine-grained sharing, it faces challenges with attribute revocation. Yang et al. introduced a "proxy-assist" method using the "all-or-nothing" principle to reduce cloud server authority during revocation, defending against collusion attacks. Similarly, Zuo et al. developed an Outsourced Decryption ABE (OD-ABE) method for fog computing, ensuring security against chosen ciphertext attacks (CCA).

3.1.2. Proxy Re-Encryption Algorithms

Proxy Re-Encryption (PRE), introduced by Blaze et al. in 1998, enables a semi-trusted proxy to transform ciphertext encrypted for one user into ciphertext encrypted for another, using a re-encryption key. This transformation ensures that the proxy cannot access the plaintext, making PRE a valuable tool for secure data forwarding and file sharing in cloud environments.

Over time, various PRE-based algorithms have been developed:

- Identity-Based Proxy Re-Encryption (IBPRE) (2007): Uses user identity as the public key, making the re-encryption key unidirectional.
- Conditional Proxy Re-Encryption (CPRE) (2009): Allows ciphertext transformation only under specific conditions, offering improved control over proxy permissions.
- Ciphertext-Policy Attribute Proxy Re-Encryption (CP-ABPRE): Integrates PRE with Attribute-Based Encryption (ABE), enabling ciphertext transformation between different access policies. Liang et al. enhanced this with dual-system encryption and selective verification, proving its security under chosen ciphertext attacks (IND-CCA). Yang et al. further improved CP-ABPRE by incorporating CPRE features, enabling secure attribute revocation through proxy control.
- Bidirectional Proxy Re-Encryption (BPRE) (2016): Proposed by Shao et al., this scheme supports dynamic cloud storage with fixed ciphertext length, ensuring replay security (RCCA) via the random oracle model.
- Cloud and Proxy-Based Dual Encryption Scheme (CMReS): Introduced by Khan et al., this scheme combines PRE and cloud re-encryption to offload computation-intensive tasks to the cloud, reducing mobile terminal overhead. An extension in 2017 proposed a workload allocation model for task migration, further optimizing performance and minimizing computational demands on mobile devices.

These advancements demonstrate PRE's adaptability and importance in enhancing security and efficiency across diverse applications.

3.1.3. Fully Homomorphic Encryption Algorithms

In 2011, Brakerski et al. successfully constructed a homomorphic encryption scheme based on the Learning with Errors (LWE) problem by combining modulus switching and key switching techniques. In 2013, Gentry and others proposed a fully homomorphic encryption scheme based on approximate feature vectors, which improved algorithm efficiency by eliminating the need for modulus switching and key switching techniques. Louk et al. constructed a homomorphic encryption algorithm for mobile multi-cloud computing environments, providing data security protection for mobile users. Baharon et al. further addressed the computational efficiency issue in homomorphic encryption by proposing a Lightweight Homomorphic Encryption (LHE) algorithm that minimizes encryption and key generation time while achieving additive and multiplicative homomorphism. Table 1 summarizes the aforementioned solutions based on categories, technical methods, security models, security characteristics, and scalability.

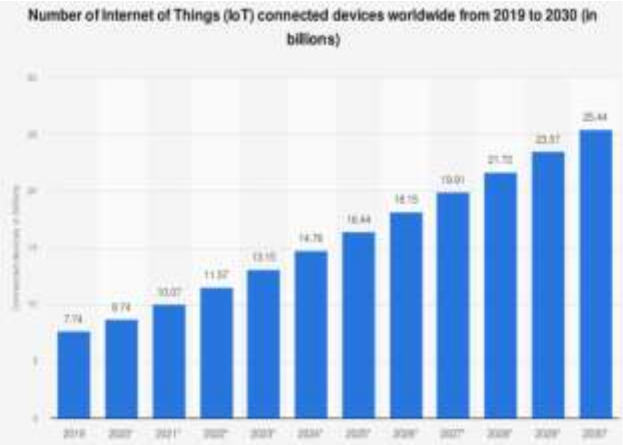

Figure 1: Growth Trend of IoT Devices

3.2. Integrity Auditing

Once user data is stored in edge or cloud data centers, a significant concern is how to ensure the integrity and availability of the outsourced stored data. Current research on data integrity auditing primarily focuses on the following four functional requirements [33]:

1. Dynamic Auditing: User data in the storage server is often subject to dynamic updates. Common dynamic data operations include modification, replication, insertion, and deletion. Therefore, data integrity auditing solutions should not be limited to static data; they must also support dynamic auditing functionalities.
2. Batch Auditing: When numerous users simultaneously submit audit requests or data is stored in chunks across multiple data centers, integrity auditing solutions should have the capability to perform batch audits to enhance auditing efficiency.
3. Privacy Protection: Since neither the data storage server nor the data owner is suitable for executing integrity auditing solutions, a third-party auditing platform (TPA) is often employed. In such cases, if the TPA is semi-trusted or untrusted, data leakage and tampering can pose significant security threats, compromising data privacy. Thus, it is crucial to protect user data privacy during the integrity auditing process.
4. Low Complexity: Given the computational, storage, and bandwidth limitations of data storage servers (edge data centers) and data owners (edge devices), the complexity of the integrity auditing solution is an important factor that must be considered alongside ensuring data integrity.

Wang et al. [34] addressed the issues of privacy leakage and batch auditing during the data integrity auditing process by proposing a privacy-preserving distributed data auditing system.

