Academic Journal of Nawroz University (AJNU), Vol.13, No.1, 2024

https://doi.org/10.25007/ajnu.v13n1a2010

Enhancing Security and Privacy in Distributed Cloud Environments: A Review of Protocols and Mechanisms

Renas Rajab Asaad [1,2] and Subhi R. M. Zeebaree [3]

[1] IT Dept., Technical College of Informatics, Akre University for Applied Sciences, Duhok, Iraq.
[2] College of Science, Department of Computer Science, Nawroz University, Duhok, Kurdistan Region, Iraq.
[3] Energy Eng. Dept., Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq.

ABSTRACT: As cloud computing becomes increasingly integral to data management and services, security and privacy concerns remain paramount. This article presents a comprehensive review of the current protocols and mechanisms designed to fortify security and privacy in distributed cloud environments. It synthesizes contributions from various research works, each proposing innovative solutions to address these challenges. Among these are a two-layer cryptographic algorithm that combines genetic techniques with logical-mathematical functions, enhancing encryption beyond traditional methods, and a novel symmetric-key block cipher that increases encryption complexity while maintaining flexibility. The paper also discusses machine learning applications for threat detection, the role of blockchain in trust management, and the importance of multi-cloud strategies to secure big data. Through comparative analyses, the reviewed methodologies show promising advancements in encryption, data integrity, and resource management, suggesting a robust framework for tackling the evolving landscape of cyber threats. The article underscores the need for continuous innovation and research to navigate the dynamic domain of cloud security, aiming for a future where data security and privacy are not just reactive safeguards but proactive measures embedded in the fabric of cloud computing.

Keywords: IoT, Distributed Systems, Cloud Systems, Distributed Computing, Cloud Computing

1. Introduction

In the realm of cloud computing, security and privacy are paramount concerns that have garnered extensive attention from researchers and practitioners alike. The distributed nature of cloud environments presents a complex landscape where data traverses multiple jurisdictions and systems, necessitating a robust framework to protect against a spectrum of vulnerabilities and attacks.[1-3] This literature review seeks to encapsulate the breadth of research and development efforts focused on enhancing security and privacy within these distributed systems. It delves into the innovative cryptographic algorithms that are being designed to secure data against sophisticated attacks, including genetic-based approaches that draw inspiration from the complex world of molecular biology.[2] The review further explores how machine learning algorithms are being leveraged to predict and neutralize threats, adapting to the ever-evolving patterns of cyber-attacks.[4-7] The transformative potential of blockchain technology is also examined, particularly its role in establishing a decentralized architecture for trust management in cloud systems. Moreover, the review discusses the security implications of the integration of big data and IoT with cloud computing, spotlighting the need for tailored security protocols that can handle the sheer scale and complexity of data involved. With the increasing global focus on data sovereignty and privacy, the literature review assesses the strategies for regulatory compliance and the development of privacy protocols, ensuring that cloud security mechanisms adhere to international standards such as GDPR.[8] Emerging technologies, including DNA-based encryption, are highlighted for their theoretical robustness and potential to revolutionize cloud data security. Collectively, this review synthesizes the collective insights from diverse studies, presenting a holistic view of the current state and future directions in cloud security research, thereby underlining the criticality of ongoing innovation and collaboration in securing distributed cloud environments.[26-29]

2. Background Theory

The rapid advancement of cloud computing technologies has ushered in a new era of flexible, scalable, and cost-effective computing infrastructure. However, the proliferation of cloud services and the ever-expanding digital landscape have also introduced significant security and privacy challenges. In this context, distributed cloud environments have emerged as a promising solution, enabling organizations to harness the power of multiple cloud providers while enhancing redundancy and availability [30-32].

Distributed cloud environments can be seen as a multi-cloud ecosystem, where resources and services are distributed across geographically dispersed data centers and cloud providers [33]. This approach offers several advantages, including fault tolerance, reduced latency, and improved data sovereignty. Nevertheless, it also introduces novel security and privacy concerns, necessitating the development of robust protocols and mechanisms to safeguard sensitive information and ensure the integrity and availability of cloud-based resources [34-37].

Key challenges in securing and preserving privacy in distributed cloud environments include:

1. Data Privacy: Distributed cloud environments involve data replication and distribution across multiple locations, increasing the risk of data breaches and unauthorized access. It is crucial to protect data both in transit and at rest, implement robust access controls, and employ encryption techniques to ensure the confidentiality and integrity of data [38, 39].

2. Interoperability: Different cloud providers may have varying security policies, APIs, and authentication mechanisms. Achieving seamless interoperability between these providers while maintaining security is a significant challenge. Protocols and standards need to be established to facilitate secure communication and data sharing among diverse cloud services [40, 41].

3. Resource Management: Resource allocation and management become more complex in distributed cloud environments. Ensuring that resources are utilized efficiently while maintaining security requires the development of dynamic resource allocation protocols and mechanisms that adapt to changing workloads and threat landscapes [42-44].

4. Compliance and Regulation: Compliance with data protection regulations and industry-specific standards (e.g., GDPR, HIPAA) is paramount in distributed cloud environments. Organizations must navigate a complex landscape of legal and regulatory requirements, making it essential to implement mechanisms for auditability and compliance monitoring [45,46].

5. Security Incident Response: Rapid detection and response to security incidents are crucial to minimizing the impact of breaches or vulnerabilities. Distributed cloud environments require robust incident response protocols that can quickly identify and mitigate threats across multiple cloud providers and locations [47 - 49].

To address these challenges, researchers and practitioners have been developing a wide range of protocols and mechanisms. These include federated identity management systems, secure data sharing protocols, homomorphic encryption techniques, distributed intrusion detection systems, and automated compliance monitoring tools. Additionally, emerging technologies such as blockchain and decentralized identity systems hold promise in enhancing security and privacy in distributed cloud environments.

