SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I12P119

Volume 11 Issue 12, 208-228, December 2024

Review Article

Cloud Safe: A Survey of Encryption, Access Control, and Network Protection Strategies

A.G. Vishvanath[1]*, D. Ganesh[2]

[1,2]*School of Computer Science & IT, JAIN (Deemed-to-be University), Karnataka, India.*

**Corresponding Author : vishvanathag@bit-bangalore.edu.in*

Received: 11 October 2024 Revised: 12 November 2024 Accepted: 10 December 2024 Published: 31 December 2024

Abstract *- The rising dependence on cloud computing needs strong security measures to secure sensitive data and maintain service availability. Data breaches, illegal access, and data loss pose significant hazards to cloud security. Effective security techniques encompass numerous levels of protection. Firstly, encryption is critical for safeguarding data at rest and in transit, confirming that the information remains unreadable to unauthorized users even if intercepted. Secondly, network security methods, such as firewalls, intrusion detection and prevention systems, and secure communication protocols, are needed to defend against external threats and vulnerabilities. Lastly, access control technologies, including multi-factor authentication, role-based access control, and identity management systems, are vital for restricting who can access and modify data in the cloud. This multi-layered approach ensures comprehensive protection against a wide range of security risks. In conclusion, while cloud computing provides considerable scalability, flexibility, and cost-effectiveness benefits, it also poses new security issues. Organizations may ensure a safe cloud computing environment by establishing comprehensive security measures such as encryption, network security, and effective access restrictions for their data and systems. According to the research, compromised credentials cause 61% of data breaches, highlighting the significance of access control procedures. Additionally, there is potential for upgrading encryption systems, dynamic authorization, and anomaly detection through machine learning and deep learning approaches. This research further supports a multi-layered security approach to safeguard private cloud data from new attacks.*

Keywords *- Cloud computing, Security, Data, Encryption, Access control, Network.*

1. Introduction

Cloud Computing (CC) is quickly becoming an important service in Internet computing. Cloud-based computing services have become increasingly popular in the last few years, offering tremendous advantages for various computer activities, including business support [1]. Cloud computing focuses on management, scalability, and availability. Cloud computing offers cost-effectiveness, on-demand services, ease, universality, multi-tenancy, flexibility, and reliability [2, 3].

The cloud's pay-per-use model has attracted consumers and organizations seeking new revenue-generating methods. A 2020 poll of 750 worldwide cloud experts found that COVID-19 had led to a 47% increase in cloud service spending in 2021 alone. Cloud service customers in IoT, Machine Learning (ML)/AI, data warehousing, and server less industries are expected to rise by an average of 47.2%. Despite competition among digital titans like Google, Microsoft, and IBM, there is always a need for more research on security solutions [4]. Any cloud service's success depends on offering cloud administrators, software developers, and end users a satisfying experience. Cloud adoption faces complexity, compliance, security, dependency, privacy, control, and cost challenges. Cloud computing security is critical as data and applications may be spread over numerous tiers, depending on the selected service architecture. Researchers identified security as the primary worry for cloud computing due to uncertainty. Network security remains a fundamental security commit in CC, addressing external and internal threats [5].

The National Institute of Standards and Technology (NIST) established a service-based paradigm as the standard for cloud computing. This paradigm contains Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), which define all IT sharable resources, including software, hardware, and networks [6, 7, 8] shown in Figure 1. IaaS offers a flexible "on-demand" internet connection, allowing for server capacity adjustments based on available space. Examples are AWS EC2, GCE, GoGrid, and 3tera. The price of IaaS rises depending on the consumer's use. PaaS enables customers to create cloud services only limited by the provider by renting hardware, operating systems, and network capacity.

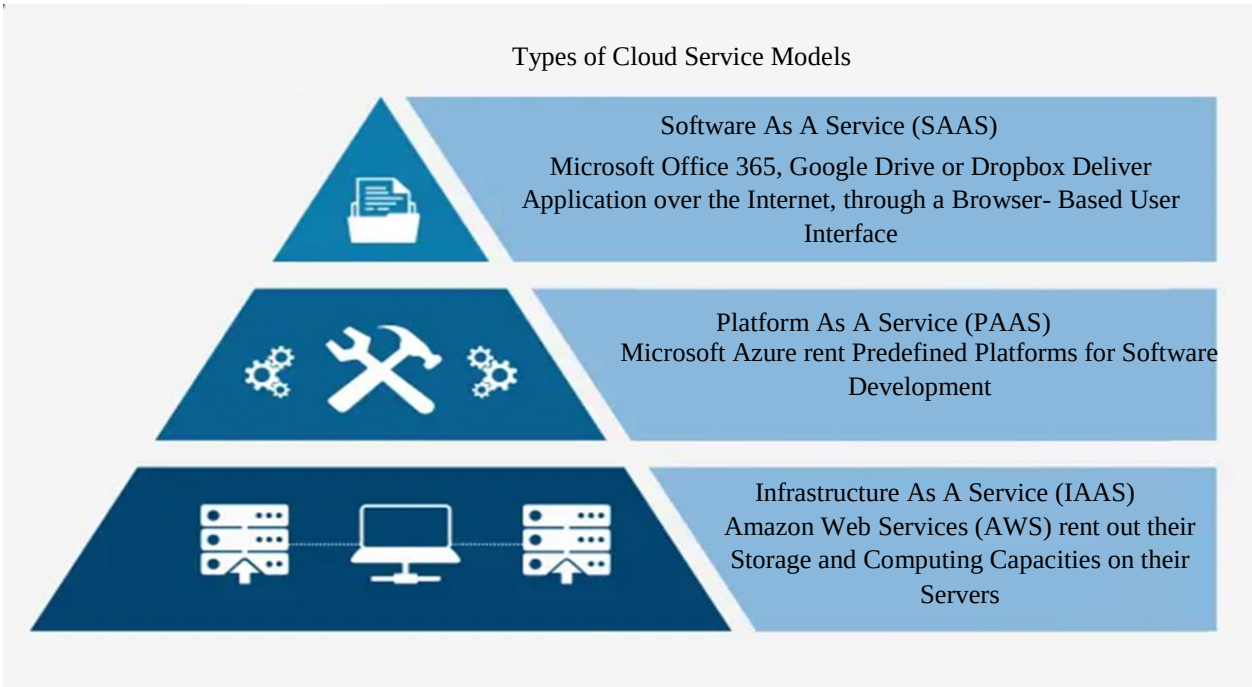

Fig. 1 Types of cloud service model

Microsoft Azure and Force.com are the best examples. Scalability, mobility, flexibility, and user-friendliness are just a few advantages of PaaS. Network and host-based intrusions pose security problems. SaaS clients employ cloud-based software. Web browsers are used to access applications, and customers rely on their service provider to ensure security. The provider must ensure that users do not access each other's information. [9, 10]. Cloud computing consists of four [11] deployment models: public cloud (cloud service provider in charge of dispersing, managing, and offering the cloud to the general public), hybrid clouds (owned and distributed by many companies), and private clouds (owned by a company that is in charge of distribution and sales), community clouds (cloud services that are shared by several companies which, assist a certain community with the same issue) [12]. Although CC is a rapidly expanding technology, security issues must be resolved before it can be widely utilized [13]. Cloud security is crucial for protecting client data, but hackers are more likely to target it since cloud systems require more excellent protection than traditional methods [14]. Cloud computing requires robust security measures to safeguard data and infrastructure from various attackers [15]. According to a survey by Fujitsu, 88% of cloud users are worried about data security and want to know what happens on physical servers. Three main concerns with cloud computing platforms are lack of transparency, control, and security guarantees [16]. While cloud computing has witnessed widespread adoption, the research gap lies in the insufficient integration of advanced, adaptive, and scalable security mechanisms to combat dynamic and sophisticated threats. Current solutions often focus on isolated aspects, such as encryption or network security, without addressing the need for a holistic approach that integrates access control, threat detection, and automated mitigation strategies. Furthermore, there is a lack of comprehensive studies that leverage ML and Deep Learning (DL) for proactive anomaly detection, context-aware authorization, and real-time response to emerging threats.

These gaps limit the ability of existing systems to ensure trust, transparency, and robust protection, especially in complex multi-tenant and hybrid cloud environments. Even though cloud computing is very helpful, several security concerns need to be resolved to protect sensitive data and maintain confidence in cloud services. The key security considerations include Data Breaches, Data Loss, Service Disruptions, Account Hijacking, Compliance and legal issues, Insider threats, and Vulnerabilities in shared technologies. This survey article examines modern security methods in cloud computing, emphasizing access control, symmetric and asymmetric encryption, and network security. It focuses on how ML, DL, and optimization techniques improve these security mechanisms. ML and DL algorithms in access control improve anomaly detection and enable dynamic authorization modification via adaptive access control systems in response to contextual factors and user behaviour. For encryption, both symmetric and asymmetric systems benefit from ML techniques that improve cryptanalysis and key management. ML and DL models improve network security by enhancing Intrusion Detection Systems (IDS), analyzing network traffic patterns to forecast possible security breaches, and automating threat mitigation using optimization techniques. Combining these sophisticated algorithmic approaches makes cloud security more resilient, flexible, and efficient, offering comprehensive protection against changing cyber threats.

1.1. Cloud Deployment Models

Cloud computing deployment models refer to the configuration of cloud infrastructure based on the ownership, management, and access patterns. The four primary deployment models are Public, Private, Hybrid, and Community Cloud—each has unique advantages, disadvantages, and implications for security.

1.1.1. Public Cloud

A Public Cloud is managed by third-party providers, offering resources like servers, storage, and applications to the public over the internet. It is cost-effective due to shared infrastructure, scalable for changing demands, and easy to manage as providers handle the infrastructure. However, it raises security concerns due to shared resources, limited customization, and potential compliance issues for organizations with strict regulatory requirements. Public clouds are ideal for small businesses, startups, and non-sensitive applications like websites, streaming, and SaaS. Security challenges include data privacy, robust access control and encryption to protect data.