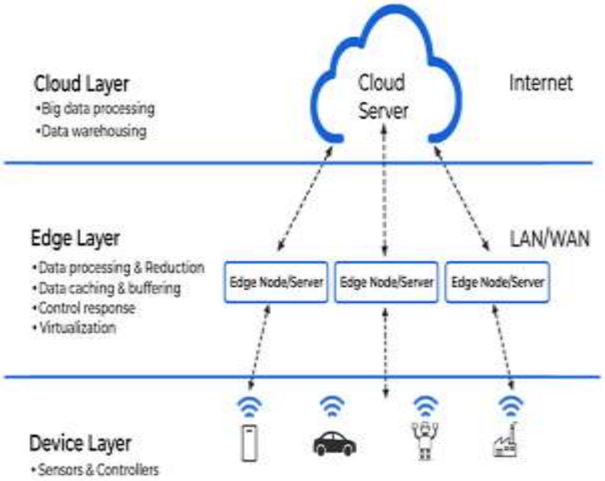

Figure 2: Edge Computing Architecture for the Internet of Things

Yang et al. [36] first analyzed the limitations of existing Remote Data Auditing (RDA) technologies, which were only applicable to static data, not dynamic data updates. They subsequently proposed an efficient, privacy-preserving dynamic auditing protocol that combines cryptographic techniques with the bilinear properties of bilinear pairs instead of random masking for privacy protection. They extended the protocol to facilitate dynamic data operations and batch approvals, providing a security proof of the protocol in the random oracle model. Building on [36], Sookhak et al. [37] introduced an efficient RDA technique based on algebraic signature characteristics, achieving minimal computational and communication costs. To address the computational limitations of mobile devices, [38] proposed two lightweight privacy-preserving integrity auditing protocols: a basic protocol and an improved protocol. The basic protocol relies on online/offline signing methods, enabling offline signature computation before outsourcing data. To tackle this issue, Lin et al. [39] proposed two mobile data possession proof schemes (MPDP) in a mobile cloud computing environment. They constructed a hash tree-based data structure to support dynamic data operations while integrating the BLS short signature method to achieve efficient and low-complexity integrity auditing. Table 2 summarizes the aforementioned solutions based on their classification, technical methods, application scenarios, security features, and scalability.

3.3. Searchable Encryption

In traditional cloud computing paradigms, users often encrypt files using some form of encryption to outsource data storage to third-party cloud servers while ensuring data security and minimizing resource consumption on end devices.

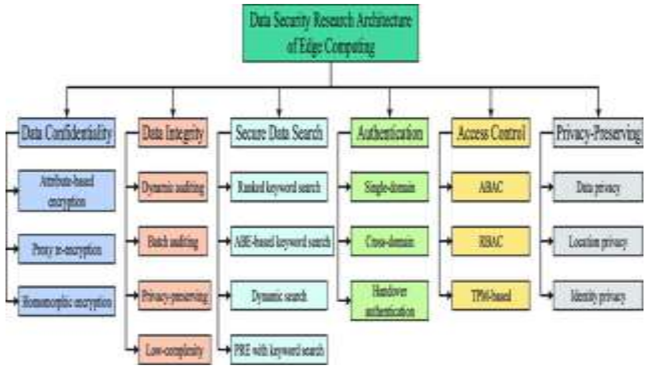

Figure 3: Research Framework for Data Security and Privacy Protection in Edge Computing

3.3.1. Secure Ranked Searchable Encryption

Secure ranked search refers to systems that return search results to users based on a certain relevance criterion (e.g., keyword frequency). This approach enhances system usability and aligns with the practical needs for privacy protection in edge computing environments.

Wang et al. [40] first proposed a Ranked Secure Symmetric Searchable Encryption (RSSE) algorithm based on Symmetric Searchable Encryption (SSE). This algorithm uses keyword frequency and inverse index strategies to measure the relevance between keywords and encrypted data, enabling secure ranked search in cloud computing. The paper also introduces a new cryptographic primitive, **Order Preserving Symmetric Encryption (OPSE)**, which utilizes one-to-many confidential mapping to protect user data privacy while allowing verification of the search results returned to users. Building on this work, Cao et al. [41] proposed a **Multi-keyword Ranked Search Algorithm (MRSE)** that returns files corresponding to keywords in a ranked order. To address the search efficiency issue in secure ranked searchable encryption, Li et al. [42] developed an **Efficient Multi-keyword Ranked Search System (EMRS)** in mobile cloud computing environments, using the same relevance methods as [41] and integrating **K-nearest neighbors (K-NN)** technology. This system ensures the accuracy of returned results and employs an efficient indexing structure to enhance search efficiency. Additionally, it uses a **blind storage** system to conceal the access patterns of search users, thus achieving privacy protection. Simulation experiments demonstrated that EMRS offers higher efficiency in multi-keyword ranked searches than MRSE. Moreover, [43] proposed a **Communication and Energy Saving Encryption Search Scheme (TEES)** that enhances search efficiency while providing privacy-preserving searchable encryption.

3.3.2. Attribute-Based Searchable Encryption

Attribute-based searchable encryption enables effective search operations while supporting fine-grained data sharing. In 2013, Wang et al. [44] proposed a **Keyword Searchable Functionality CP-ABE Scheme (KSF-CP-ABE)** that constructs a keyword retrieval system with the same access policy as the encrypted data, allowing only authorized users who meet the access policy to search for ciphertext data using keywords, thus achieving fine-grained search control. In 2014, Zheng et al. [45] defined the issue of user search permissions, asserting that an authorized user should possess three functional permissions: search, outsourcing, and verification. This scheme also allows legitimate users to outsource search operations to cloud servers while verifying whether the cloud server can accurately execute the search operations and return correct results. In the same year, Liu et al. [46] highlighted the practicality issues with the VABKS scheme, noting that its construction method necessitates establishing a secure channel between communicating parties. In 2016, Sun et al. [47] considered scenarios where outsourced datasets are provided by multiple owners and searched by multiple data users (multi-user multi-contributor case).