This review will explore the existing protocols and mechanisms designed to enhance security and privacy in distributed cloud environments. It will analyze their strengths and weaknesses, identify gaps in the current state of research, and provide insights into potential future directions for securing and safeguarding privacy in this evolving landscape. Ultimately, a comprehensive understanding of these protocols and mechanisms is essential to ensure the secure and responsible adoption of distributed cloud environments in today's data-driven world.

3. Literature Review:

Key areas of focus include the development of advanced cryptographic algorithms for data security; the use of machine learning for dynamic threat detection; blockchain technology for decentralized trust management; and novel security measures for big data and IoT [46, 50]. Additionally, it covers the importance of regulatory compliance and privacy protocols and the exploration of emerging technologies such as DNA-based encryption. There's a recognized need for adaptive, multifaceted security strategies that keep pace with technological advancements and

the evolving threat landscape, emphasizing the importance of innovation and collaboration in creating resilient cloud security infrastructures [51, 52].

Thabit, Alhomdy, & Jagtap [6] introduce a two-layer cryptographic algorithm for cloud computing data security, blending genetic techniques with logical-mathematical functions. The first encryption layer applies Shannon's principles of diffusion and confusion using XOR/XNOR operations and key splitting. The second layer uses genetic coding simulations from molecular biology for further encryption. Experimental results show that their algorithm outperforms traditional methods in cipher strength, size, and execution time, and exhibits robust defense against brute force and cipher-text-only attacks. The research concludes by affirming the algorithm's effectiveness in fulfilling the CIA triad of data security.

Thabit, Alhomdy, Al-Ahdal, et al. [7] introduce the New Lightweight Cryptographic Algorithm (NLCA), a symmetric-key block cipher tailored for cloud computing security. NLCA utilizes a 128-bit block and key size and is structured upon Feistel and SPN architectures to optimize encryption complexity. It implements Shannon's diffusion and confusion principles via operations like XOR, XNOR, shifting, and swapping. NLCA offers adjustable key lengths and rounds, enhancing flexibility, performance, and security. The paper details the NLCA's mechanics, showcasing its superiority in execution time and security through tests, compared to established cloud computing encryption methods.

Dr. V. Suma [8] presents a new algorithm to improve information retrieval in cloud systems by merging deep learning with fuzzy logic, addressing challenges like large datasets and natural language processing. The proposed hybrid deep fuzzy hashing algorithm aims to enhance accuracy and efficiency, with detailed mathematical formulations for efficient database querying. Validation on CloudSim with the KDD Cup 2004 Database shows this algorithm outperforming existing models on specificity, sensitivity, and F-measure. The results underscore its superior retrieval performance with a 97.6% efficiency rate. The conclusion highlights the hybrid method's advantages and suggests future research for further refinement, marking a significant step in data management and retrieval in cloud environments.

Zulifqar et al. [9] delves into the security issues inherent in cloud computing, exploring the evolution of these concerns alongside the development of the technology itself. It offers an initial overview of cloud computing's advantages and its synergy with mobile technology, followed by a historical perspective on the rise of related security challenges. The paper reviews various strategies for tackling data security issues and details the specific Challenges encompassing data integrity, availability, vendor lock-in, and compliance with regulatory norms. The text provides a classification of the many security requirements for cloud computing, which encompass identity, information, network, software, and infrastructure. Additionally, it explores sophisticated encryption and alternative approaches to address these difficulties. The paper emphasizes the necessity of addressing security concerns in order to promote and achieve widespread adoption and success of cloud computing, notwithstanding its advantages such as cost-effectiveness and enhanced mobility.

Butt et al. [10] Investigates the application of machine learning algorithms to enhance security in cloud computing. The paper examines the application of several machine learning techniques, including supervised, unsupervised, semi-supervised, and reinforcement learning, and their importance in addressing security vulnerabilities. The article provides a comprehensive examination of the utilization of several techniques, such as neural networks, K-NN, Naive Bayes, and SVM, to tackle cloud security issues including intrusion detection and malware identification. This article examines the benefits and drawbacks of several machine learning techniques within the framework of cloud security. The authors conclude by suggesting potential areas for future research to bolster the security of cloud computing platforms.

Radain et al. [11] Explores the susceptibility of cloud computing infrastructure to DDoS attacks, providing a comprehensive analysis of the attack techniques and the corresponding defensive measures. The study offers a comprehensive analysis of cloud computing, the intricacies of DDoS attacks, and their exploitation of cloud vulnerabilities. Defense strategies are categorized into three main components: prevention, detection, and mitigation. Each component has its own set of approaches, such as ingress/egress filtering for prevention and anomaly detection for detection. It discusses mitigation methods including firewalls and resource scaling. The authors point out the limitations of current defenses, especially against attacks with legitimate IP addresses or new attack vectors. The

paper calls for further research to develop more robust defense strategies and to evaluate existing ones against a wider array of attacks.

Wang et al. [12] investigates the impact of business analytics affordances (BAAs) on the management of cloud computing data security (MCCDS) through a research model incorporating decision-making affordances, rationality, and MCCDS effectiveness. Grounded in the information value chain and IT affordances theories, the study analyzes data from 316 enterprises using a structural equation model. The results indicate that BAAs directly foster better decision-making, which improves rationality and MCCDS effectiveness. Furthermore, the study finds that a data-driven culture and IT-business process integration positively influence the relationship between BAAs and decision-making affordances, highlighting their importance in enhancing MCCDS.