1.1.2. Private Cloud

A Private Cloud is a cloud infrastructure dedicated to a single organization, hosted internally or externally. It offers enhanced security and privacy, as the environment is exclusive to one organization, reducing the risk of data leakage. Customization is another advantage, as organizations can tailor the cloud to meet specific needs, including security configurations. Private clouds are also ideal for meeting compliance requirements, especially for industries with strict data protection regulations. However, they come with higher costs for implementation and maintenance, limited scalability compared to public clouds, and increased management overhead. Private clouds are suited for large enterprises, especially in healthcare, finance, and government, and for sensitive applications requiring strong data protection. Security implications include increased control over data, but organizations must ensure proper resource management and disaster recovery plans to protect against internal threats and data loss.

1.1.3. Hybrid Cloud

A Hybrid Cloud combines private and public cloud elements, offering organizations the flexibility to leverage the scalability of the public cloud while keeping critical workloads and sensitive data in a private cloud. The main advantages include flexibility, allowing organizations to move workloads between clouds for optimized costs and performance, and scalability, which ensures the ability to expand infrastructure while keeping sensitive data secure. It also offers cost efficiency, using the public cloud for non-critical workloads and maintaining security for sensitive data in the private cloud. However, hybrid clouds have challenges, such as complexity in managing and integrating both environments, security risks during data transfers, and significant integration costs. Hybrid clouds are ideal for organizations with fluctuating workloads, such as those involved in big data analytics or dealing with seasonal demand, and businesses needing to comply with regulatory data requirements while utilizing public cloud services. Security implications include data segmentation to appropriately manage sensitive and non-sensitive data, secure communication through encryption during transfers, and compliance, allowing organizations to meet regulatory requirements by keeping sensitive data in the private cloud.

1.1.4. Community Cloud

A Community Cloud is shared by multiple organizations with similar goals or compliance requirements, offering a dedicated infrastructure where resources, security measures, and governance are shared. Its advantages include shared resources, reducing cloud infrastructure and services costs, and fostering a collaborative environment among organizations with similar needs. It also allows for security and compliance, as the platform can be tailored to meet industry standards and regulatory requirements. However, community clouds have limited control compared to private clouds, involve complex governance due to shared policies across organizations, and may face scalability limitations depending on the community's size. They are ideal for organizations within the same industry or region, such as research institutions or government agencies, and for enterprises with common regulatory needs like healthcare or finance. Security implications include data sharing and privacy, requiring strict access control to prevent unauthorized access, shared responsibility for governance, and cost-effective security features tailored to industry requirements.

1.2. Educating End-Users and Organizations

As cloud computing becomes more integral to business operations, ensuring the security of cloud environments is a shared responsibility. While cloud providers implement robust security measures at the infrastructure level, end-users and organizations must adopt best practices to mitigate risks and safeguard sensitive data. Educating users and organizations about their role in cloud security is essential to prevent breaches, data loss, and other security incidents. The following best practices can help maintain secure cloud environments.

1.2.1. Educating End-Users on Cloud Security

End-users often serve as the first line of defense against security threats in cloud environments. By educating users on how to interact with cloud services securely, organizations can significantly reduce the risk of breaches. Key practices include:

- Strong Password Management: Encourage users to create strong, unique passwords for cloud accounts, at least 12 characters long, with a mix of uppercase, lowercase, numbers, and symbols. Avoid weak or reused passwords.

Password managers can help securely store and generate complex passwords.

- Multi-Factor Authentication (MFA): Implement MFA for all cloud accounts to add a layer of security beyond just passwords. Users should be encouraged to activate MFA and understand how to use it effectively (e.g., via SMS, email, or authentication apps).
- Awareness of Phishing Attacks: Educate users on identifying phishing attempts and malicious links in emails, texts, or cloud communication platforms. Users should be instructed not to click on suspicious links or share sensitive information without verification.
- Regular Software Updates: Encourage end-users to keep their devices and applications up to date, including operating systems, browsers, and any software used to access cloud services. Security patches often address vulnerabilities that attackers can exploit.
- Access Control and Data Sharing: Users should understand the importance of carefully managing data access. Educate them on secure best practices for sharing data, such as using encrypted links or cloud-based sharing settings that allow only authorized users to access data.

1.2.2. Organizational Responsibilities in Cloud Security

While educating end-users is critical, organizations must take proactive steps to manage and secure their cloud environments. The following organizational practices are crucial:

- Data Encryption: Encrypt sensitive data both at rest and in transit to ensure that even if data is intercepted, it remains unreadable without the proper decryption keys. Educate employees on encrypting files before uploading them to cloud storage services.
- Implementing Role-Based Access Control (RBAC): Organizations should implement RBAC to ensure only authorized users can access specific data or systems. This minimizes the risk of data leakage or accidental exposure. Users should be educated about their specific roles and their associated permissions.
- Regular Security Audits and Monitoring: Regularly audit cloud infrastructure to identify and address vulnerabilities. This includes monitoring cloud services for suspicious activity, such as unauthorized access attempts or unusual data transfers. Automated tools can track and alert administrators to potential security threats.
- Backup and Disaster Recovery Plans: Implement a robust backup strategy to ensure that data can be recovered in case of a breach, natural disaster, or system failure. Regularly test the backup process and educate employees on initiating disaster recovery protocols when necessary.
- Compliance and Regulatory Requirements: Organizations must ensure their cloud usage complies with relevant regulations and standards. Providing employees with training on these compliance requirements ensures that the organization adheres to necessary security measures and avoids penalties.

1.2.3. Security Policies and Training for Employees

Continuous training and establishing security policies are essential for maintaining a secure cloud environment. Some key aspects include:

- Security Awareness Training: Provide ongoing security training to employees, covering topics such as cloud security, phishing prevention, safe cloud data sharing, and incident reporting. Training should be regularly updated to address evolving security threats.
- Incident Response and Reporting: Ensure employees know how to report suspicious activity, breaches, or vulnerabilities. A clear incident response plan and training employees to react to security events are vital to minimize damage.
- Cloud Vendor Security Assessment: Organizations should regularly assess their cloud service providers to ensure they meet security standards. Cloud vendors should provide transparency regarding their security protocols, compliance certifications, and response times to security incidents.

1.2.4. Best Practices for Using Cloud-Based Applications and Services

Organizations should adopt secure practices when utilizing various cloud services, such as Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS):

- Secure API Usage: When integrating third-party applications with cloud services, ensure that APIs are securely implemented with authentication and authorization mechanisms.
- Survey Permissions for Cloud Applications: Regularly survey and update user permissions for cloud applications and services. Remove access for users who no longer require it and ensure that only necessary applications can access sensitive data.
- Monitor Cloud Usage: Monitor cloud usage to ensure that cloud resources are used appropriately. This includes tracking user activity, data access patterns, and service consumption to identify any abnormal behavior that may indicate a security threat.

1.2.5. Leveraging Cloud Security Tools

Organizations can further enhance cloud security by utilizing various tools and technologies, such as:

- Cloud Security Posture Management (CSPM): CSPM tools help organizations identify and remediate security risks in cloud environments, ensuring compliance with best practices and security frameworks.
- Identity and Access Management (IAM) Systems: IAM tools allow organizations to define and manage user

access policies across cloud platforms, ensuring that only authorized individuals can access sensitive data and systems.

- Cloud Access Security Brokers (CASB): CASBs provide an additional layer of security by monitoring cloud usage and enforcing security policies for both cloud services and devices accessing them.

Maintaining secure cloud environments is not solely the responsibility of cloud providers—it is a shared responsibility that involves both end-users and organizations. By educating end-users on safe practices, implementing organizational policies, and leveraging security tools, cloud environments can be better protected against evolving threats. Security awareness training, strong access controls, and continuous monitoring are key strategies to prevent data breaches, ensure compliance, and promote a culture of cloud security.

1.3. Access Control Mechanisms

Access control is critical to cloud security, ensuring that only authorized users can access and modify sensitive data. The following sub-sections explore specific implementations of three key access control technologies: Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and Identity Management Systems (IDMS), along with real-world examples.

- Multi-Factor Authentication (MFA): Multi-factor authentication strengthens security by requiring users to provide two or more verification forms before accessing a system. These factors typically include something the user knows (password), something the user has (security token or smartphone app), or something the user is (biometric data).
- Role-Based Access Control (RBAC): RBAC is an access control model where permissions are assigned based on a user's organizational role. Users are granted access to resources depending on their job function, limiting exposure to sensitive information only to those who need it.
- Identity Management Systems (IDMS): Identity management systems manage an organization's user identities, authentication, and access control. These systems ensure that only authenticated users can access specific cloud resources with the appropriate permissions. IDMS also enables features like Single Sign-On (SSO), where users can access multiple systems with one set of credentials.

These technologies ensure cloud systems' integrity, confidentiality, and security by restricting access to only authorized individuals based on established criteria.

1.4. Analysis of Symmetric and Asymmetric Encryption

Encryption plays a pivotal role in ensuring the confidentiality and integrity of data within cloud environments.

Table 1. Summary of comparative analysis for symmetric and asymmetric encryption

Feature	Symmetric Encryption	Asymmetric Encryption
Key Mechanism	Single shared key for encryption and decryption	Public-private key pair for encryption/decryption
Performance	High speed; suitable for large datasets	Slower; ideal for secure key exchange and authentication
Security	Vulnerable to key distribution issues	Higher security but computationally intensive
Examples	AES, DES	RSA, ECC
Use Cases	Data at rest, bulk encryption	Key exchange, digital signatures

Two primary types of encryption commonly utilized in cloud security are symmetric and asymmetric. Symmetric encryption, such as Advanced Encryption Standard (AES), is highly efficient for encrypting large volumes of data but faces challenges in secure key distribution. Asymmetric encryption, exemplified by RSA and Elliptic Curve Cryptography (EEC), provides robust solutions for secure key exchange and digital signatures but can be computationally intensive. Recent advancements in encryption technologies include homomorphic encryption, which enables computations on encrypted data without decryption, and post-quantum cryptography, which addresses the potential threats quantum computing poses. A hybrid approach combining symmetric and asymmetric encryption is often adopted to balance performance and security. Table 1 provides a comparative analysis of symmetric and asymmetric encryption to illustrate their characteristics and applications better:

1.5. Network Protection Strategies

Network security is essential to safeguard cloud environments from external and internal threats. While traditional methods like firewalls and Intrusion Detection Systems (IDS) are still widely used, emerging technologies like zero-trust architectures and behavioral analytics have become critical in enhancing network security. The following sub-sections explore these advancements in detail.