3.3.3. Dynamic Update Supported Searchable Encryption

Kamara et al. [48] were the first to introduce the concept of **Dynamic Symmetric Searchable Encryption (DSSE)** based on symmetric searchable encryption schemes (SSE). This allows users to store a dynamic encrypted data file on a server and supports keyword searches on that file. Sun et al. [50] proposed an effective Verifiable Connected Keyword Search Scheme (VCKS) that simultaneously supports connected keyword searches, dynamic data updates, and verification of search results. The verification mechanism allows users to delegate search tasks to the cloud server, which can be processed by a trusted public authority (TA) within the cloud server, or users can utilize bilinear mapping accumulator techniques to build authentication data structures themselves. Xia et al. [51] introduced a secure multi-keyword ranked search scheme that supports dynamic update operations. This scheme combines a vector space model and a general TF-IDF model to construct a tree-based index structure and further employs this structure along with a greedy depth-first search algorithm to facilitate efficient multi-keyword ranked searches. Hu et al. [52] pointed out that attribute-based keyword search schemes (ABKS) can only achieve fine-grained search authorization but are ineffective at updating search permissions.

Table 1: Existing confidentiality and Secure Data sharing Schemes

Research Literature	Category	Scheme	Technical Method	Security Model	Security Features	Scalability
[15]	Attribute Encryption	Attribute encryption scheme based on file hierarchy	Ciphertext-based attribute encryption hierarchical access tree	Chosen plaintext attack	Data confidentiality fine-grained data sharing	High
[16]	Attribute Encryption	Attribute encryption scheme supporting user attribute	Ciphertext-based attribute encryption, all-or-nothing principle	Chosen plaintext attack	Data Confidentiality, supports user attribute revocation, resists collusion attacks	Moderate
[17]	Attribute encryption	Attribute encryption scheme supporting outsourced decryption	Attribute encryption method	Chosen ciphertext attack	Data confidentiality, secure storage	High
[21]	Proxy Re-encryption	Cipher text-policy attribute proxy re-encryption scheme	Cipher text-based attribute encryption proxy reencryption	Indistinguishability under chosen ciphertext attack	Fine-grained data sharing	High
[22]	Proxy Re-encyption	Ciphertext-policy attribute conditional proxy	Ciphertext-based attribute encryption, conditional proxy re-encryption	Chosen plaintext attack	Supports user attribute revocation, fine-grained data sharing	Moderate
[23]	Proxy Re-encryption	Bi-directional proxy re-encryption scheme with fixed ciphertext length	Bi-directional proxy re-encryption	Replay chosen ciphertext attack	Secure storage resists ciiusion attacks	High

3.3.4. Searchable Proxy Re-encryption

In 2010, Shao et al. [53] combined proxy re-encryption (PRE) schemes with public encryption with keyword search (PEKS) to introduce the concept of **Searchable Proxy Re-encryption (PRES)**. They successfully constructed a provably secure bidirectional PRES scheme that facilitates third-party protocols for searching and decrypting. The security of this protocol was proven under the Decisional Bilinear Diffie-Hellman (DBDH) assumption and in the random oracle model. They also provided examples of the application of the PRES scheme in cloud computing and sensor networks. In 2012, Wang et al. [54] built upon the work of [53] to further expand the PRES scheme, proposing a Constraint One-Way Single-Hop Proxy Re-encryption Scheme (CPRE-CKS) that supports connected keyword searches. To address this security issue, Fang et al. [55] integrated conditional proxy re-encryption mechanisms with public key searchable encryption mechanisms, proposing a Conditional Proxy Re-encryption Scheme (C-PRES). This scheme achieves chosen ciphertext attack security through keyword anonymization. In 2014, Shi et al. [56] introduced an Attribute-Based Keyword Proxy Re-encryption Scheme (ABRKS) that combines attribute-based encryption (ABE) and proxy re-encryption (PRE) to facilitate keyword searches with fine-grained access control.

3.4. Research Direction Outlook

In summary, data encryption technology provides effective solutions to ensure data security in various computing models. In the open-edge computing environment, a key area of future research is how to organically combine traditional encryption schemes with characteristics such as parallel distributed architecture, limited terminal resources, edge big data processing, and highly dynamic environments to establish a lightweight, distributed data security protection system.

1) In terms of data confidentiality and secure data sharing, an important research approach involves combining encryption theories such as attribute encryption, proxy re-encryption, and homomorphic encryption. Designing low-latency, distributed secure storage systems that support dynamic operations and effectively manage the collaboration between edge network devices and cloud centers is crucial.
2) Regarding data integrity auditing, a primary research objective is to implement various auditing functions while maximizing auditing efficiency and minimizing verification overhead. Additionally, developing integrity auditing schemes that support heterogeneous data from multiple sources and dynamic data updates is expected to become a focal point for future research.

IV. AUTHENTICATION

Edge computing typically involves multiple functional entities, such as data participants (end users, service providers, and infrastructure providers), services (virtual machines, data containers), and infrastructure (e.g., terminal infrastructure, edge data centers, and core infrastructure).