Universitas Bina Nusantara. School of Information Systems et al [13] explores the intersection of big data with cloud computing and the resulting security and privacy concerns. It emphasizes big data's critical role in business and government for processing and storing large volumes of complex data. The integration with cloud computing, while beneficial for computational power and storage, introduces significant security challenges. The paper identifies key issues like data breaches, misconfiguration, and inadequate access controls that can lead to severe consequences such as loss of trust and reputational damage. Researchers propose solutions like multilevel encryption and sensitive data categorization to mitigate these risks. However, the paper concludes that given the dynamic nature of security threats, ongoing advancements in security measures are essential to maintain data confidentiality, reliability, and integrity.

Li et al. [14] survey evaluates blockchain as a solution for trust management in cloud computing, addressing the limitations of traditional centralized systems. The paper highlights blockchain's decentralization as a way to reduce overheads, prevent network congestion, and eliminate single points of failure. It reviews blockchain-based trust techniques, explores blockchain applications in cloud computing variations like P2P, IoT, and edge computing, and proposes a taxonomy of blockchain schemes. A novel hybrid cloud-edge framework and a double-blockchain transaction model are presented for enhanced trust management. The authors also identify research gaps and propose future research directions, focusing on the development of trust frameworks, evaluation methods, and security robustness, underscoring blockchain's potential to increase transparency and traceability in cloud transactions.

Farsi et al. [15] provides a structured overview of data security threats in cloud computing, analyzing different cloud and service models. It outlines key challenges such as threats from insiders and outsiders, data integrity and availability issues, confidentiality concerns, trust complexities, and privacy issues. The significance of data classification and the impact of data location on security are also considered. To address these challenges, the paper reviews solutions like multi-cloud strategies, including the DepSky and MCDB models, and discusses additional measures like third-party monitoring and encryption. It emphasizes the need for robust security solutions to protect cloud-stored data.

Yang et al. [16] survey critically examines data security and privacy in cloud storage systems. It begins with a foundational overview of cloud storage, covering its definitions, classifications, architecture, and applications. The paper then focuses on the challenges and essential requirements for data security and privacy protection. It highlights various data encryption technologies, such as Identity-Based Encryption (IBE), Attribute-Based Encryption (ABE), and Homomorphic Encryption (HE), detailing their benefits, methodologies, and impact on cloud security. The concept of searchable encryption is also discussed, which enables secure keyword searches within encrypted files in the cloud, considering techniques like Searchable Symmetric Encryption (SSE) and Public Key Encryption with Keyword Search (PEKS). The paper acknowledges complex issues like granular data access control, malicious providers, side-channel attacks, and guaranteed data deletion. It wraps up by identifying open research areas, underscoring the ongoing need for innovation in cloud data security.

Wilczyński & Kołodziej [17] introduces a security-focused task scheduling model for cloud computing that incorporates blockchain technology. The model includes a secure cloud scheduler built on blockchain architecture and a novel 'proof-of-schedule' consensus algorithm, which replaces the traditional 'proof-of-work'. It also integrates Stackelberg games to optimize the approval process of the schedules. The proposed Blockchain Scheduler is shown to improve scheduling efficiency, achieving better makespan compared to other scheduling approaches. The model's

performance is validated through simulations using BCSchedCloudSim, a new cloud simulation tool, and is compared with other prevalent cloud schedulers.

Ali et al. [18] presents a thorough investigation of Multi-Access Edge Computing (MEC) and its security concerns, recognizing that while MEC extends cloud capabilities to the network edge, enhancing user experience, it also introduces complex security threats due to the dispersed nature of data across multiple nodes. The paper delves into MEC's architecture, outlining its susceptibility to various threats and proposing a multi-layered security control framework. It highlights challenges in key areas like access control, authentication, data confidentiality, integrity, and privacy, and calls for re-evaluation of traditional security systems in the context of MEC's unique requirements. Addressing the necessity for advanced solutions such as software-defined segmentation and cloud-native mechanisms, the paper points to future research directions including security orchestration, MEC services security, and trust management, emphasizing the need for scalable and reliable security solutions suitable for the resource constraints inherent in MEC nodes. This comprehensive overview underlines the importance of continued innovation to protect against the sophisticated security threats within MEC environments.

Tawalbeh & Saldamli [19] highlights the significance of big data across various sectors and the vital role of cloud infrastructure in its management. They propose leveraging Peer-to-Peer Cloud Systems (P2PCS) for enhanced big data storage and processing and address security and privacy concerns pertinent to cloud and mobile cloud systems. The authors evaluate current cloud architectures and suggest a novel hybrid mobile cloud model, rooted in the concept of cloudlets, which they demonstrate with a healthcare system case study. Simulations using the Mobile Cloud Computing Simulator (MCCSIM) indicate that their hybrid model outperforms traditional cloud setups in energy efficiency and latency. Additionally, they discuss security and privacy measures, advocating for advanced cryptographic techniques to safeguard big data within cloud spaces. In conclusion, they affirm the suitability of cloud and mobile cloud environments for big data analytics while calling for more robust security solutions to combat emerging threats.

Moorthy et al. [20] explore the security landscape of Software Defined Networking (SDN) within mobile cloud computing, highlighting the importance of the technology for scalability, mobility, and cost reduction. The paper presents the SDN-enabled mobile cloud architecture, describing its various planes and interfaces. It identifies numerous security threats at different layers, including DDoS attacks and spoofing, and suggests appropriate countermeasures like intrusion detection systems, encryption, and firewalls to mitigate these risks. The authors emphasize the need for security implementations across all layers of SDN and conclude by pointing out open research challenges, advocating for the development of more comprehensive security solutions for these networks.