- Zero-Trust Architecture (ZTA): Zero-trust architecture operates on the principle of "never trust, always verify." In a zero-trust model, every user, device, and system is treated as potentially compromised, and all access requests must be continuously verified, regardless of the network's location. This approach mitigates risks associated with insider threats and lateral movement within the network.
- Behavioral Analytics: Behavioral analytics leverages machine learning and data analysis to monitor and analyze user activity patterns across the network. By

establishing baselines of normal behavior, it can detect deviations indicative of malicious activity, such as insider threats or compromised accounts. This proactive security measure allows for the early identification of threats, even before they are fully executed.

- Advanced Intrusion Detection and Prevention Systems (IDPS): While traditional IDS and IPS rely on signature-based detection, advanced systems integrate anomaly detection and machine learning to enhance accuracy and reduce false positives. These systems use real-time network traffic analysis, looking for unusual patterns that may indicate a potential threat.

These emerging technologies—zero-trust architectures, behavioral analytics, and advanced IDPS—work together to create a more dynamic and resilient network security framework. They provide better protection against evolving cyber threats by continuously verifying and analyzing access requests, ensuring that unauthorized activity is detected and mitigated as early as possible. This survey offers a complete survey of numerous techniques and recommends future research possibilities for improving cloud security. This study discusses privacy and security issues in the cloud and offers possible remedies. The primary contributions of the study are as follows:

1. The fundamental ideas of CC and the entities linked with CC architecture are introduced.
2. Highlights the importance of strong security measures due to threats like data breaches, illegal access, and data loss.
3. Research issues and future research directions are discussed.
4. A categorization of risks and solutions is established.
5. Cloud security risks and challenges are classified into three groups based on their security condition.

2. Literature Survey

The survey examined cloud computing security standards: encryption, access restrictions, and network security. Encryption protects data integrity and confidentiality, whereas access controls govern user privileges and guarantee that only authorized people may access resources. Firewalls, VPNs, and intrusion detection systems are examples of network security tools that protect data flows and the network perimeter. Organizations may improve the security posture of their cloud installations by identifying vulnerabilities and best practices in these areas. Organizations may improve their resistance to emerging attacks and cloud security posture by addressing these critical areas.

2.1. Cloud Security Measures Based on Encryption

Orobosade et al. [17] The increasing number of fraudulent cloud users has made cloud data more vulnerable. A hybrid encryption technique that combines symmetric and asymmetric cryptography schemes is offered to overcome this. The privacy model employs an Advanced Encryption Standard (AES) as the initial data encryption algorithm, followed by Elliptic Curve Cryptography (ECC) with an AES key. This technique assures data confidentiality and security in the cloud, providing a secure environment for users who use the cloud for various objectives. However, encryption procedures might have an impact on data availability. For example, accessing the data is difficult if the encryption keys are lost or damaged.

Kumar et al. [18] The study provides a multilayer cryptography-based security architecture for cloud computing that combines symmetric and asymmetric key cryptography methods. DES and RSA are used for multilayer encryption and decryption on the sender and receiver sides, increasing security. This strategy increases cloud consumer's and service providers' openness, lowering security risks. Implemented in Java with the CloudSim cloud simulator tool, the approach improves data security and uploads and downloads text files faster than previous systems. However, integrating the proposed paradigm with older systems that do not support DES or RSA may be difficult, restricting the adoption of the security model.

Shukla et al. [19] The study article compares a new encryption-based method for cloud computing against established encryption procedures like DES, AES, and Blowfish. The algorithm's performance was evaluated using characteristics such as encryption time and the avalanche impact on plain text data. Experimental findings on MATLAB revealed that the suggested method performed 64% better with these parameters and a key, generating 57% better outcomes than other standard algorithms. This new technique is essential for ensuring efficient data protection in cloud computing settings.

Deng et al. [20] Cloud computing has increased data sharing, raising privacy concerns. To solve this, an Identity-Based Encryption Transformation (IBET) paradigm is proposed, which combines Identity-Based Encryption (IBE) with Identity-Based Broadcast Encryption (IBBE). IBET enables data access based on known identities, hence eliminating certificate administration in secure distributed systems. It also transforms IBE ciphertexts to IBBE ciphertexts, enabling new users to access data. The suggested approach has been demonstrated to be both secure and efficient. However, thorough security study and validation of IBET's resistance to attacks can be difficult and time-consuming. Ramachandra et al. [21] Sensitive data are protected by cloud security, making big data research an essential study area. However, privacy and security issues have limited cloud service utilization. The disadvantages of current privacy-preserving techniques include their dependence on third parties, incorrect analysis, lack of data privacy, and performance efficiency. The Triple Data

Encryption Standard (TDES) methodology addresses these issues by increasing key sizes to safeguard attacks and data privacy. According to experimental results, TDES may effectively protect massive healthcare data in the cloud while requiring less time for encryption and decryption. However, depending only on TDES for large data security in the Cloud may pose regulatory problems, particularly in highly regulated industries like healthcare.

Shawkat et al. [22] Resources are shared across the Internet in the context of the distributed computing paradigm known as CC, which raises security issues with regard to data availability, integrity, and confidentiality. The Rivest Shamir Adlemen (3kRSA) technique outperforms the Triple Data Encryption Standard (3DES) approach in terms of output bytes and complexity, according to a comparative analysis conducted on eyeOS. The primary drawback of 3kRSA is its processing time; 3DES operates more quickly. This is beneficial for storing big volumes of data in CC. Asymmetric encryption's key distribution, authentication, speed, data integrity, and secrecy are also significant, as they allow calculations to be performed on encrypted data. However, encryption techniques are intended to improve security, and they are prone to flaws and attacks, which might expose sensitive data to misuse or modification.

Teng et al. [23] study investigates improved data encryption techniques for cloud computing, emphasizing increasing data security. The authors investigate standard AES and offer a modified version that incorporates random disturbance information, enhances column mix operation and key choreography, and is tested on Hadoop. Based on the findings, the suggested actions will enhance data security in the cloud computing environment by protecting attribute privacy and improving encryption efficiency for outsourced data storage in mobile cloud computing. To improve data security, the encryption procedure is made more difficult by changing the column mix operation and key choreography in AES.

Jayaprakash et al. [24] The study suggests an improved Merkle hash tree approach for multi-owner cloud data security. This approach uses leaf nodes with hash tags and a non-leaf node with a hash table to encrypt vast amounts of data. The model's correct structure allows for effective data mapping and easy identification of changes. It enables privacy-preserving public audits and safe cloud storage. Data owners upload and modify their data using a private key; the data is then stored on a cloud server and divided into batches. Compared to existing approaches, the suggested method saves 2-167 ms on encryption and decryption. However, Introducing additional security measures, such as private key authentication and third-party audits, may influence the user experience, causing usability issues or increased complexity for end users of the cloud storage system. Chinnasamy et al. [25] Cloud computing enables public users to access computer data, but data security remains an issue. Existing encryption techniques, such as CP-ABE, may compromise user and data privacy by providing plaintext access policies with ciphertext. In order to address this, a unique method is created that uses a hashing technique to conceal access policies and a signature verification scheme to defend against insider attacks. The proposed system is computationally and expressively comparable to current CP-ABE systems; it may be evaluated for Internet of Things (IoT) access control. However, Adding extra levels of encryption and verification may raise the system's complexity. This complexity could increase computational overhead and resource needs, affecting system performance and scalability.

Goyal et al. [26] Remote Cloud services are effective at overcoming native resource shortages, but their availability is dependent on the quality of the connection to the server. Poor connectivity can fail. For big data transfers, computing on a device can outperform remote processing. Good performance depends on the proper distribution of application mechanisms between devices and cloud platforms, determined by runtime situations. Data is distributed between clouds using hybrid encryption (DES and Blowfish), and a cloud structure with dynamic checking across various cloud facilities is established. However, implementing a dynamic cloud structure with dynamic checking demands advanced algorithms and procedures, which might add complexity and overhead to the system.

Abroshan et al. [27] This work offers a cryptographic method that minimizes performance impact while enhancing cloud computing security. It increases security and performance by encrypting data and keys using an EC-based method and an enhanced Blowfish algorithm. The use of digital signature technology ensures data integrity. After evaluation, the method improved throughput, execution time, and memory use. This strategy is especially beneficial in cloud situations where computational speed is critical. However, managing encryption keys can add complexity and overhead, especially when using various encryption techniques.

Senthilkumar et al. [28] Cloud computing provides various functions, including data sharing and distribution. The Asymmetric Key Blum-Goldwasser Cryptography (AKBGC) technique is presented to increase communication security in cloud services while incurring minimum expenses. Users submit queries to a cloud server, which employs Blum-Goldwasser Cryptography (BGC) to improve confidentiality and data security. The AKBGC approach employs a probabilistic encryption algorithm to encrypt user data using a public key, generate ciphertext, and distribute it to users. The receiver must first undertake a key authentication process to access the original data. Experiments with several criteria, including data secrecy, communication overhead, space complexity, and throughput, have demonstrated that the approach enhances data confidentiality while reducing

communication overhead. However, Managing and securely delivering public keys to users and cloud servers can be difficult. Chinnasamy et al. [29] Cloud companies face difficulty assuring file security due to data processing and transfer threats. Researchers propose hybrid approaches that combine ECC and Blowfish to overcome this issue to create a hybrid algorithm. This technology ensures great data security and secrecy while overcoming the constraints of classic symmetric and asymmetric methods. Hybrid cryptography is used to overcome the disadvantages of symmetric and asymmetric approaches, resulting in high-quality data transit and storage. This approach is related to previous hybrid methods, illustrating the utility of hybrid cryptography in CC. However, while the suggested hybrid technique strives to provide high data security and secrecy, there may be performance trade-offs compared to existing methods. Bermani et al. [30] Researchers have been concentrating on cloud computing security due to the growing relevance of data storage and its varied uses. Cryptography techniques are critical for securing data on cloud services. A hybrid cryptographic algorithm made up of Blowfish, AES, and the Message-Digest method (MD5) is used in this study's data security paradigm to produce quick and dependable data encryption. This method addresses the vital topic of data security in CC. However, managing keys for ECC and Blowfish adds complexity to key production, distribution, and storage. Table 2 shows the Cloud security measures based on Encryption.