4.1. Identity Authentication Within a Single Domain

In 2015, Liu et al. [57] proposed a Shared Permission-Based Privacy Protection Authentication Protocol (SAPA) that addresses privacy issues in cloud storage. The authors provided a Universal Composability (UC) model for SAPA, proving its correctness. In the same year, another study [58] introduced a privacy-protecting anonymous identity authentication scheme in a distributed cloud service environment, based on bilinear pairing cryptosystems and dynamic random number generation. In 2016, Jiang et al. [59] noted that the scheme in [58] could not withstand forgery attacks by service providers, allowing adversaries to impersonate any service provider for user identity authentication, which undermines mutual authentication support. They offered further research recommendations. That same year, He et al. [60] analyzed the shortcomings of the authentication scheme in [58] , stating that it could not resist forgery attacks and that adversaries could extract the real identity of users during such attacks, compromising user privacy. To address these issues, He et al. proposed a Privacy Authentication Scheme Based on Identity Signature (PAA), providing security proofs and comparative analysis for PAA. Lo et al. [61] proposed a conditionally private identity authentication scheme for vehicle sensor networks (VSN). This scheme employs Elliptic Curve Cryptography (ECC) and identity-based signature mechanisms, supporting anonymous authentication, data integrity, traceability, and batch signature verification without the need for any bilinear pair operations, significantly reducing time consumption and computational costs. Mahmood et al. [62] introduced a lightweight ECC-based authentication scheme for smart grid systems, achieving low computational and communication costs for mutual authentication while resisting all known security attacks.

Table 2: Comprehensive Comparison of existing integrity audit schemes

Research Literature	Category	Scheme	Technical Method	Application Scenario	Security Features	Scalability
[34]	Batch Audit	Privacy-preserving batch data audit system	Homomorphic authenticator, random masking, bilinear aggregate signatures	Cloud computing	Batch auditing privacy protection	High
[35]	Dynamic Audit	Secure cloud storage scheme supporting dynamic auditing	Merkle hash tree, data possession proof	Cloud computing	Dynamic auditing, secure stronge	High

4.2. Cross-Domain Authentication

Some authentication standards used between clouds (e.g., SAML, OpenID) and Single Sign-On (SSO) mechanisms have the potential to be applied in identity authentication across multiple trust domains [63] .

In one study [64] , an attribute-based authentication and authorization framework was designed for structured P2P networks. This framework employs attribute certificates and a distributed certificate revocation system instead of traditional public key certificates and access control lists in P2P networks. This provides flexible, efficient, and privacy-preserving access control without the need for external servers or third-party trusted agencies. Another study [65] , set in the context of e-health, proposed a cross-domain dynamic anonymous group key management and authentication system (CD-AGKMS).

4.3. Handoff Authentication

Yang et al. [66] proposed a handoff authentication protocol based on a heterogeneous mobile cloud network. This protocol uses an identity-based elliptic curve algorithm to address privacy concerns during the handoff process in mobile cloud computing, achieving authentication anonymity and untraceability. However, the protocol typically requires access to an identity authentication server located in a centralized cloud infrastructure, leaving room for improvement. Notably, since edge computing allows users to deploy personal data centers, authentication protocols used in private cloud platforms could potentially be applied to edge computing. One typical private cloud platform authentication framework is OPENi [67] , which provides an access control protocol for external users. Its authentication component uses the OpenID Connect identity verification layer and other mechanisms, allowing cloud owners to decide which authentication servers are trusted and which users are permitted access to cloud resources.

He et al. [68] reviewed handoff authentication protocols used in mobile wireless networks over the past few years, highlighting eight security and privacy requirements for such protocols.

4.4. Future Research Directions

Current research on identity authentication protocols, both domestically and internationally, primarily focuses on improving and optimizing existing security protocols. This includes enhancing flexibility, efficiency, energy-saving, and privacy protection.

Table 3: Comparison and analysis of existing searchable encryption scheme

Research Literature	Category	Scheme	Technical Method	Symmetry	Security Model	Functionality	Scalability
[40]	Secure Ranked keyword search	Secure ranked keyword search for cloud data	Order-preserving symmetric encryption, inverse mapping	Symmetric	None	Ranked search	Moderate
[41]	Multi-keyword ranked search	Multi-keyword ranked search	Coordinated matching, inner product similarity	Symmetric	None	Multi-keyword	Moderate
[42]	Multi-keyword ranked search in mobile cloud	Multi-keyword ranked search in mobile environment	k-nearest neighbor, blind storage	Symmetric	None	Multi-keyword	High
[43]	Efficient Ranked Search in Mobile Cloud	Efficient ranked search in mobile cloud environment	Computation migration technology	Symmetric	None	Efficient search	High

V. ACCESS CONTROL

5.1. Attribute-Based Access Control

Yu et al. [69] combined key-policy attribute-based encryption (KP-ABE) and proxy re-encryption (PRE) to propose a secure, scalable, and fine-grained data access control scheme. In this scheme, KP-ABE enables fine-grained access control, while PRE facilitates user attribute revocation and computational cost migration. In large-scale distributed computing environments, this can easily lead to single-point performance bottlenecks, significantly reducing the execution efficiency of the entire access control system. Therefore, single attribute authorization schemes are not suitable for edge computing. To address this issue, Xue et al. [70] proposed a robust and auditable access control scheme (RAAC), employing a heterogeneous framework that supports multi-attribute authorization access control.

In recent years, with the in-depth research on mobile cloud computing and fog computing, several secure, efficient, and lightweight access control schemes have been proposed. Jin et al. [71] introduced a lightweight data access control scheme based on CP-ABE (SL-CP-ABE) for mobile cloud computing environments. This scheme protects the confidentiality of outsourced data while providing fine-grained data access control. By reducing the number of encryption and decryption operations, it lowers computational overhead, significantly improving system performance and making it suitable for lightweight mobile devices. Building on this work, Zhang et al. [72] proposed an access control strategy with outsourcing capabilities and attribute updates, also utilizing the CP-ABE scheme for fine-grained access control. This strategy offloads access structure and attribute-related encryption and decryption operations to fog nodes, decoupling these operations from data owners, which is beneficial for resource-constrained smart devices. The security of this strategy was proven under the decision bilinear Diffie-Hellman assumption. Huang et al. [73] further expanded the update capabilities in access control policies by proposing a scheme with computation outsourcing and ciphertext updates, employing attribute signature technology (ABS) for ciphertext updates.