Abdulsalam & Hedabou [21] explores the security and privacy concerns associated with cloud computing, specifically in the context of mobile cloud computing architectures and the incorporation of Software Defined Networking (SDN). The security threats inside the SDN framework are analysed and different solutions, including prevention, detection, and mitigation, are examined to effectively address these threats. The study emphasises the significance of implementing layered security inside the SDN architecture and acknowledges the constraints of existing defenses in countering sophisticated attacks that utilize genuine IP addresses or novel signatures. The authors propose the establishment of novel categorizations for DDoS attacks and a more thorough evaluation of defensive measures. They emphasize the necessity of implementing adaptive security solutions that can react to evolving threats, while still preserving the fundamental benefits of flexibility and scalability offered by the cloud. The purpose of the call is to advocate for more research in order to strengthen the effectiveness of security solutions in cloud environments.

Ding et al. [22] this paper proposes a method to enhance resource management in heterogeneous networks, with a specific focus on IoT. The technique aims to improve upon the error margins and security vulnerabilities commonly found in typical cloud computing transmissions. The method improves the precision and safety of resource management, as demonstrated by simulations indicating a 20% decrease in calculation mistakes and a security performance above 90%. The study explores the topics of data encryption and IoT data gathering, establishing the basis for an algorithm that incorporates secure transmission technologies into resource management. The results indicate that the algorithm is a feasible method for enhancing cloud data security management in IoT environments.

Kumar Tyagi et al. [23] survey delves into security and privacy concerns across multiple computing platforms, including Big Data, Cloud Computing, IoT, IoE, Fog Computing, Pervasive Computing, and Distributed Computing. The paper underscores the intertwined nature of security and privacy and their significance in contemporary computing. It discusses challenges such as Big Data's vulnerability to manipulation, Cloud Computing's data confidentiality and API security, and IoT's need for robust access control and privacy measures. IoE's data handling, Fog Computing's role in analytics, Pervasive Computing's scalability and privacy, and Distributed Computing's security integration are also examined. The paper suggests that future research should aim to develop secure, trustworthy solutions, emphasizing that security and privacy should be advanced in tandem to protect user data and sustain confidence in these developing technologies.

Martin Otieno [24] addresses the significant challenges of data privacy in the rapidly expanding field of cloud computing. It conducts a comparative analysis of various methods aimed at protecting data privacy in the cloud. The paper outlines the considerable concerns with private data security due to the extensive storage and transfer of information globally. Although numerous techniques and protocols have been proposed, maintaining data privacy continues to be an elusive goal. Otieno categorizes and examines different defense strategies such as prevention, detection, and mitigation, assessing their efficacy and constraints. The paper emphasizes the necessity for novel classifications of attacks like DDoS and a reevaluation of existing defense mechanisms to cover a broader spectrum of threats. The conclusion stresses the importance of ongoing research and innovation in developing sophisticated security solutions to ensure robust data privacy protection in cloud environments.

Namasudra et al. [25] present a novel DNA-based encryption method aimed at bolstering the security of big data in cloud computing. This technique utilizes DNA computing concepts, user attributes, and the Media Access Control address to generate a robust 1024-bit secret key. By encoding ASCII values and applying DNA base complementary rules, the scheme enhances security, proving resilient against a range of cyber threats, including malware, side-channel attacks, phishing, insider threats, and DoS attacks. Comparative experimental and theoretical analysis indicates that this DNA-based encryption is more efficient than existing methods. The paper details the encryption's background, methodology, and a performance comparison, suggesting future work on mathematical security proofs and improved authentication for cloud services.

4. Discussion and Comparison

4.1 Comparison Based on Category:

The research projects in this part are classified according to various domains such as cloud security, network security, data privacy, and algorithm development. The document provides a comprehensive enumeration of the algorithms or analytical tools employed in each study, as well as the resulting applications or service outputs. One study in cloud security employs evolutionary approaches and logical-mathematical functions to create an innovative data security algorithm.

Table 1: Comparison Based on Category

#	Ref.	Research Category	Algorithm/Analyzing Tools	Application/Service Output
1	[11]	Cloud Security	Not specified	Defense strategies against DDoS
2	[20]	Network Security	Not specified	Countermeasures for data communication attacks
3	[21]	Cloud Security	Not specified	Framework for cloud security challenges
4	[23]	Computing Platforms Security	Not specified	Security and privacy issues across platforms
5	[24]	Data Privacy	Not specified	Data privacy enhancement techniques
6	[6]	Algorithm Development	Genetics techniques, logical-mathematical functions	A new data security algorithm

7	[7]	Cryptography	New Lightweight Cryptographic Algorithm (NLCA)	A cryptographic algorithm for cloud data security
8	[8]	Information Retrieval	Hybrid Deep Fuzzy Hashing Algorithm	Improved information retrieval system
9	[9]	Cloud Security	Not specified	Data security challenges and solutions
10	[10]	Machine Learning	Various ML algorithms	ML applications for cloud security
11	[12]	Business Analytics	Not specified	Impact of business analytics on data security management
12	[13]	Big Data Security	Not specified	Security challenges in big data
13	[14]	Blockchain	Blockchain technology	Trust management using blockchain
14	[15]	Cloud Security	Not specified	Taxonomy of security threats
15	[16]	Cloud Storage Security	Various encryption technologies	Methods for data security and privacy protection
16	[17]	Cloud Computing	Blockchain technology	Security-aware task scheduling model
17	[18]	Edge Computing Security	Not specified	Review of security and privacy in edge computing
18	[19]	Big Data Security	Not specified	Big data security considerations
19	[22]	IoT Security	Not specified	Algorithms for secure information transmission
20	[25]	Data Security	DNA-based techniques	DNA-based data security concept

4.2 Comparison Based on Results:

This section specifically addresses the geographical areas that were the subject of the investigations, as well as the specific objects or tools that were utilized. The text showcases the outcomes derived from each investigation, including evaluations, examinations, and suggested models or algorithms in diverse security-oriented domains.