Table 2. Cloud security measures based on encryption

Ref	Author	Techniques	Significance	Limitation / Future Scope	Implementation Details
[17]	Orobosade et al.	Hybrid Encryption (AES + ECC)	The dual-layer encryption technique offers a higher degree of protection, making it more difficult for attackers to compromise the system's security.	Key management issues can impact data availability if encryption keys are lost or damaged.	Hybrid encryption is used in cloud-based healthcare and financial services to protect sensitive data during transmission.
[18]	Kumar et al.	Multilayer Cryptography (DES + RSA)	The approach increases the cloud storage environment's resilience to future attacks by strengthening its security by integrating the RSA and DES algorithms.	In the future, this approach may be enhanced using AI to improve cloud security.	Deployed in financial cloud services f or secure online banking transactions.
[19]	Shukla et al.	Proposed encryption Techniques like key generation and encryption phase.	The algorithm's efficiency and security advantages make it ideal for the scalable nature of cloud computing.	Organizations seeking technical help, upgrades, or troubleshooting resources may encounter difficulties due to the algorithm's niche status and minimal ecosystem support.	Efficient for cloud storage solutions handling large volumes of user-generated data.
[20]	Deng et.al	IBET	IBET's transformation technique converts IBE ciphertext into IBBE ciphertext, allowing for efficient data transfer without sacrificing security or needing substantial encryption adjustments.	Implementing IBET may be difficult owing to the intricacy of the transformation mechanism and underlying cryptographic techniques.	Implemented in secure cloud services providing sensitive information access based on verified identities.
[21]	Ramachandra et al.	TDES	In the continuously The TDES technique offers a strong defense against known and new attacks in the changing environment of cyber security threats.	The TDES technique should include effective key management procedures to prevent theft, loss, or unauthorized access.	Used in cloud-based healthcare applications for patient data security.
[22]	Shawkat et.al	3kRSA	The proposed approach focuses on algorithmic efficiency, allowing for efficient encryption while reducing computing costs.	The higher complexity of RSA can affect the processing speed of large datasets.	Suitable for secure data transmission across large enterprise cloud platforms.

[23]	Teng et al.	Modified AES	The proposed approach enhances the decryption efficiency.	Key choreography and column mix operations may lead to performance overhead.	Effective for cloud storage services that require high encryption standards for mobile applications.
[24]	Jayaprakash et al.	Merkle hash tree approach	Cloud data security is improved by employing an updated Merkle hash tree authentication architecture.	Additional security measures might introduce complexity and affect user experience.	Used in cloud audit services for verifying data integrity in large-scale cloud deployments.
[25]	Chinnasamy et al.	Hashing algorithm	The suggested method's compliance with CP-ABE and other encryption algorithms improves interoperability with various cloud computing platforms and services.	Increased computational overhead and resource requirements may impact scalability.	Deployed in IoT access control systems to secure device-level data exchange in cloud environments.
[26]	Goyal et al.	DES and Blowfish	The hybrid encryption strategy improves data security and privacy, making it appropriate for managing sensitive customer records in the healthcare or financial industries.	Complex algorithms may add overhead, affecting real-time performance.	Hybrid encryption is used in multi-cloud environments for secure data distribution.
[27]	Abroshan et al.	Enhanced Blowfish algorithm with elliptic-curve-based algorithm.	The suggested system improves throughput using practical encryption algorithms and optimization tactics, allowing faster data processing and transmission inside the cloud environment.	Managing multiple encryption keys can add complexity.	Applied in cloud-based systems that require high-performance, real-time data protection.
[28]	Senthilkumar et al.	AKBGC technique	The AKBGC approach attempts to provide greater security with minimal overhead, guaranteeing that the encryption and decryption processes have no substantial influence on system performance.	Future work on the AKBGC approach can incorporate other hashing and tree-based data structures to enhance cloud data security.	Used in cloud computing for secure user data access, reducing latency in cloud query responses.
[29]	Chinnasamy et al.	ECC and Blowfish	By combining ECC with Blowfish, the hybrid technique utilizes symmetric and asymmetric encryption capabilities, resulting in a stronger security framework.	Potential trade-offs in performance compared to existing methods.	Implemented enterprise cloud solutions for secure file transfers and storage.
[30]	Bermani et al.	AES, Blowfish, and MD5	Ensures high degrees of data secrecy by encrypting data with Blowfish and safeguarding keys with ECC.	Complexity in managing encryption keys, especially for distributed systems.	Deployed in public cloud services, offering secure, scalable data storage for diverse applications.

Summary. Future studies will look at cloud data security in quantum computing environments, including the potential for AI to improve security. Implementing IBET may be difficult owing to its complexity and lack of ecosystem assistance. TDES procedures should be created based on physics and quantum theory to avoid key theft. Elliptic curve encryption will be utilized to secure data retrieval in cloud storage applications, notably in the small healthcare sector. The method's applicability in other fields, including data governance, compliance, and interaction with current systems, is also being investigated. AES will be evaluated in various infrastructures, including cloud computing, which has enormous data volumes. Future work on the AKBGC technique may include various hashing and tree-based data structures. Steganography might be utilized to solve major distribution problems.

2.2. Cloud Security Measures Based on Access Control

Access control is essential for cloud security, regulating user permissions and preventing unauthorized access. Modern approaches integrate cryptographic techniques, trust-based policies, and dynamic role assignments to address evolving challenges. Key mechanisms include Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and Identity Management Systems (IDMS), each contributing unique advantages. This section surveys their specific implementations, highlighting their roles in strengthening cloud security.

2.2.1. Implementations of Multi-Factor Authentication (MFA)

According to Celiktas et al. [31], this work offers a crucial approach to access management that transfers hierarchical access controls to digital platforms. This method allows data owners to use public cloud services from within and outside their company's network, turning public cloud systems into private clouds. It suits hierarchical organizational structures and reduces concerns about moving mission-critical data to the public cloud. It is based on Shamir's secret-sharing technique and the polynomial interpolation method. It minimizes significant overheads, such as public and private storage requirements and is computationally efficient. The method is immune to collaborative attacks and provides key distinguishability security, eliminating the possibility of data breaches caused by key disclosures. However, ensuring all users understand and effectively use the key access control system can be difficult. User training is necessary to prevent mistakes that might harm security, but it costs time and resources.

Mabdal et al. [32] COVID-19 pandemic has raised the likelihood of cyber security threats, MAC spoofing, and DDoS/DoS attacks as people transition to cloud computing services. In order to illustrate MAC spoofing threats in the context of Software-Defined Networks (SDNs), this paper provides a zero-trust access control policy that restricts inbound network traffic. The technique uses dynamic threshold stamping, self-learning features, a multiplicative increase and additive reduction algorithm, and other techniques to identify complex attacks and rectify legitimate user traffic before labelling it as an attacker. However, implementing a zero-trust network model with dynamic thresholds and self-learning characteristics can be challenging and resource-intensive.

Abdul et al. [33] The fast growth of mobile technology has caused people to switch from traditional devices to smartphones and tablets, which are projected to carry most worldwide IP traffic. Mobile Cloud Computing (MCC) helps to reduce resource constraints by providing computing resources with low effort. However, security in MCC is challenging due to users' unpredictable and dynamic behavior and the proliferation of online computerized data. To solve this, a study proposes an access control method that estimates trust based on the user's unpredictable behavior to reduce fraudulent acts by authenticated users. Performance statistics demonstrate that the method correctly detects and mitigates malicious users. However, integrating this method into the current mobile cloud infrastructure might be difficult and require considerable changes.

2.2.2. Specific Implementations of Role-Based Access Control (RBAC)

Bhatt et al. [34] The Internet of Things (IoT) is changing people's lives. However, hackers gain unauthorized access to consumer gadgets and data by circumventing access control and inadequate authentication procedures. Prominent cloud and IoT service providers use customized versions of policy-based access control and role-based access control (RBAC), such as Google Cloud Platform (GCP), Azure, and Amazon Web Services (AWS). In order to secure smart devices, data, and resources in a cloud-enabled Internet of Things architecture, a dynamic and adaptable access control strategy is needed to get around limitations. This work builds upon the previous method by formalizing Attribute-Based Access Control (ABAC) for AWS IoT. The AWS IoT platform is used to implement the strategy, shown through an industrial IoT use case. However, the proposed approach intends to improve security and must be thoroughly evaluated to discover and mitigate possible security threats. Thilakarathne et al. [35] Cloud computing provides worthwhile services like SaaS, IAAS, and PAAS. Though, it confronts issues such as data security, abuse of cloud services, and cyber-attacks. This research determines to examine current cloud access control model approaches and identify future research possibilities for establishing an enhanced model for public cloud data storage. A hybrid cloud architecture and hybrid cryptography schema were added to the model, and its security implications, functionality, performance, and data integrity were evaluated. However, integrating the proposed paradigm with current cloud services and older systems may raise compatibility concerns, necessitating considerable changes. Harnal et al. [36] Cloud computing decreases user burdens, but security concerns remain. The objective is to detect and protect user data against illegal access. Users grant access based on their traits, not on established identities. The Efficient and Flexible Role-Based Access Control (EF-RBAC) approach for CC that guarantees security and confidentiality is presented in this paper. RBAC ensures that only particular information is available and limits resource access to authorized users. The proposed method provides more flexibility for a better cloud user experience. However, implementing an EF-RBAC system can be difficult and time-consuming, necessitating extensive analysis and role and permission definition.

Opakunle et al. [37] Businesses are increasingly using semantic technology to address complex information management issues. The emergence of access control restrictions has become a critical security concern with the growth of cloud computing. Numerous strategies have been

implemented, but the outcomes have been negligible. These strategies include Role Based Access Control (RBAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Obligatory Access Control (OAC). A Semantic Time-Based Access Control (STBAC) paradigm is introduced to address the particular security needs of cloud environments. It generates a time-sensitive key for user access control and access to cloud data resources. This concept was created and used to protect patients' medical records in a cloud setting. However, integrating this approach with current cloud systems and apps may be difficult, resulting in compatibility and interoperability concerns. Gunjal et al. [38] The growing trend of storing vast volumes of data in the cloud has created worries about security and preventing illegal access.