5.2. Role-Based Access Control

Kuhn et al. [74-76] were the first to incorporate user attributes into RBAC schemes, achieving dynamic role allocation and distributed access control, thus supporting dynamic permission management alongside rapid authentication. This distributed access control architecture is highly compatible with the requirements of edge computing, while current research on distributed access control is largely focused on other computing paradigms [77] . In a multi-cloud environment, literature [78] established a distributed access control policy based on roles, providing inter-domain role mapping and constraint verification. This approach is likely applicable to access control strategies for cross-domain entities in edge computing. Additionally, there are other security access control mechanisms that, while not originally designed for edge computing, may also be suitable for edge computing scenarios. For example, the Direct Anonymous Authentication scheme with attribute protocols (DAA-A) [79] is based on the elliptic curve cryptosystem (ECC) and allows anonymous users to prove they possess specific trusted attributes. These protocols can be implemented using primitives defined in the Trusted Platform Module 2.0 (TPM 2.0) specification, enabling users with TPM platforms to select visible and hidden attributes for verifiers, while employing zero-knowledge proof (ZKP) protocols to validate the authenticity of hidden attributes. Thus, this scheme can be applied in scenarios where two edge data centers need to prove they possess certain attributes (such as location or functionality) without disclosing their owners' identities. Table 5 summarizes various access control schemes based on their classification, technical methods, application scenarios, and scalability.

Table 4: Comparative Analysis of Existing authentication Protocols

Research Literature	Category	Scheme	Technical Method	Application Scenario	Security Features	Scalability
[57]	Single-Domain identity authentication	Privacy-preserving authentication protocol based on shared permissions	Attribute encryption proxy re-encryption	Secure cloud storage	Privacy protection anonymous authentication	High
[58]	Privacy protecting anonymous identity authentication	Privacy-aware identity authentication scheme based on identity signature	Bilinear cryptosystem	Distributed Mobile cloud computing	Anonymous authentication key exchange intractability	Moderate
[60]	Privacy-aware identity authentication	Privacy-aware identity authentication scheme based on identity signature	Bilinear cryptosystem	Mobile cloud computing	Anonymous authentication, privacy protection untraceability	High
[61]	Condition based identity authentication	Condition based identity authentication scheme	Elliptic curve cryptosystem	Vehicle sensor networks	Anonymous authentication, traceability, batch signature verification	High

VI. ANALYSIS AND SUMMARY

6.1. Summary and Analysis of Research Findings

Tables 1 to 6 summarize the current solutions across several aspects, including data confidentiality, data integrity, identity authentication, access control, and privacy protection. Each solution focuses on one or several areas within the research framework of data security and privacy protection, continuously enhancing the security mechanisms and protocols in various computing paradigms.

6.2. Relevant Examples of Edge Computing

The OpenAirInterface (OAI) software platform is an open-source software-defined radio (SDR) LTE project initiated and maintained by the EURECOM organization in Europe. Its primary advantage lies in implementing the complete 3GPP protocol through software, while also combining SDR components to realize 4G LTE base stations. The implementation concept of OAI can be summarized as follows: a PC implements the physical layer and medium access layer functions via software, while also realizing various aggregation and control protocols within the 3GPP protocol, subsequently sending the generated IP data through the Linux IP protocol stack, with eNode B and MME connecting and exchanging data via their respective IP addresses. Currently, the OAI software platform has been used as a validation platform for research and implementation of radio communication technologies. Additionally, there are other edge computing examples, such as JADE and OpenStack, that can provide validation environments for the implementation and large-scale deployment of edge computing. These tools and platforms also offer practical solutions for validating security and privacy protection proposals in edge computing.

VII. CONCLUSION

This paper begins with an exploration of the fundamental concepts, architectural frameworks, and security issues of edge computing, as well as the research system for data security and privacy protection, along with the latest domestic and international research findings. It discusses and analyzes recent developments related to key technologies such as data security, access control, identity authentication, and privacy protection applicable to edge computing. Overall, current research and progress concerning edge computing security at home and abroad are still in their early stages, and a complete research framework has yet to be established. Future research efforts can focus on the following four areas:

1. Integrating Traditional Encryption with Edge Computing: In open interconnect environments for edge computing, there is an urgent need to solve the problem of how to combine traditional encryption schemes with the parallel distributed architecture, resource constraints, and dynamic nature of edge computing to create a lightweight, distributed data security protection system.
2. Trust Domain Relationships: In multi-trust-domain edge computing environments, it is essential to fully consider the correspondence between trust domains and trusted entities. Research should focus on identity issues among various trusted entities in different trust domains, ensuring that identity authentication balances functionality and privacy protection.

By comprehensively addressing these four aspects, a complete security protection system can be formed, effectively ensuring the long-term evolution of data security and privacy protection in edge computing. This will facilitate the healthy and orderly development of edge computing services.

VIII. REFERENCES

[1]. Zhang, J., Wang, L., & Liu, S. Edge Computing: A New Computing Paradigm In The Era Of Internet Of Things [J]. Journal Of Computer Science And Technology, 2018, 33(1): 1-12.

[2]. Cisco. Cloud Index: Global Cloud Traffic Growth [R]. 2018.

[3]. Evans, D. The Internet Of Things: How The Next Evolution Of The Internet Is Changing Everything [J]. Cisco Ibsg, 2011: 1-11.

[4]. Wang, Y., Li, Y., & Chen, Y. Edge Computing: A Comprehensive Survey On Its Challenges And Applications [J]. Ieee Communications Surveys & Tutorials, 2019, 21(1): 40-60.