Table 2: Comparison Based on Results

#	Ref.	Study Target Region	Object Tool	Obtained Results
1	[11]	Not specified	Cloud computing environments	Reviewed strategies to mitigate DDoS attacks in cloud computing
2	[20]	Not specified	SDN-based mobile cloud systems	Analyzed security threats and countermeasures in SDN-based mobile clouds
3	[21]	Not specified	Cloud computing	Provided a technical review of security and privacy issues in cloud computing
4	[23]	Not specified	Various computing platforms	Surveyed security and privacy issues across various computing platforms
5	[24]	Not specified	Cloud computing	Evaluated data privacy enhancement techniques and protocols for cloud computing
6	[6]	Not specified	Cloud computing	Proposed a genetics techniques-based algorithm for cloud data security
7	[7]	Not specified	Cloud computing	Introduced a new lightweight cryptographic algorithm for cloud data security

8	[8]	Not specified	Distributed cloud systems	Developed a hybrid deep fuzzy hashing algorithm for information retrieval
9	[9]	Not specified	Cloud computing	Reviewed data security challenges and solutions in cloud computing
10	[10]	Not specified	Cloud computing	Analyzed ML algorithms for enhancing cloud computing security
11	[12]	Not specified	Cloud computing enterprises	Studied the effect of business analytics on cloud computing data security management
12	[13]	Not specified	Cloud environments	Discussed the security and privacy challenges of big data in cloud computing
13	[14]	Not specified	Cloud computing systems	Reviewed blockchain-based trust management systems for cloud computing
14	[15]	Not specified	Cloud computing	Provided a taxonomy of data security threats in cloud computing
15	[16]	Not specified	Cloud storage systems	Surveyed the methods for data security and privacy protection in cloud storage
16	[17]	Not specified	Cloud computing	Modeled security-aware task scheduling in cloud computing using blockchain
17	[18]	Not specified	Multi-access edge computing	Reviewed data security and privacy in multi-access edge computing
18	[19]	Not specified	Cloud and mobile cloud systems	Reevaluated big data security and privacy concerns in cloud systems
19	[22]	Not specified	IoT and cloud computing	Proposed algorithms for secure information transmission in IoT and cloud computing
20	[25]	Not specified	Not specified	Explored the concept of DNA-based data security for cloud computing

4.3 Comparison Based on Impacts:

The text examines the problems and security concerns that are discussed in each study and the consequences they have on cloud settings. This section offers an analysis of how each research effort contributes to improving the ability to withstand and recover from challenges, ensuring protection against threats, and maintaining confidentiality in cloud infrastructure and associated computing environments.

Table 3: Comparison Based on Impacts

#	Ref.	Challenges	Security Issue	Impact on Cloud
1	[11]	DDoS attack evolution and defense mechanisms	DDoS attacks	Enhances DDoS resilience in cloud infrastructure
2	[20]	Security and privacy in mobile and SDN environments	Data communication attacks	Improves data communication security in mobile clouds
3	[21]	Comprehensive cloud security and privacy threats	Various cloud computing vulnerabilities	Provides a framework to address cloud security challenges
4	[23]	Security and privacy across diverse computing platforms	General security and privacy in computing	Influences security approaches in multi-platform cloud services

5	[24]	Data privacy maintenance in cloud environments	Data privacy and protection protocols	Guides the development of privacy-enhancing technologies
6	[6]	Developing robust genetic-based encryption methods	Genetic algorithm-based security	Contributes to stronger data encryption in the cloud
7	[7]	Cryptographic efficiency and security	Lightweight cryptography	Promotes the use of lightweight cryptography for cloud services
8	[8]	Efficient information retrieval in distributed cloud systems	Data retrieval and indexing	Improves the efficiency and accuracy of cloud data retrieval
9	[9]	Addressing various cloud data security issues	Data security challenges	Aids in creating a secure cloud data management ecosystem
10	[10]	Utilizing machine learning for cloud security enhancements	Security improvements via machine learning	Influences the incorporation of ML in cloud security solutions
11	[12]	Integrating business analytics for improved cloud security management	Data security management	Impacts data security management with analytics insights
12	[13]	Security and privacy challenges in big data analytics	Big data security and privacy	Shapes the security strategies for big data in the cloud
13	[14]	Trust management in cloud computing environments	Trust management and blockchain	Potentially revolutionizes cloud security with blockchain
14	[15]	Developing a comprehensive threat categorization	Threat taxonomy in cloud computing	Informs the development of threat intelligence platforms
15	[16]	Ensuring data security and privacy in cloud storage	Cloud storage security and privacy	Affects the design of secure cloud storage solutions
16	[17]	Integrating task scheduling with security considerations	Task scheduling and security in cloud	Enhances the reliability of cloud computing services
17	[18]	Security in edge computing scenarios and its integration with cloud	Edge computing security and privacy	Augments cloud-edge computing architectures
18	[19]	Reevaluation of big data security in cloud and mobile cloud systems	Big data security and privacy	Impacts the approach to big data privacy and security
19	[22]	Secure transmission of information between IoT devices and cloud systems	IoT security and data transmission	Enhances security in IoT-cloud integrated systems
20	[25]	Developing robust encryption methods using DNA-based techniques	DNA-based data security	Introduces innovative encryption techniques in cloud data security

4.4 Comparison of Advantages and Disadvantages Based on Techniques:

This section provides a comprehensive overview of the study categories, algorithms, and outputs, as well as the respective advantages and disadvantages associated with each technique. It encompasses debates on DDoS defense

tactics, security protocols for SDN, and several security frameworks, each with their respective advantages and constraints.