A safe data sharing method is provided that employs Role Based Access Control and AES encryption to achieve secure key distribution and information exchange for dynamic groups. The technology safeguards data and enables regeneration in the event of unlawful use. A proxy server is responsible for fulfilling this operation, which involves keeping information in public and private cloud storage. Users can access data on the public cloud, but the private cloud retains higher security. The user receives a recovery of the original data that was safeguarded in the private cloud. The technology provides the highest level of security and privacy. However, using a proxy server for data regeneration presents a single point of failure, which may pose a security and reliability risk.

2.2.3. Implementations of Identity Management Systems (IDMS)

Prabhu Kavin et al. [39] This study presents a more robust security outline for cloud consumers' data by combining access control mechanisms, encryption/decryption techniques, and digital signature algorithms. It includes a novel ECC based key generation algorithm for highly secure keys, an Identity-based Elliptic Curve Access Control mechanism (Id-EAC) for limiting data accessibility, a binary value-based two-phase encryption and decryption algorithm, and a module function-based Lightweight Digital Signature Algorithm for data integrity. The system provides excellent data security, accessibility, and integrity, with experimental findings indicating better efficiency over previous techniques. However, The suggested approaches employ advanced cryptographic algorithms that may be difficult to implement and demand specialist knowledge.

Khan et al. [40] Cloud computing enables low-cost access to shared resources such as storage, applications, networks, and services. However, data security remains a serious concern, with inadequate identity and access management, unsecured interfaces, hijacking, persistent attacks, and data threats. Traditional access control techniques fail to monitor user behavior and are vulnerable to assaults. This paper presents a trust-based access control system that evaluates user, network, demand, and security behavior to determine trust value before giving user access. The mechanism's policies are specified in terms of trust value outcomes. However, monitoring and evaluating diverse actions may generate privacy concerns among users since it requires considerable data collecting and processing.

Karthik et al. [41] Attribute-based encryption is a potential method for securing data sharing in the cloud, particularly in Big Data settings such as Apache Hadoop. However, standard attribute-based encryption lacks efficient keyword-based search, critical for swiftly extracting data from big databases. This work introduces Strategy-Attribute-Based Access Control to overcome this issue using a full-fledged key-strategy attribute-based encryption system. This technique gives users flexible and fine-grained access control over encrypted data, making it perfect for secure data sharing scenarios like cloud computing. However, the additional layer of encryption and access restriction may result in delay, notably during data retrieval and decryption. Raid et al. [42] study introduce a novel Token-Revocation Access Control (TR-AC) that improves the security of cloud-based energy optimization services. TR-AC employs a series of multi-authorities to assess each user's authenticity level, allowing them to withdraw their authorization before accessing the utilities. This method is safe against non-authentic attackers, according to Diffie-Hellman assumptions. TR-AC takes far less time to encrypt and decrypt data than earlier methods, guaranteeing that it has no impact on the performance of the cloud-hosted system.

This strategy is critical for increasing local energy output while limiting the cybersecurity risks associated with cloud storage. However, regardless of the improved security procedures, putting sensitive data in the cloud poses cybersecurity concerns. Attackers constantly evolve their tactics, and new weaknesses may develop, possibly jeopardizing the system. While Multi-Factor Authentication (MFA) is not the primary focus of most studies, it is often integrated with security frameworks like zero-trust and trust-based access controls to provide multi-layered protection in cloud environments.

Role-Based Access Control (RBAC) emerges as a widely adopted security mechanism, with enhancements such as Efficient and Flexible RBAC (EF-RBAC) and integration with attribute-based controls for more granular and adaptable access management. Identity Management Systems (IDMS) are further advanced through innovative approaches like Identity-based Elliptic Curve Access Control (Id-EAC) and trust-based mechanisms, ensuring secure and efficient access in complex environments, including big data and IoT systems. These mechanisms underline a comprehensive approach to strengthening security across diverse technological ecosystems. Table 3 shows the Cloud security measures based on Access control.

Table 3. Cloud security measures based on access control

Ref. No	Author	Techniques	Significance	Limitation/ Future scope	Implementation Details
[31]	Celiktas et al.	Shamir's secret sharing scheme and Newton's interpolation method	The technique provides strong security measures, limiting access to keys to authorized users with proper permissions and reducing data breaches.	Organizations without a clearly defined or stable hierarchy may struggle to adapt this plan to their needs, limiting its usefulness.	Used in corporate cloud infrastructures to secure sensitive data.
[32]	Mandal et al.	Zero trust access control policy	The conceptual and practical findings show that the suggested strategy outperforms existing methodologies regarding accuracy and detection rates. This results in enhanced security against a variety of cyber assaults.	Analyzing traffic and deleting faked users are time-consuming tasks that might be improved in future research.	Used in SDN environments to prevent MAC spoofing in cloud systems.
[33]	Abdul et al.	Trust- and Role-Based Access Control	The system adapts to the users' unpredictable and dynamic behavior, ensuring continuous security evaluation and reaction.	The additional processes necessary for trust value computation may cause delays in gaining access, hurting user xperience, particularly during busy hours.	Applied in mobile cloud services for secure user access.
[34]	Bhatt et al.	ABAC	ABAC can handle various IoT scenarios, including device kinds, communication protocols, and data formats. Its adaptability makes it appropriate for complicated IoT environments.	The fine-grained nature of ABAC rules can cause performance overheads.	Implemented in AWS IoT for securing industrial IoT systems.
[35]	Thilakarathne et al.	Role based access control	The methodology allows for more exact control over who may access specific data and resources, lowering the risk of unwanted access.	Future research might refine cryptographic algorithms and access control methods to decrease computational cost and increase performance.	Applied in hybrid cloud systems for enterprise-level data storage.
[36]	Harnal et.al	EF-RBAC	The RBAC paradigm is ideal for large businesses with complicated access control requirements, as it enables scalable and manageable security rules.	Implementing an EF-RBAC system can be challenging and time-consuming because it requires considerable analysis and determining roles and permissions.	Used in cloud-based CRM systems to control access based on user roles.

[37]	Opakunle et.al	DAC,OAC, MAC, and RBAC, STBAC	It provides more granular control over who has access to what data and when which improves security and compliance in sensitive situations like healthcare.	The approach is designed for cloud environments and may not be easily adaptable to other types of IT infrastructure without significant changes.	Applied in cloud-based healthcare systems for patient data protection.
[38]	Gunjal et al.	Role-Based Access Control	It provides numerous redundancy choices, which improves system dependability and fault tolerance.	The extra procedures necessary for encryption, decryption, and data regeneration may cause delays, harming the user experience.	Implemented hybrid cloud storage systems with public and private tiers.
[39]	Prabhu Kavin et al.	Id-EAC	It provides extremely secure keys, making it difficult for attackers to compromise the system.	Future research could explore the use of intelligent agents with time constraints and fuzzy rules to make decisions during data transfer.	Deployed in financial services to secure sensitive transaction data.
[40]	Khan et al.	Trust-based access control mechanism	This technique greatly improves data integrity and minimizes the danger of data breaches.	Users may find the trust-based approach more complex and less straightforward than traditional access control systems.	Used in cloud-based e-commerce platforms to secure user transactions.
[41]	Karthik et al.	Strategy-Attribute-Based Access Control	The technique is intended to manage massive volumes of data shared in Big Data contexts while guaranteeing that security measures do not impair performance or scalability.	Without improvements, the ABE scheme may lack efficient keyword search capabilities, crucial for swiftly accessing data in Big Data applications.	Used in cloud-hosted Big Data analytics platforms for controlled data sharing.
[42]	Riad et.al	TR-AC	Hosting the energy optimization utility on the cloud improves scalability, flexibility, and resource management.	TR-AC will offer the option to specify a range and period for each permission granted to the UID in the future.	Deployed in energy optimization cloud systems to secure user data access.

Summary. The ABAC system, intended for cloud settings, may be challenging to adapt to various IT infrastructures due to its fine-grained nature and time-consuming duties. Future research might concentrate on improving cryptographic algorithms and access control mechanisms to reduce computational costs while increasing performance. Intelligent agents with time limits and fuzzy rules might be considered for data transport. Implementing an EF-RBAC system might be difficult since it requires significant analysis to determine roles and permissions. Users may find the trust-based method more challenging than standard access control systems, and the ABE scheme may lack efficient keyword search capabilities. Future TR-AC will provide the ability to set a range and time for each permission issued to the UID.

2.3. Cloud Security Measures Based on Network Security

Attou et al. [43] CC offers on-demand admission to network and computing resources, but security remains a concern. The solutions seek to increase security by monitoring resources, services, and networks and identifying assaults. An Intrusion Detection System (IDS) monitors traffic and detects

unusual activity. This study describes a cloud-based intrusion detection approach based on random forest and feature engineering, which includes an RF classifier to improve accuracy. The model was examined and verified on two datasets, yielding 98.3% ACC and 99.99% ACC, indicating superior performance in terms of ACC, accuracy, and recall compared to earlier efforts. However, Integrating the IDS into the current cloud infrastructure can be complicated, requiring significant maintenance efforts to ensure ongoing functioning and upgrades.

Setia et al. [44] The paper focuses on the security problems of Vehicular Ad-Hoc Network (VANET) technology, namely VANET Cloud, which is rapidly employed in connected and driverless cars. The study provides a novel architectural framework for capturing and analyzing network flows in the VANET Cloud environment, including ML techniques for categorization and predictive analytics. The framework has a 99.59% accuracy rate, indicating the potential to improve security measures in VANET Cloud installations dramatically. Its versatility guarantees practical application to real-world systems, allowing fast responses to security risks and breaches. However, adding security methods like traffic analysis and ML-based categorization to the VANET Cloud environment may increase connection latency. Ramamoorthy et al. [45] Cloud computing provides flexible resources and services over the internet, but security remains an issue. To solve this, a Modified Dove Swarm Optimization Based Enhanced Feed Forward Neural Network (MDSO-EFNN) is developed to analyze network traffic in a cloud context. Network Intrusion Detection Systems (NIDS) are used to detect assaults. An NSL-KDD network traffic dataset is used in the study, which is preprocessed with Z-Score normalization and the Continuous Wavelet Transform before being examined with MDSO-EFNN. The approach shows considerable accuracy, precision rate, sensitivity, and specificity improvements.