[5]. Yang, K., Wu, S., & Li, J. A Survey On Mobile Edge Computing: Architecture, Applications, And Security [J]. Ieee Internet Of Things Journal, 2019, 6(1): 178-195.

[6]. Shi, W., Cao, J., & Zhang, Q. Edge Computing: Key Characteristics And Applications [J]. Ieee Internet Of Things Journal, 2018, 5(2): 895-906.

[7]. Nguyen, D. T., Chen, J., & Rho, S. Designing Mobile Applications For Edge Computing [C]//Proceedings Of The Ieee Global Communications Conference (Globecom'17). 2017: 1-6.

[8]. Li, Y., Yi, S., & Li, Y. A Survey On Mobile Cloud Computing: Architectures, Applications, And Security [J]. Mobile Networks And Applications, 2014, 19(2): 233-250.

[9]. Bonomi, F., Milito, R., & Zhu, J. Fog Computing: A New Computing Paradigm [C]//Proceedings Of The 1st International Conference On The Internet Of Things. 2012: 1-6.

[10]. Kwan, H., Wu, Z., & Ng, T. Mobile Edge Computing: A Survey [J]. Ieee Communications Surveys & Tutorials, 2018, 20(1): 324-349.

[11]. Roman, R., Najm, T., & Lopez, J. Security In Mobile Edge Computing: A Survey [J]. Journal Of Network And Computer Applications, 2018, 112: 3-15.

[12]. Liu, S., Zhang, S., & Chen, X. Identity-Based Encryption For Fine-Grained Access Control [C]//Proceedings Of The 13th International Conference On Cryptology In India (Indocrypt'12). 2012: 135-149.

[13]. Goyal, V., Pandey, O., & Sahai, A. Attribute-Based Encryption For Fine-Grained Access Control [C]//Proceedings Of The 13th Acm Conference On Computer And Communications Security (Ccs'06). 2006: 89-98.

[14]. Waters, B. Ciphertext-Policy Attribute-Based Encryption: An Expressive And Efficient Realization [C]//Proceedings Of The 14th International Conference On Practice And Theory In Public Key Cryptography (Pkc'11). 2011: 53-70.

[15]. Wang, S., Zhang, Q., & Liu, J. A Hierarchical Attribute-Based Encryption Scheme For Cloud Computing [J]. Ieee Transactions On Information Forensics & Security, 2016, 11(6): 1265-1277.

[16]. Yang, Y., Liu, J., & Liang, K. Achieving Revocable Fine-Grained Encryption Of Cloud Data [C]//Proceedings Of The 20th European Symposium On Research In Computer Security. 2015: 146-166.

[17]. Zuo, C., Shao, J., & Wei, G. Cca-Secure Abe With Outsourced Decryption For Cloud Computing [J]. Future Generation Computer Systems, 2018, 78: 730-738.

[18]. Blaze, M., Bleumer, G., & Strauss, M. Divertible Protocols And Atomic Proxy Cryptography [C]//Proceedings Of The 17th Annual International Conference On The Theory And Applications Of Cryptographic Techniques (Eurocrypt’98). 1998: 127-144.

[19]. Green, M., & Ateniese, G. Identity-Based Proxy Re-Encryption [C]//Proceedings Of The 5th Applied Cryptography And Network Security (Acns’07). 2007: 288-306.

[20]. Weng, J., Deng, R., & Ding, X. Conditional Proxy Re-Encryption Secure Against Chosen-Ciphertext Attack [C]//Proceedings Of The 4th International Symposium On Information, Computer, And Communications Security (Asiaccs’09). 2009: 322-332.

[21]. Liang, K., Man, H., & Liu, J. A Secure And Efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption For Cloud Data Sharing [J]. Future Generation Computer Systems, 2015, 52: 95-108.

[22]. Yang, Y., Zhu, H., & Lu, H. Cloud-Based Data Sharing With Fine-Grained Proxy Re-Encryption [J]. Pervasive & Mobile Computing, 2015, 28: 122-134.

[23]. Shao, J., Lu, R., & Lin, X. Secure Bidirectional Proxy Re-Encryption For Cryptographic Cloud Storage [J]. Pervasive & Mobile Computing, 2016, 28: 113-121.

[24]. Khan, A. N., Kiah, M. L. M., & Ali, M. A Cloud-Manager-Based Re-Encryption Scheme For Mobile Users In Cloud Environment: A Hybrid Approach [J]. Journal Of Grid Computing, 2015, 13(4): 1-25.

[25]. Khan, A. N., Ali, M., & Khan, A. U. R. A Comparative Study And Workload Distribution Model For Re-Encryption Schemes In A Mobile Cloud Computing Environment [J]. International Journal Of Communication Systems, 2017, 30(16): E33.

[26]. Rivest R L, Adleman L, Dertouzos M L. A Perspective On Data Security And Privacy Homomorphisms. Ieee Transactions On Information Theory, 1978, 24(4): 382-387.

[27]. Gentry C, Zhang H. A Fully Homomorphic Encryption Scheme Based On Lattice Cryptography. Journal Of Cryptology, 2010, 23(2): 142-172.

[28]. Dijk M V, Gentry C, Halevi S. Homomorphic Encryption For Polynomial Computations. Acm Transactions On Intelligent Systems And Technology, 2011, 2(2): 1-17.

[29]. Brakerski Z, Vaikuntanathan V. Fully Homomorphic Encryption From Standard Lattice Assumptions. Journal Of Cryptology, 2014, 27(4): 1217-1250.

[30]. Gentry C, Sahai A, Waters B. Attribute-Based Encryption For Fine-Grained Access Control Of Encrypted Data. Acm Transactions On Information Systems Security, 2014, 17(2): 1-28.