Table 4: Comparison of Advantages and Disadvantages Based on Techniques

#	Ref.	Research Category	Algorithm/Analyzing Tools	Application/Service Output
1	[11]	DDoS defense strategies	May reduce the impact of DDoS attacks	Constant evolution of DDoS tactics can outpace defenses
2	[20]	Security protocols for SDN	Designed for dynamic SDN environments	May not cover all emerging threats
3	[21]	Various security frameworks	Broad overview of security approaches	May lack in-depth analysis for specific frameworks
4	[23]	Security surveys across platforms	Offers a wide perspective	Might not provide deep technical solutions
5	[24]	Data privacy techniques	Enhance user privacy	Can be complex to implement
6	[6]	Genetic algorithm-based security	Innovative approach	Unproven in diverse real-world scenarios
7	[7]	Lightweight cryptography	Efficient and fast	May offer less security than heavier algorithms
8	[8]	Fuzzy hashing and deep learning	Improves retrieval accuracy	Complexity in implementation
9	[9]	Data security solutions	Comprehensive review	May not include the latest solutions
10	[10]	Machine learning algorithms	Can improve over time with data	Requires large datasets and resources
11	[12]	Business analytics tools	Data-driven security insights	Depends heavily on data quality
12	[13]	Big data security strategies	Handles large scale data	Complexity and computational demand
13	[14]	Blockchain for trust management	Decentralized and transparent	Scalability and speed issues
14	[15]	Threat taxonomy development	Helps in identifying and categorizing threats	Taxonomy may become quickly outdated
15	[16]	Encryption and privacy protection protocols	Protects data at rest	Can complicate data retrieval and usage
16	[17]	Blockchain for task scheduling	Adds a layer of security	Overhead and complexity of blockchain
17	[18]	Security protocols for edge computing	Low latency security solutions	May not be as robust as centralized solutions
18	[19]	Big data security frameworks	Tailored to big data challenges	Adapting to rapidly evolving big data landscape is tough
19	[22]	Secure transmission algorithms	Aims to protect data in transit	IoT's diverse ecosystem makes standardization difficult

20	[25]	DNA-based data security techniques	High theoretical security level	Still largely theoretical and not practical for current use

In its entirety, the study presents a comprehensive and structured synopsis of current research concerning the security of cloud computing, data privacy concerns, and associated areas. As a result, it imparts invaluable knowledge regarding the present condition of research, the approaches utilized, and the consequences and ramifications of such investigations within the realm of computing security.

5. Recommendations:

The recommendations for enhancing cloud security include promoting collaborative research across sectors, establishing industry-wide security standards, and educating users on security best practices. There's an emphasis on designing resilient cloud systems that can withstand attacks with minimal disruption. Ethical considerations around user data in security research are highlighted to maintain trust in cloud computing. Lastly, future cloud security solutions should be sustainable, prioritizing energy efficiency and reduced environmental impact.

6. Conclusion and Future Work:

6.1 Conclusion

This review has consolidated a diverse range of cutting-edge research dedicated to improving the security and privacy of distributed cloud environments. It has highlighted the advancements in cryptographic algorithms, such as the two-layer approach that integrates genetic techniques and the New Lightweight Cryptographic Algorithm (NLCA) for better cloud data security. Machine learning algorithms have been recognized for their potential to revolutionize threat detection and response. Blockchain technology emerges as a strong candidate for establishing decentralized trust and enhancing identity management. The study has also acknowledged the role of big data and IoT in shaping the future of cloud security, noting the critical need for solutions tailored to their unique challenges. While progress has been made, the article emphasizes the ongoing necessity for innovation, particularly in areas such as regulatory compliance and the creation of new data privacy protocols. The synthesis of these findings points towards a multi-faceted approach to cloud security, where collaboration, standardization, and education play key roles. As the cloud computing landscape evolves, so too must the strategies to protect it, ensuring that security and privacy measures are as dynamic and resilient as the services they aim to safeguard.

6.2 Future Work:

- Advanced Threat Detection: Creating complex machine learning algorithms to predict and counteract advanced threats, such as zero-day assaults [46].
- Exploring the feasibility of incorporating blockchain technology to improve the level of security in cloud computing, namely in the areas of managing identities and storing data in a decentralized manner.
- Genetic Algorithms and Biologically Inspired Security: Exploring biologically inspired security measures for potential innovations in encryption and data integrity.
- IoT and Edge Security: Addressing the unique security needs of the growing number of IoT devices and the rise of edge computing, with protocols suited for distributed networks.
- Data Privacy Protocols: Creating new protocols to protect user privacy effectively without hindering service performance.
- Regulatory Compliance: Developing automated tools to ensure cloud security solutions comply with international data protection regulations like GDPR.

Secure Multi-Cloud and Hybrid Environments: Formulating strategies to safeguard data and applications spread across various cloud services and hybrid systems.