However, the suggested method may be limited in its interpretability and transparency due to the black-box nature of neural network models and the complexity created by optimization techniques. Gulia et al. [46] Cloud computing is essential for sharing resources and information, but keeping it safe from hackers is difficult. An Intrusion Detection System (IDS) is required to detect and monitor network activity. This study aims to control assaults using ML with an Artificial Bee Colony (ABC) algorithm known as Group-ABC. The IDS detector was applied, and the simulation outcomes were obtained using G-ABC. Various attacks were found, including user-to-rotation, probing, root to local, backdoors, worms, and denial-of-service attacks. The simulation study was carried out on two datasets. However, combining ML approaches with optimization algorithms such as G-ABC can result in substantial computational complexity and overhead. Almiani et al. [47] Cloud-native computing is gaining popularity owing to its ease and convenience in developing distributed systems and applications. However, it is also vulnerable to hostile intrusions, notably Distributed Denial of Service (DDoS) attacks. An effective backpropagation neural network was used to develop a sophisticated model for network intrusion detection for modern DDoS attacks. The model outperformed most existing learning models by detecting reflecting DDoS attacks with an accuracy of 97.07%. It also achieved competitive run time performance while fulfilling the containerized cloud computing's latency criteria. Although the approach delivers competitive runtime performance, extending the system to accommodate enormous data and significant traffic volumes in large cloud-native systems may cause difficulties. Balajee et al. [48] The increased data flow, flexibility, pay-as-you-go, and internationally distributed resources in today's environment make network security and cloud settings essential. According to a recent poll, 79% of North American firms had a cloud data break in March 2022. AWS dominates the industry with 34% and a $200 billion market in 2022. A hybrid DL-based solution was developed to improve network vulnerability detection using the CSECIC-IDS-2018 dataset. The approach pre-processes and normalizes raw data before extracting features from normalized data using Principal Component Analysis (PCA) and classifying attack cluster data with the Smart Monkey Optimized Fuzzy C-Means algorithm (SMO-FCM). The DL-based AutoEncoder method classifies attacks. Compared to 11 other methodologies, the methodology attained an intrusion detection accuracy of 95 percent.

However, integrating the suggested intrusion detection system with current cloud infrastructure and security standards may cause compatibility and interoperability issues. Talib et al. [49] The study propose a Virtual Private Network (VPN) to ensure the security of connections across large networks. After meeting network performance parameters like time delay and throughput, a VPN is suggested for network security. Artificial intelligence attack predictors and VPNs are also used to prevent malicious activities on these connections. ML techniques like Random Forests (RF) and Naive Bayes (NB) can detect and prevent harmful assaults. Artificial neural networks, which utilize DL to learn attack behaviors, can also be used for attack prediction. According to the study, ML and AI approaches can dramatically improve VPN security and performance by identifying and stopping unwanted attacks. However, integrating the proposed solution with existing network infrastructure and security standards may offer compatibility issues, necessitating considerable changes and disrupting current operations.

Krishnan et al. [50] The study provides a network management architecture for OpenStack Clouds that incorporates Software-Defined Networking (SDN), Network Function Virtualization (NFV), and ML/AI. The framework uses artificial intelligence to monitor virtual machine and application behaviour, allowing for speedy issue resolution. The OpenStackDP architecture contains lightweight

monitoring, intelligent sensors that identify anomalies, a threat analytics engine, and defensive responses implemented as virtual network functions. This design delivers high-speed risk finding and response, resulting in better Quality of Service (QoS) and speedier recovery from cyber-attacks. The framework outperforms previous SDN-based OpenStack solutions for Cloud architectures. Despite high accuracy, there is a possibility of false positives and false negatives in threat detection, which can result in unnecessary defensive responses or missing threats. Dong et al. [51] This paper introduces a Dynamic Uncertain Causal Attack Graph (DUCAG) model and a Causal Chain-based Risk Probability Calculation (CCRP) algorithm to address the difficulties of assessing network assaults in cloud computing.

The DUCAG model provides unclear causalities between attack events, but the CCRP algorithm changes causality weights using alarm data and causal chain reasoning. Despite insufficient and redundant warning information, the CCRP accurately forecasts attacker actions and attack probabilities in unclear settings. The DUCAG approach may accurately define and forecast complex attack causalities, making it useful for assessing network security, forecasting future attacker behavior, and changing defense methods. However, keeping the DUCAG model and CCRP algorithm up to date with new threats and attack patterns may necessitate ongoing maintenance and updates, increasing the operational overhead of cloud computing systems.

Fatani et al. [52] Intrusion Detection Systems (IDS) are critical components of cyber security, and recent advances in metaheuristic optimization algorithms and DL approaches have increased their accuracy and efficiency. This research proposes a novel IDS model that incorporates DL and optimization techniques. The model employs a CNN-based feature extraction method and a revised version of Growth Optimizer (GO), known as MGO, along with the Whale Optimization Algorithm (WOA), to speed up the search practice. Extensive surveys and evaluations of public datasets from cloud and IoT contexts have yielded promising findings in detecting previously undisclosed assaults with high accuracy rates.

However, the proposed method's effectiveness may be limited to specific datasets or network environments, resulting in a lack of robustness and generalization skills across varied cyber threat landscapes. Srilatha et al. [53] this paper presents a Network Intrusion Detection and Prevention System (NIDPS) designed to identify and protect various network assaults. The NSLKDD benchmark data set, created over a decade ago, is not current network traffic and low-footprint attacks. The Canadian Institute of Cyber Security introduced the CICIDS2017 network data set, which solves the NSL-KDD problem. The efficient IDPS is implemented and tested in a network environment using ML techniques like Linear Regression (LR), Random Forest (RF), and ID3. An Enhanced ID3 is proposed to identify abnormalities in network activity and classify them. The study also develops an auto encoder network, PCA, and K-Means Clustering for benchmark purposes. Self-Taught Learning (STL) is applied to the CICIDS2017 dataset for network intrusion. However, implementing numerous ML algorithms and methodologies may increase complexity and overhead, affecting the system's performance and scalability in production applications.

Praise et al. [54] High-performance computer resources and sensitive data are distributed and stored rapidly using CC infrastructure. However, because of outside threats, security lapses are happening more frequently. Typical firewall rules and packet filtering techniques are inappropriate to solve these problems. A Deep Packet Inspection-based firewall (RLPM) verifies incoming packets' payload signatures to stop malicious attacks. Reinforcement learning and parallel rapid pattern matching are combined in RLPM to produce an optimum solution that outperforms current techniques regarding reaction speed, throughput, and stopping malicious attacks.

In real cloud computing scenarios, RLPM reduces response time by 10% while increasing throughput by 10%. However, the enhanced security features of RLPM may necessitate additional processing resources and memory, particularly in large-scale cloud systems, raising infrastructure costs. Table 4 shows the Cloud security measures based on network security. Sharma et al. [55] propose implementing the Zero Trust security model in cloud environments to address challenges like growing access points, visibility issues, and multi-cloud complexity. The model enhances security by continuously verifying user and device identities using IAM, micro-segmentation, and continuous monitoring. Benefits include reduced attack vectors and improved security, particularly in healthcare and finance. However, challenges include scaling Zero Trust across hybrid and multi-cloud platforms and integrating it with existing systems.

The paper does not specify a dataset but highlights the need for further research on scalability and integration. Hossain et al. [56] propose the ASMCC+ authentication scheme for mobile cloud computing using a PKE model with ADOW trapdoor functions. It ensures security against IND-CCA attacks and malicious private key generators (mPKG) and achieves adaptive one-wayness, pseudorandom ciphertext, and key-dependent message security. The model improves privacy by minimizing third-party access to master-secret keys. However, it lacks a specified dataset and detailed result measures, focusing on security proofs and performance analysis. A key limitation is mitigating mPKG risks and scaling the scheme for real-world use. Mahmood et al. [57] propose a hybrid ML-based Network Intrusion Detection System (NIDS) that integrates feature selection via XGBoost and data balancing through SMOTE.

Table 4. Cloud security measures based on network security

Ref.No	Author	Techniques	Significance	Limitation/ Future scope
[43]	Attou et al.	Intrusion detection model based RF.	The model's capacity to detect anomalous activity makes it useful for spotting previously undiscovered and developing dangers. This proactive security technique helps mitigate hazards before they evolve into full-scale assaults.	DL and ensemble learning approaches will be used in future work to increase memory, as NSL-KDD is currently insufficient.
[44]	Setia et al.	ML approach	The method's adaptation means it can grow with evolving security risks, offering strong protection against fresh attack vectors while maintaining long-term efficiency.	Adding security methods like traffic analysis and ML-based categorization to the VANET Cloud environment may increase connection latency.
[45]	Ramamoorthy et al.	MDSO-EFNN	Combining optimization approaches with neural network processing provides a comprehensive approach to security, covering different types of vulnerabilities and attack vectors prevalent in cloud systems.	The future work will be improved with more improvements in performance evaluations.
[46]	Gulia et al.	ML with ABC	The combination of ML and G-ABC optimization improves the accuracy and reliability of intrusion detection.	Future evaluations will assess more attacks to improve the effectiveness of the proposed IDS.
[47]	Almiani et al.	Resilient back Propagation neural network.	The proposed method satisfies containerized cloud computing platforms' delay requirements while offering competitive runtime performance.	Expanding the resilience and reliability of the intrusion detection model should be the goal of investigating ensemble learning techniques, which combine many models to enhance prediction performance.
[48]	Balajee et.al	Hybrid DL	The method is capable of identifying a wide range of network assaults, which improves overall network security.	Scaling the approach to handle massive volumes of data and high-speed network traffic may be difficult due to its complexity and computing needs.
[49]	Talib et al.	DL and ML methods like RF and NB.	The system is built to manage broad networks and many users; hence, it is ideal for expansive and dynamic network environments.	More studies are needed to evaluate the usefulness of these strategies in real-world circumstances and determine the best algorithms for different types of networks and data.
[50]	Krishnan et.al	ML/AI techniques	By immediately recognizing and mitigating risks, the technology helps cloud providers and consumers maintain and improve their Quality of Service.	The suggested work's implementation approach does not identify high/low volume attack variants, which will be addressed in future research.
[51]	Dong et.al	DUCAG and CCRP.	The suggested method dynamically examines the network security state, resulting in a better awareness of current security circumstances and prospective threats.	The future will focus on creating algorithms that automatically generate DUCAGs using domain expertise and historical log data, which will be deployed to large-scale actual cloud platform networks.
[52]	Fatani et.al	CNN, MGO,WOA	The use of DL and optimization approaches improves the accuracy of the IDS, allowing it to recognize and classify harmful activities within networks.	Future uses for the developed MGO may include human activity recognition, healthcare, and identifying false news.