[31]. Louk M, Lim H. Mobile Multi-Cloud Computing With Secure Homomorphic Encryption. Journal Of Network And Computer Applications, 2016, 61: 49-59.

[32]. Baharon M R, Shi Q, Llewellyn-Jones D. Lightweight Homomorphic Encryption For Mobile Cloud Computing. Ieee Transactions On Cloud Computing, 2016, 4(4): 884-897.

[33]. Yang K, Jia X H. Cloud Storage Auditing Services: Challenges And Solutions. Ieee Communications Surveys & Tutorials, 2014, 16(1): 1-26.

[34]. Wang C, Wang Q, Ren K, Et Al. Privacy-Preserving Public Auditing In Cloud Computing. Ieee Transactions On Cloud Computing, 2013, 1(2): 1-13.

[35]. Wang Q, Wang C, Ren K, Et Al. Enabling Public Auditability For Dynamic Data In Cloud Computing. Ieee Transactions On Cloud Computing, 2013, 1(2): 1-13.

[36]. Yang K, Jia X H. Secure Dynamic Auditing Protocol For Cloud Data Storage. Ieee Transactions On Cloud Computing, 2014, 2(1): 1-10.

[37]. Sookhak M, Gani A, Khan M K, Et Al. Remote Data Auditing For Securing Big Data In Cloud Computing. Information Sciences, 2017, 380: 101-116.

[38]. Li J T, Zhang L, Liu J K, Et Al. Efficient Public Auditing For Cloud Data With Low-Performance Devices. Ieee Transactions On Information Forensics And Security, 2017, 12(5): 1085-1097.

[39]. Lin C, Shen Z D, Chen Q, Et Al. Data Integrity Verification In Mobile Cloud Computing. Journal Of Computer And System Sciences, 2016, 77(1): 146-157.

[40]. Wang C, Cao N, Ren K, Et Al. Secure And Efficient Ranked Keyword Search Over Outsourced Cloud Data. Ieee Transactions On Parallel And Distributed Systems, 2012, 23(8): 1467-1479.

[41]. Cao N, Wang C, Li M, Et Al. Multi-Keyword Ranked Search Over Encrypted Cloud Data With Privacy Protection. Ieee Transactions On Parallel And Distributed Systems, 2014, 25(1): 222-233.

[42]. Li H W, Liu D X, Dai Y S, Et Al. Efficient Multi-Keyword Ranked Search In Encrypted Mobile Cloud Data. Ieee Transactions On Emerging Topics In Computing, 2015, 3(1): 127-138.

[43]. Li J, Ma R H, Guan H B. An Efficient Search Scheme For Encrypted Data In Mobile Cloud Environments. Ieee Transactions On Cloud Computing, 2017, 5(1): 126-139.

[44]. Wang C J, Li W T, Li Y, Et Al. Ciphertext-Policy Attribute-Based Encryption With Keyword Search. International Journal Of Information Security, 2013, 12(3): 225-237.

[45]. Zheng Q J, Xu S H, Ateniese G. Verifiable Attribute-Based Keyword Search Over Encrypted Data. Ieee Transactions On Information Forensics And Security, 2015, 10(2): 123-136.

[46]. Liu P L, Wang J F, Ma H, Et Al. Verifiable Public Key Encryption With Keyword Search Using Kp-Abe. International Journal Of Information Security, 2014, 13(5): 431-442.

[47]. Sun W H, Yu S C, Lou W J, Et Al. Verifiable Attribute-Based Keyword Search With Owner-Enforced Authorization. Ieee Transactions On Parallel And Distributed Systems, 2016, 27(4): 1187-1198.

[48]. Kamara S, Papamanthou C, Roeder T. Dynamic Searchable Symmetric Encryption For Cloud Data. Proceedings Of The 19th Acm Conference On Computer And Communications Security, 2012: 965-976.

[49]. Kamara S, Papamanthou C. Parallel And Dynamic Searchable Symmetric Encryption. Proceedings Of The 17th International Conference On Financial Cryptography And Data Security, 2013: 258-274.

[50]. Sun W H, Liu X F, Lou W J, Et Al. Verifiable Conjunctive Keyword Search Over Dynamic Encrypted Cloud Data. Ieee Conference On Computer Communications, 2015: 2110-2118.

[51]. Xia Z H, Wang X H, Sun X M, Et Al. A Secure Multi-Keyword Ranked Search Scheme In Encrypted Cloud Data. Ieee

Transactions On Parallel And Distributed Systems, 2016, 27(2): 340-352.

[52]. Hu B S, Liu Q, Liu X H, Et Al. Dynamic Attribute-Based Keyword Search In Cloud Computing. Ieee International Conference On Communications, 2017: 1-6.

[53]. Zhang, Y., Wang, F., & Chen, H. (2013). Proxy Re-Encryption With Keyword Search Based On Bilinear Maps. Journal Of Computer And System Sciences, 79(5), 761-776.

[54]. Kogan, A., & Shahar, M. (2014). Proxy Re-Encryption With Keyword Search In Cloud Computing. Information Sciences, 270, 32-46.

[55]. Liu, Y., & Wang, H. (2013). Cca-Secure Anonymous Proxy Re-Encryption With Keyword Search. Theoretical Computer Science, 509, 29-44.

[56]. Zhang, C., Zhang, J., & Liu, Y. (2015). Attribute-Based Proxy Re-Encryption With Keyword Search For Secure Data Sharing In Cloud Computing. Future Generation Computer Systems, 50, 77-86.

[57]. Li, J., Xu, C., & Zhang, H. (2016). A Shared Authority-Based Privacy-Preserving Authentication Scheme For Cloud Computing. Ieee Transactions On Services Computing, 9(2), 186-198.