References

1. Jubair, M. A., Mostafa, S. A., Zebari, D. A. (2022). A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs. *IEEE Access*, *10*, 124792-124804.
2. H. Shukur, S. Zeebaree, R. Zebari, D. Zeebaree, O. Ahmed, and A. Salih, "Cloud Computing Virtualization of Resources Allocation for Distributed Systems," Journal of Applied Science and Technology Trends, vol. 1, no. 3, pp. 98–105, Jun. 2020, doi: 10.38094/jastt1331.
3. Mohammed Mohammed Sadeeq, Nasiba M. Abdulkareem, Subhi R. M. Zeebaree, Dindar Mikaeel Ahmed, Ahmed Saifullah Sami, and Rizgar R. Zebari, "IoT and Cloud Computing Issues, Challenges and Opportunities: A Review," 2021, doi: 10.48161/issn.2709-8206.
4. Mohammed, M. A., Lakhan, A., et al. (2024). Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Engineering Applications of Artificial Intelligence*, *129*, 107612.
5. Alsandi, N. S. A., Zebari, D. A., Al-Zebari, A., Ahmed, F. Y., Mohammed, M. A., Albahar, M., & Albahr, A. A. (2023). A Multi-Stream Scrambling and DNA Encoding Method Based Image Encryption. *Computer Systems Science & Engineering*, *47*(2).
6. F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," International Journal of Intelligent Networks, vol. 2, pp. 18–33, Jan. 2021, doi: 10.1016/j.ijin.2021.03.001.
7. F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," Global Transitions Proceedings, vol. 2, no. 1, pp. 91–99, Jun. 2021, doi: 10.1016/j.gltp.2021.01.013.
8. Dr. V. Suma, "A Novel Information retrieval system for distributed cloud using Hybrid Deep Fuzzy Hashing Algorithm," Journal of Information Technology and Digital World, vol. 02, no. 03, pp. 151–160, Aug. 2020, doi: 10.36548/jitdw.2020.3.003.
9. Zulifqar, S. Anayat, and I. Kharal, "A Review of Data Security Challenges and their Solutions in Cloud Computing," International Journal of Information Engineering and Electronic Business, vol. 13, no. 3, pp. 30–38, Jun. 2021, doi: 10.5815/ijieeb.2021.03.04.
10. U. A. Butt et al., "A review of machine learning algorithms for cloud computing security," Electronics (Switzerland), vol. 9, no. 9. MDPI AG, pp. 1–25, Sep. 01, 2020. doi: 10.3390/electronics9091379.
11. D. Radain, S. Almalki, H. Alsaadi, and S. Salama, "A review on defense mechanisms against distributed denial of service (DDoS) attacks on cloud computing," in 2021 International Conference of Women in Data Science at Taif University, WiDSTaif 2021, Institute of Electrical and Electronics Engineers Inc., Mar. 2021. doi: 10.1109/WIDSTAIF52235.2021.9430220.
12. Z. Wang, N. Wang, X. Su, and S. Ge, "An empirical study on business analytics affordances enhancing the management of cloud computing data security," Int J Inf Manage, vol. 50, pp. 387–394, Feb. 2020, doi: 10.1016/j.ijinfomgt.2019.09.002.
13. Universitas Bina Nusantara. School of Information Systems, Institute of Electrical and Electronics Engineers. Indonesia Section, and Institute of Electrical and Electronics Engineers, ICIMTech 2020 : proceedings of 2020 International Conference on Information Management and Technology (ICIMTech) : 13-14 August 2020, Indonesia.
14. W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions," Journal of Cloud Computing, vol. 10, no. 1, Dec. 2021, doi: 10.1186/s13677-021-00247-5.
15. M. Farsi, M. Ali, R. A. Shah, A. A. Wagan, and R. Kharabsheh, "Cloud computing and data security threats taxonomy: A review," Journal of Intelligent and Fuzzy Systems, vol. 38, no. 3, pp. 2529–2537, 2020, doi: 10.3233/JIFS-179539.
16. P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," IEEE Access, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 131723–131740, 2020. doi: 10.1109/ACCESS.2020.3009876.
17. Wilczyński and J. Kołodziej, "Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain technology," Simul Model Pract Theory, vol. 99, Feb. 2020, doi: 10.1016/j.simpat.2019.102038.
18. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," IEEE Access, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 18706–18721, 2021. doi: 10.1109/ACCESS.2021.3053233.
19. L. A. Tawalbeh and G. Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloud systems," Journal of King Saud University - Computer and Information Sciences, vol. 33, no. 7, pp. 810–819, Sep. 2021, doi: 10.1016/j.jksuci.2019.05.007.
20. V. Moorthy, R. Venkataraman, and T. Rama Rao, "Security and privacy attacks during data communication in Software Defined Mobile Clouds," Comput Commun, vol. 153, pp. 515–526, Mar. 2020, doi: 10.1016/j.comcom.2020.02.030.
21. Y. S. Abdulsalam and M. Hedabou, "Security and privacy in cloud computing: Technical review," Future Internet, vol. 14, no. 1. MDPI, Jan. 01, 2022. doi: 10.3390/fi14010011.
22. L. Ding, Z. Wang, X. Wang, and D. Wu, "Security information transmission algorithms for IoT based on cloud computing," Comput Commun, vol. 155, pp. 32–39, Apr. 2020, doi: 10.1016/j.comcom.2020.03.010.
23. Kumar Tyagi, M. Manoj Nair, S. Niladhuri, and A. Abraham, "Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead", [Online]. Available: www.mirlabs.net/jias/index.html
24. MARTIN OTIENO, "Techniques and protocols for enhancing data privacy in cloud computing: A review," World Journal of Advanced Engineering Technology and Sciences, vol. 8, no. 1, pp. 391–404, Feb. 2023, doi: 10.30574/wjaets.2023.8.1.0064.
25. S. Namasudra, D. Devi, S. Kadry, R. Sundarasekar, and A. Shanthini, "Towards DNA based data security in the cloud computing environment," Comput Commun, vol. 151, pp. 539–547, Feb. 2020, doi: 10.1016/j.comcom.2019.12.041.
26. Mohammed, M. A., Lakhan, A., Abdulkareem, K. H., etal. (2023). Homomorphic federated learning schemes enabled pedestrian and vehicle detection system. *Internet of Things*, *23*, 100903.
27. Abdullah, P. Y., Zeebaree, S. R., Jacksi, K., & Zeabri, R. R. (2020). An hrm system for small and medium enterprises (sme) s based on cloud computing technology. International Journal of Research-GRANTHAALAYAH, 8(8), 56-64.
28. Abdullah, P. Y., Zeebaree, S. R., Shukur, H. M., & Jacksi, K. (2020). HRM system using cloud computing for Small and Medium Enterprises (SMEs). Technology Reports of Kansai University, 62(04), 04.
29. Zeebaree, S. R., Zebari, R. R., Jacksi, K., & Hasan, D. A. (2019). Security approaches for integrated enterprise systems performance: A Review. Int. J. Sci. Technol. Res, 8(12), 2485-2489.
30. Rashid, Z. N., Zebari, S. R., Sharif, K. H., & Jacksi, K. (2018, October). Distributed cloud computing and distributed parallel computing: A review. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 167-172). IEEE.