[53]	Srilatha et al.	LR, RF, ID3	The suggested NIDPS can identify and prevent a wide range of well-known network assaults, improving enterprises' overall security posture against cyber threats.	Further research into advanced ML and DL techniques, like reinforcement learning and transformer-based models, could improve detection skills and resilience to sophisticated attacks.
[54]	Praise et al.	RLPM	Safeguarding the firewall's ability to identify and prevent harmful attacks is ensured by the RLPM's fast convergence to an optimal solution.	The proposed solution can be expanded further to address future attacks on cloud data centres.
[55]	Sharma et al.	Zero Trust security model	Enhances security by continuously verifying user and device identities using IAM, micro-segmentation, and continuous monitoring. Reduces attack vectors and improves security, especially in healthcare and finance.	Challenges include scaling Zero Trust across hybrid and multi-cloud platforms and integrating it with existing systems.
[56]	Hossain et al.	ASMCC+ authentication scheme (PKE model with ADOW trapdoor functions)	Ensures security against IND-CCA attacks and malicious private key generators (mPKG) and achieves adaptive one-wayness, pseudorandom ciphertext, and key-dependent message security. Enhances privacy by minimizing third-party access to master-secret keys.	Lacks specified datasets and detailed result measures. Challenges include mitigating mPKG risks and scaling the scheme for real-world use.
[57]	Mahmood et al.	Hybrid ML-based NIDS (XGBoost, SMOTE, RF, DT, KNN, MLP, CNN, ANN)	Integrates feature selection via XGBoost and data balancing through SMOTE, achieving impressive accuracy in network attack detection. Strengths include heightened detection rates, scalability, and real-time deployment suitability.	Performance could be further optimized for emerging security threats-additional research is needed for feature selection refinement.

This system employs various algorithms to detect network attacks, including RF, DT, KNN, MLP, CNN, and ANN. The model achieved impressive accuracy with RF, reaching 99% on the CIC-MalMem-2022 dataset and 94% on the MSS Dataset. The study demonstrates the hybrid model's strengths, including heightened detection rates, scalability, and real-time deployment suitability. However, the model's performance could be further optimized for emerging security threats, and additional research is needed for feature selection refinement. Summary. Future research will concentrate on applying DL and ensemble learning approaches to expand memory and increase the efficacy of the intrusion detection model. The VANET Cloud environment may include security features like traffic analysis and ML-based classification. The suggested IDS will be assessed for durability and reliability. Scaling the technique to accommodate high-speed network traffic might be difficult owing to its complexity. Future studies will focus on high/low volume attack variations and develop methods to generate DUCAGs automatically using log data and domain expertise. The MGO will be utilized for various purposes, including healthcare, human activity identification, and false news detection. Advanced ML and DL approaches may improve recognition capabilities and resilience to complex assaults.

3. Discussion

The survey comprehensively explores various cloud security measures, focusing on encryption, access control, and network security. It highlights the importance of encryption techniques, such as AES, RSA, and Blowfish, in securing cloud data while acknowledging future challenges like the impact of quantum computing and the need for AI integration to enhance security. Access control methods, including ABAC, RBAC, and trust-based systems, are discussed for their ability to manage user privileges effectively, though scalability and performance issues remain.

Regarding network security, Intrusion Detection Systems (IDS) using ML and DL techniques show promise in identifying new threats, but challenges remain in scaling these methods for large, high-speed networks. Future work in these areas will likely focus on improving performance, scalability, and adaptability to emerging threats, including integrating advanced techniques like DL, ensemble learning, and ML-based classification. The goal is to enhance cloud security by addressing vulnerabilities across encryption, access control, and network security, ensuring the systems remain resilient to evolving cyber threats.

The paper primarily explores the technical aspects of hybrid encryption techniques, focusing on their efficiency, security, and adaptability in cloud environments. However, it overlooks the broader implications of these encryption models regarding scalability, real-time applications, and their potential role in addressing emerging cybersecurity threats like quantum computing. The paper could benefit from a discussion on integrating hybrid encryption with ML models for intrusion detection and dynamic access control, enhancing security and system performance. It would also be valuable to link these advancements to broader goals such as ensuring privacy in the Internet of Things (IoT) and promoting secure cloud-based solutions for diverse industries, contributing to a more resilient digital ecosystem. This broader perspective could further underscore hybrid encryption's importance in addressing current and future cybersecurity challenges.

4. Future Trends and Challenges

The rapid evolution of cloud computing introduces new opportunities and challenges in cloud security. While the existing strategies discussed, including encryption, access control, and network security, offer robust mechanisms to counter current threats, the emergence of novel technologies demands forward-thinking approaches. Below are some key future trends and challenges:

- Quantum Computing and Cryptographic Challenges: The advent of quantum computing threatens traditional encryption algorithms like RSA and ECC, which rely on computational complexity for security. Quantum-resistant algorithms, such as lattice-based, hash-based, and multivariate cryptosystems, are essential to ensure data confidentiality in the future.
- Integration of Artificial Intelligence (AI) and ML: AI and ML are pivotal in predicting, detecting, and mitigating cloud-based cyberattacks. Techniques like anomaly detection, behavioral analytics, and self-healing networks will enhance cloud security systems. However, adversarial attacks on ML models present a significant challenge, necessitating robust training and validation strategies.
- Homomorphic Encryption for Secure Computation: Homomorphic encryption enables secure computations on encrypted data without decryption, thus maintaining data confidentiality during processing. Despite its potential, high computational overhead and complexity hinder its practical implementation, necessitating further optimization.
- Blockchain for Cloud Security: Blockchain provides decentralized and immutable data storage, enhancing access control, secure data sharing, and audit trails in cloud environments. However, scalability, energy efficiency, and integration with existing cloud infrastructure remain significant challenges.
- Security Implications of Edge Computing: Integrating cloud computing with edge and fog architectures introduces security challenges due to distributed nodes and resource-constrained devices. Lightweight encryption techniques and localized intrusion detection systems are crucial to address these issues.
- Regulatory Compliance and Cross-Border Data Governance: Evolving global data protection regulations, such as GDPR and CCPA, create challenges in ensuring compliance while maintaining efficient cloud services. Organizations must adopt dynamic security models to adapt to these changing regulatory landscapes.
- Security in Multi-Cloud and Hybrid Environments: Adopting multi-cloud and hybrid strategies complicates the enforcement of unified security policies across diverse platforms. Solutions such as cloud access security brokers (CASBs) and unified threat management (UTM) systems will be essential for addressing these challenges.
- Data Privacy and Ethical AI: Employing AI for cloud security must balance user data privacy with ethical considerations. Transparent AI systems with explainability and bias mitigation mechanisms are essential for creating secure and trustworthy cloud ecosystems.

Future trends in cloud security highlight the need for proactive measures to address emerging threats and technological shifts. Incorporating quantum-resistant encryption, AI-driven security, decentralized models like blockchain, and robust access control mechanisms will ensure resilient and adaptive cloud environments. Continued research and collaboration among industry, academia, and policymakers are vital for building secure, scalable, and future-ready cloud systems.

5. Conclusion

Cloud computing provides enterprises with scalability, flexibility, and cost savings but also introduces security risks. Protecting sensitive data and ensuring service uptime is critical for avoiding data breaches, unwanted access, and loss. It is important to have a thorough security strategy that includes stringent access control procedures, intrusion detection systems, firewalls, encryption, and secure communication protocols. Regular audits and compliance checks are necessary to detect and rectify potential vulnerabilities to maintain robust security. Additionally, applying multi-factor authentication, RBAC, and complete identity supervision systems can effectively limit unauthorized access to cloud-based data, ensuring higher protection.

In addition to these measures, organizations should take a proactive approach to security by keeping up with security trends, offering ongoing IT staff training, and building a strong incident response approach. Modern technologies such as AI and ML can develop risk recognition and response capabilities. Furthermore, implementing data redundancy and backup solutions protects data integrity and availability.

Additionally, establishing a security-conscious culture enables staff to identify and effectively respond to potential risks. Finally, implementing layered security measures, including encryption, network security, access restrictions, constant monitoring, and vigilance, results in a safe and resilient cloud environment.