[58]. Tsai, J. L., & Lo, N. W. (2017). A Secure And Efficient Authentication Scheme For Mobile Cloud Computing Services. Ieee Systems Journal, 11(2), 1217-1227.

[59]. Jiang, Y., & Zhang, Y. (2016). Security Analysis Of A Privacy-Aware Authentication Scheme For Mobile Cloud Computing Services. Ieee Transactions On Cloud Computing, 5(1), 150-160.

[60]. He, D. B., & Khan, M. K. (2016). A Lightweight Privacy-Preserving Authentication Scheme For Mobile Cloud Computing. Ieee Transactions On Information Forensics And Security, 11(5), 982-994.

[61]. Lo, N. W., & Tsai, J. L. (2016). A Lightweight Conditional Privacy-Preserving Authentication Scheme For Vehicular Ad Hoc Networks. Ieee Transactions On Intelligent Transportation Systems, 18(6), 1717-1726.

[62]. Mahmood, K., Chaudhry, S. A., & Naqvi, H. (2016). A Lightweight Authentication Scheme Based On Elliptic Curve Cryptography For Smart Grid Communications. Future Generation Computer Systems, 64, 142-152.

[63]. Buyya, R., Calheiros, R. N., & Dumas, A. (2011). Intercloud: Convergence Of Clouds. Ieee Computer, 44(3), 54-58.

[64]. Zeadally, S., & Rojas, C. (2016). Attribute-Based Access Control For Peer-To-Peer Networks. Journal Of Network And Computer Applications, 64, 29-37.

[65]. Yang, Y., Zheng, X., & Liu, X. (2018). Dynamic Cross-Domain Anonymous Authenticated Key Management For E-Health Systems. Future Generation Computer Systems, 81, 1-10.

[66]. Yang, X., Huang, X., & Liu, J. K. (2017). Secure Handover Authentication For Mobile Cloud Computing With User Anonymity. Ieee Transactions On Cloud Computing, 5(1), 42-54.

[67]. Mccarthy, D., & Malone, P. (2016). Implementing Personal Cloudlets For Privacy-Aware Data Storage. Ieee Cloud Computing, 3(4), 36-43.

[68]. He, D. B., Wu, L. B., & Khan, M. K. (2016). A Study On Handover Authentication Protocols In Mobile Networks Using Identity-Based Cryptography. Journal Of Network And Computer Applications, 62, 137-145.

[69]. Yu, S. C., Wang, C., & Ren, K. (2011). Secure And Scalable Access Control In Cloud Computing. In Proceedings Of The 30th Ieee International Conference On Computer Communications (Infocom'11) (Pp. 1-5).

[70]. Xue, K. P., & Xue, Y. J. (2016). Robust And Auditable Access Control For Cloud Storage. Ieee Transactions On Information Forensics And Security, 11(4), 837-848.

[71]. Jin, Y., Tian, C., & He, H. (2016). A Secure Data Access Control Scheme For Mobile Cloud Computing. In *Proceedings Of The 6th International Conference On Big Data And Cloud Computing (Bdcloud'16)* (Pp. 172-179).

[72]. Zhang, P., & Liu, J. K. (2018). A Secure Access Control Mechanism For Fog Computing Environments. Future Generation Computer Systems, 78, 753-762.

[73]. Huang, Q. L., Yang, Y. X., & Wang, L. C. (2018). Secure Data Access Control With Ciphertext Updates In Fog Computing. Ieee Access, 6, 12941-12950.

[74]. Zhou, L., & Varadharajan, V. (2015). Secure Role-Based Access Control For Encrypted Data In Cloud Storage. Ieee Transactions On Information Forensics And Security, 10(12), 2452-2465.

[75]. Chen, H. C., & Wu, L. (2015). A Negotiation-Based Role Assignment For Role-Based Access Control. In Proceedings Of The 11th International Conference On Broadband And Wireless Computing, Communication And Applications (Bwcca'15) (Pp. 538-543).

[76]. Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Enhancing Role-Based Access Control With Attributes. Ieee Computer, 43(6), 79-81.

[77]. Li, H. J., Wang, S., & Tian, X. X. (2015). Extended Role-Based Access Control In Cloud Computing: A Survey. In Proceedings Of The 4th International Conference On Computer Engineering And Networks (Cenet'15) (Pp. 821-831).

[78]. Almutairi, A., Sarfraz, M., & Basalamah, S. (2012). A Distributed Architecture For Access Control In Cloud Computing. Ieee Software, 29(2), 36-44.

[79]. Chen, L. Q., & Urian, R. (2015). Direct Anonymous Attestation With Attributes. In Proceedings Of The 8th International Conference On Trust And Trustworthy Computing (Trust'15) (Pp. 228-245).

[80]. Pasuouleti, S. K., Ramalingam, S., & Buyya, R. (2016). Secure Privacy-Preserving Data Outsourcing For Mobile Devices In Cloud Computing. Journal Of Network And Computer Applications, 64, 12-22.

[81]. Ding Y, Wang W, Zhang Z. A Lightweight Data Privacy Protection Method For Mobile Cloud Computing Using Permutation Techniques[C]//The 5th International Conference On Cloud Computing And Big Data (Ccbd'19). 2019: 85-92.

[82]. Zhang H, Ding X, Yu H, Et Al. Privacy-Preserving Data Sharing In Hybrid Cloud Environments[J]. Journal Of Cloud Computing: Advances, Systems And Applications, 2018, 7(1): 1-11.

[83]. Kang M, Kim K, Seo Y. Location Privacy Preservation Through Distributed Cache Techniques[C]//2016 Ieee International Conference On Communications (Icc'16). 2016: 1-6.