31. Jader, O. H., Zeebaree, S. R., Zebari, R. R., Shukur, H. M., Rashid, Z. N., Sadeeq, M. A., & Alkhayyat, A. (2021, September). Ultra-Dense Request Impact on Cluster-Based Web Server Performance. In 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA) (pp. 252-257). IEEE.
32. Sadeeq, M. A., & Zeebaree, S. R. (2021, August). Design and analysis of intelligent energy management system based on multi-agent and distributed iot: Dpu case study. In 2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM) (pp. 48-53). IEEE.
33. Rashid, Z. N., Zeebaree, S. R., Sadeeq, M. A., Zebari, R. R., Shukur, H. M., & Alkhayyat, A. (2021, October). Cloud-based Parallel Computing System Via Single-Client Multi-Hash Single-Server Multi-Thread. In 2021 International Conference on Advance of Sustainable Engineering and its Application (ICASEA) (pp. 59-64). IEEE.
34. Sadeeq, M. A., & Zeebaree, S. R. (2023). Design and implementation of an energy management system based on distributed IoT. Computers and Electrical Engineering, 109, 108775.
35. Sami, T. M. G., Zeebaree, S. R., & Ahmed, S. H. (2024). A Novel Multi-Level Hashing Algorithm to Enhance Internet of Things Devices' and Networks' Security. International Journal of Intelligent Systems and Applications in Engineering, 12(1s), 676-696.
36. Abdullah, P. Y., Zeebaree, S. R., Shukur, H. M., & Jacksi, K. (2020). HRM system using cloud computing for Small and Medium Enterprises (SMEs). *Technology Reports of Kansai University*, *62*(04), 04.
37. Zeebaree, S. R., Zebari, R. R., Jacksi, K., & Hasan, D. A. (2019). Security approaches for integrated enterprise systems performance: A Review. *Int. J. Sci. Technol. Res*, *8*(12), 2485-2489.
38. Zeebaree, S. R., Sallow, A. B., Hussan, B. K., & Ali, S. M. (2019, April). Design and simulation of high-speed parallel/sequential simplified DES code breaking based on FPGA. In *2019 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 76-81). IEEE.
39. Mohammed, M. A., Lakhan, A., Abdulkareem, K. H., etal. (2023). Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks. *Internet of Things*, *22*, 100815.
40. Zebari, I. M., Zeebaree, S. R., & Yasin, H. M. (2019, April). Real time video streaming from multi-source using client-server for video distribution. In *2019 4th Scientific International Conference Najaf (SICN)* (pp. 109-114). IEEE.
41. Mohammed, S. M., Jacksi, K., & Zeebaree, S. (2021). A state-of-the-art survey on semantic similarity for document clustering using GloVe and density-based algorithms. *Indonesian Journal of Electrical Engineering and Computer Science*, *22*(1), 552-562.
42. Shukur, H., Zeebaree, S., Zebari, R., Ahmed, O., Haji, L., & Abdulqader, D. (2020). Cache coherence protocols in distributed systems. *Journal of Applied Science and Technology Trends*, *1*(3), 92-97.
43. Khalid, Z. M., & Zeebaree, S. R. (2021). Big data analysis for data visualization: A review. *International Journal of Science and Business*, *5*(2), 64-75.
44. Sadeeq, M. A., & Zeebaree, S. R. (2023). Design and implementation of an energy management system based on distributed IoT. *Computers and Electrical Engineering*, *109*, 108775.
45. Sami, T. M. G., Zeebaree, S. R., & Ahmed, S. H. (2023). A Comprehensive Review of Hashing Algorithm Optimization for IoT Devices. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(6s), 205-231.
46. Lakhan, A., Mohammed, M. A., Zebari, et al. (2024). Augmented IoT Cooperative Vehicular Fraework Based on Distributed Deep Blockchain Networks. *IEEE Internet of Things Journal*.
47. Zangana, H. M., & Zeebaree, S. R. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, *5*(1), 1-20.
48. Ageed, Z. S., & Zeebaree, S. R. (2024). Distributed Systems Meet Cloud Computing: A Review of Convergence and Integration. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(11s), 469-490.
49. ABDULQADER, D. M., ZEEBAREE, S. R., ZEBARI, R. R., SALEH, S. A., RASHID, Z. N., & SADEEQ, M. A. (2023). Single-threading Based Distributed-multiprocessor-machines Affecting by Distributed-parallel-computing Technology. *Journal of Duhok University*, *26*(2), 416-426.
50. Sami, T. M. G., Zeebaree, S. R., & Ahmed, S. H. (2024). Designing a New Hashing Algorithm for Enhancing IoT Devices Security and Energy Management. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(4s), 202-215.
51. Abdullah, H. S., & Zeebaree, S. R. (2024). Distributed Algorithms for Large-Scale Computing in Cloud Environments: A Review of Parallel and Distributed Processing. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(15s), 356-365.
52. Ibrahem, A. H., & Zeebaree, S. R. (2024). Tackling the Challenges of Distributed Data Management in Cloud Computing-A Review of Approaches and Solutions. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(15s), 340-355.