References

[1] Sunita Swain, and Rajesh Kumar Tiwari, "Cloud Security Research - A Comprehensive Survey," *International Journal of Electronics Engineering and Applications*, vol. 8, no. 2, pp. 29-39, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] PanJun Sun, "Security and Privacy Protection in Cloud Computing: Discussions and Challenges," *Journal of Network and Computer Applications*, vol. 160, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] G.R. Tsochev, and R.I. Trifonov, "Cloud Computing Security Requirements: A Review," *IOP Conference Series: Materials Science and Engineering*, vol. 1216, no. 1, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Fatemeh Khoda Paras et al., "Cloud Computing Security: A Survey of Service-Based Models," *Computers & Security*, vol. 114, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Fursan Thabit et al., "A New Lightweight Cryptographic Algorithm for Enhancing Data Security in Cloud Computing," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 91-99, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Er. Seema Rani, "Data Security Issues in Cloud Environment: A Survey," *Computer Science & Electronics Journals*, vol. 10, no. 2, pp. 141-149, 2017. [Google Scholar] [Publisher Link]

[7] Rashi Saxena, and E. Gayathri, "A Study on Vulnerable Risks in Security of Cloud Computing and Proposal of its Remedies," *Journal of Physics: Conference Series*, vol. 2040, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Albert Jeo San, and Xiola John, "Cloud Security Using Supervised Machine Learning," *International Journal of Advanced Scientific Innovation*, vol. 2, no. 4, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sajid Habib Gill et al., "Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study," *Intelligent Automation & Soft Computing*, vol. 31, no. 1, pp. 117-128, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Tanweer Alam, *Cloud Computing and its Role in the Information Technology*, IAIC Transactions on Sustainable Digital Innovation (ITSDI), 2nd ed., pp. 108-115, 2020. [Google Scholar] [Publisher Link]

[11] Syed Amma Sheik, and Amutha Prabakar Muniyandi, "Secure Authentication Schemes in Cloud Computing with Glimpse of Artificial Neural Networks: A Review," *Cyber Security and Applications*, vol. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Muhammad Manjurul Ahsan et al., "Applications and Evaluations of Bio-Inspired Approaches in Cloud Security: A Review," *IEEE Access*, vol. 8, pp. 180799-180814, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Sanaa Hammad Dhahi et al., "Using Support Vector Machine Regression to Reduce Cloud Security Risks in Developing Countries," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, pp. 1159-1166, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Poonam Kumari, and Meeta Singh "A Review: Different Challenges in Energy-Efficient Cloud Security," *IOP Conference Series: Earth and Environmental Science*, vol. 785, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Fursan Thabit et al., "Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with their Alleviating Techniques," *Journal of Information and Computational Science*, vol. 12, no. 10, 2020. [Google Scholar] [Publisher Link]

[16] Wenjuan Li et al., "Blockchain-based Trust Management in Cloud Computing Systems: A Taxonomy, Review and Future Directions," *Journal of Cloud Computing*, vol. 10, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Alabi Orobosade et al., "Cloud Application Security Using Hybrid Encryption," *Communications on Applied Electronics*, vol. 7, no. 33, pp. 25-31, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Sanjeev Kumar et al., "Cloud Security Using Hybrid Cryptography Algorithms," *2021 2nd International Conference on Intelligent Engineering and Management* (ICIEM), London, United Kingdom, pp. 599-604, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Dhirendra K.R. Shukla, Vijay K.R. Dwivedi, and Munesh C. Trivedi, "Encryption Algorithm in Cloud Computing," *Materials Today: Proceedings*, vol. 37, pp. 1869-1875, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Hua Deng et al., "Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3168-3180, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Mohan Naik Ramachandra et al., "An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard," *Big Data and Cognitive Computing*, vol. 6, no. 4, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Shihab A. Shawkat, Bilal A. Tuama, and Israa Al_Barazanchi, "Proposed System for Data Security in Distributed Computing using Triple Data Encryption Standard and Rivest-Shamir-Adleman," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 6, pp. 6496-6505, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Lin Teng et al., "A Modified Advanced Encryption Standard for Data Security," *International Journal of Network Security*, vol. 22, no. 1, pp. 112-117, 2020. [Google Scholar] [Publisher Link]

[24] J. Stanly Jayaprakash et al., "Cloud Data Encryption and Authentication Based on Enhanced Merkle Hash Tree Method," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 519-534, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] P. Chinnasamy et al., "Ciphertext-Policy Attribute-Based Encryption for Cloud Storage: Toward Data Privacy and Authentication in AI-Enabled IoT System," *Mathematics*, vol. 10, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mani Goyal, and Avinash Sharma, "A Hybrid Encryption Model to Lower the Complexity of Securing the Data in Cloud," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 6, pp. 2664-2668, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Hossein Abroshan, "A Hybrid Encryption Solution to Improve Cloud Computing Security Using Symmetric and Asymmetric Cryptography Algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] R. Senthilkumar, and B.G. Geetha, "Asymmetric Key Blum-Goldwasser Cryptography for Cloud Services Communication Security," *Journal of Internet Technology*, vol. 21, no. 4, pp. 929-939, 2020. [Google Scholar] [Publisher Link]

[29] P. Chinnasamy et al., "Efficient Data Security Using Hybrid Cryptography on Cloud Computing," *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020*, Singapore, pp. 537-547, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] Ali Kadhim Bermani, Tariq A.K. Murshedi, and Zaid A. Abod, "A Hybrid Cryptography Technique for Data Storage on Cloud Computing," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 6, pp. 1613-1624, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[31] Baris Celiktas, Ibrahim Celikbilek, and Enver Ozdemir, "A Higher-Level Security Scheme for Key Access on Cloud Computing," *IEEE Access*, vol. 9, pp. 107347-107359, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Sudakshina Mandal, Danish Ali Khan, and Sarika Jain, "Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic," *New Generation Computing*, vol. 39, no. 3, pp. 599-622, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[33] Arif Mohammad Abdul et al., "Enhancing Security of Mobile Cloud Computing by Trust-and Role-Based Access Control," *Scientific Programming*, vol. 2022, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[34] Smriti Bhatt et al., "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future," *IEEE Access*, vol. 9, pp. 107200-107223, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[35] N.N. Thilakarathne, and Dilani Wickramaaarachchi, "Improved Hierarchical Role-Based Access Control Model for Cloud Computing," *arXiv*, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[36] Shilpi Harnal, and R.K. Chauhan, "Efficient and Flexible Role-Based Access Control (EFRBAC) Mechanism for Cloud," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 7, no. 26, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[37] Idowu Mayowa Opakunle et al., "Semantic Time-Based Access Control: A Model for Patients' Data Security in a Cloud Environment," *International Journal of Scientific Engineering and Science*, vol. 7, no. 1, pp. 24-33, 2023. [Google Scholar] [Publisher Link]

[38] Mahesh B. Gunjal, and Vijay R. Sonawane, "Multi Authority Access Control Mechanism for Role-Based Access Control for Data Security in the Cloud Environment," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 2s, pp. 250-264, 2023. [Google Scholar] [Publisher Link]

[39] Balasubramanian Prabhu Kavin et al., "An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA," *Wireless Personal Communications*, vol. 115, pp. 1107-1135, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] Aakib Jawed Khan, and Shabana Mehfuz, "Fuzzy User Access Trust Model for Cloud Access Control," *Computer Systems Science & Engineering*, vol. 44, no. 1, pp. 113-128, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[41] D. Karthik, and A. Vinayagam, "Strategy Attribute Based Access Control with Improved Key Generation Method for Cloud Computing," *International Journal of Computational Intelligence in Control*, vol. 13, no. 2, 2021. [Google Scholar] [Publisher Link]

[42] Khaled Riad, "Token-Revocation Access Control to Cloud-Hosted Energy Optimization Utility for Environmental Sustainability," *Applied Sciences*, vol. 13, no. 5, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[43] Hanaa Attou et al., "Cloud-Based Intrusion Detection Approach using Machine Learning Techniques," *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 311-320, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[44] Himanshu Setia et al., "Securing the Road Ahead: Machine Learning-driven DDoS Attack Detection in VANET Cloud Environments," *Cyber Security and Applications*, vol. 2, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[45] Ramakrishnan Ramamoorthy, Ramesh Kumar Ranganathan, and Sivakumar Ramu, "Scalable Network Intrusion Detection in Cloud Environments through Parallelized Swarm-Optimized Neural Networks," *Yanbu Journal of Engineering and Science*, vol. 20, no. 2, pp. 62-70, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[46] Nishika Gulia et al., "Intrusion Detection System Using the G-ABC with Deep Neural Network in Cloud Environment," *Scientific Programming*, vol. 2023, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[47] Muder Almiani et al., "Resilient Back Propagation Neural Network Security Model for Containerized Cloud Computing," *Simulation Modelling Practice and Theory*, vol. 118, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[48] Balajee R.M., and Jayanthi Kannan M.K., "Intrusion Detection on AWS Cloud through Hybrid Deep Learning Algorithm," *Electronics*, vol. 12, no. 6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[49] Hasanien Ali Talib, Raya Basil Alothman, and Mazin S. Mohammed, "Malicious Attacks Modelling: A Prevention Approach for Ad Hoc Network Security," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 3, pp. 1856-1865, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[50] Prabhakar Krishnan et al., "OpenStackDP: A Scalable Network Security Framework for SDN-based OpenStack Cloud Infrastructure," *Journal of Cloud Computing*, vol. 12, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[51] Chunling Dong, Yu Feng, and Wenqian Shang, "A New Method of Dynamic Network Security Analysis based on Dynamic Uncertain Causality Graph," *Journal of Cloud Computing*, vol. 13, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[52] Abdulaziz Fatani et al., "Enhancing Intrusion Detection Systems for IoT and Cloud Environments Using a Growth Optimizer Algorithm and Conventional Neural Networks," *Sensors*, vol. 23, no. 9, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[53] Doddi Srilatha, and N. Thillaiarasu, "Implementation of Intrusion Detection and Prevention with Deep Learning in Cloud Computing," *Journal of Information Technology Management*, vol. 15, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[54] J. Jeya Praise, R. Joshua Samuel Raj, and J.V. Bibal Benifa, "Development of Reinforcement Learning and Pattern Matching (RLPM) based Firewall for Secured Cloud Infrastructure," *Wireless Personal Communications*, vol. 115, no. 2, pp. 993-1018, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[55] Himanshu Sharma, "Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security," *ESP Journal of Engineering & Technology Advancements (ESP-JETA)*, vol. 2, no. 2, pp. 78-91, 2022. [Google Scholar] [Publisher Link]

[56] Md Jakir Hossain et al., "ASMCC^{+}: A Secure Authentication Scheme for Mobile Cloud Computing Environment Based on Zero Trust Architecture," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 6236-6249, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[57] Rafah Kareem Mahmood et al., "Optimizing Network Security with Machine Learning and Multi-Factor Authentication for Enhanced Intrusion Detection," *Journal of Robotics and Control (JRC)*, vol. 5, no. 5, pp. 1502-1524, 2024. [Google Scholar] [Publisher Link]