International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Securing the Cloud: A Critical Appraisal of Data Security Strategies

Madhura Yadav M P
Research Scholar, Dept. of Computer Science and Engineering,
Srinivas University Institute of Engineering & Technology, Mangalore, Karnataka, India
mpmy.madhura@gmail.com
ORCID: 0009-0009-9143-9660

Dr. Sanjeev Kulkarni
Associate Professor, Dept. of Computer Science and Engineering,
Srinivas University Institute of Engineering & Technology Mangalore Karnataka, India
sanjeev.d.kulkarni@gmail.com

Abstract— Cloud computing, a paradigm shift in the evolution of the internet, has garnered significant attention. However, security remains a primary concern, hindering its widespread adoption. Cloud computing essentially transfers user data and applications to remote data centers, where users relinquish control, and data management practices may not always adhere to the highest security standards. This unique characteristic of cloud computing raises a multitude of security concerns that warrant careful consideration and understanding. One of the most crucial and prevalent security concerns is the potential exposure of user data and applications stored on service provider premises. In this article, an attempt is made to review the literature in this area of research.

Keywords- Data security, cloud data concealment, cloud security, review

I. INTRODUCTION

The information technology (IT) environment has undergone a major transformation in the twenty-first century. Cloud computing is an innovative development in IT architecture that has replaced traditional methods that were characterized by locally managed services and on-premises data centers. The development of cloud computing constitutes an important milestone that has transformed the way businesses and organizations function in the modern era. Regardless of an organization's size or industry, the cloud has opened up previously unattainable opportunities by providing scalability, flexibility, and cost-efficiency. Data security has become a significant concept as a result of workloads, applications, and important data migrating to the cloud.

Cloud data security is not only a technological consideration; it is absolutely necessary. Because cloud computing is virtualized and data is stored on remote computers, it presents special security challenges. Ensuring that confidential, intact, and accessible sensitive information is available to only authorized entities is not only a basic business need but also a legal and ethical necessity. This study begins with a thorough examination of data security in the context of cloud computing. The origins of cloud computing can be found in the late 1990s and early 2000s, when virtualization technologies were still in their infancy and the World Wide Web was just getting started. The basis for a technological revolution that would shape the ensuing decades was created by these fundamental advancements. The ownership and control of physical hardware and software gave way to a model where resources are made available as services over the internet with the advent of cloud computing. Through the on-demand rental of computing power, storage, and services, the cloud has allowed businesses to quickly expand and innovate, cut expenses associated with running their operations, and reconsider their approach to marketing [1].

The first commercial cloud computing services appeared in the first ten years of the twenty-first century. Driven by the promise of increased efficiency and agility, corporations and government agencies were the main users of these early services, and these services were offered by a small number of organizations. In the decade of the 2010s, the industry for cloud computing saw an unheard-of boom. As cloud computing became the standard for offering IT services, a variety of new cloud providers joined the market, and services became more accessible and affordable [1]. The trend is still present in the 2020s, with cloud computing acting as a major means of delivering IT to a wide range of businesses, including startups, large corporations, and government agencies.

1.1 **Significance of Cloud Computing**

Beyond its technological capabilities, cloud computing is significant because it radically changes how businesses operate, develop, and compete in a digitally driven world. Several important benefits of cloud computing are highlighted [2]:

- Reduced IT Costs: Capital expenditure is greatly reduced when cloud services take the place of large initial investments in hardware and data centers. The benefits of scale that cloud providers offer also optimize operating expenses.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

- Improved Agility and Scalability: Cloud services are scalable and versatile; therefore, businesses may easily adjust to the demands and changes in their environment. One of the key features of cloud computing is the flexibility to scale resources up or down as needed.
- Increased Security and Reliability: Reputable cloud providers make significant investments in data redundancy and security protocols. They frequently outperform conventional data centers in terms of maintaining data security and continuity.
- Access to the Latest Innovations: By giving businesses access to cutting-edge innovations and technology, cloud services help them stay ahead of the curve and competitive in their particular markets.

The cloud is a transformational force as much as a technological advancement. Because of its flexibility, traditional IT infrastructure would not have made it possible for businesses to adopt cutting-edge business models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Organizations that move to the cloud face new security dynamics, obligations, and challenges when it comes to their data, which is frequently the lifeblood of their business.

1.2 Data Security in the Cloud

While the cloud offers unmatched benefits, it also comes with a set of difficulties, one of which is data security. The methods, tools, and regulations used to shield data from unwanted access, disclosure, alteration, and destruction are collectively referred to as data security. Strong data security measures are more important in cloud computing environments since data is kept remotely on servers run by other companies. Because of this shared responsibility paradigm, businesses have to have faith in cloud providers to protect their services and data. Therefore, building confidence with the cloud service provider is just as important as implementing technical protections when it comes to data security [3].

Data security is now a top priority in the IT sector because of the rise of cloud computing. Complete data security measures are crucial as more and more businesses throughout the world move their applications and data to the cloud. There are numerous challenges to be resolved, including the shared responsibility model, regulatory compliance, and data breaches and threats. To ensure that their digital assets are protected in this environment, companies and organizations need to manage the complexity of data security. They use a number of techniques, such as encryption, identity and access management, frequent security audits, and compliance with legal requirements, to do this. However, customers are not solely accountable for maintaining data security in the cloud. Understanding the security features and policies of cloud providers is essential for enterprises to make well-informed decisions regarding their cloud environments, since these providers play a critical role. The data security sector is always changing due to data breaches, data privacy laws, and the ever-changing threat landscape.

1.3 Data Security Challenges in Cloud Computing

Some of the most important data security issues in cloud computing are as follows:

- Lack of visibility and control: The underlying hardware and software used to store and process data are usually highly controllable by cloud providers. Organizations may find it challenging to keep control and visibility over their data as a result.
- Shared infrastructure: Usually, cloud providers share their infrastructure with several clients. This implies that there's a chance that criminal actors or other customers could gain access to a customer's data.
- Insecure interfaces: Users and apps can access a range of interfaces through cloud services. An attacker could be able to obtain data using these interfaces because they are susceptible to attack.
- Malicious insiders: Many employees are usually employed by cloud providers to manage and operate their services in cloud infrastructure. There's an opportunity that one of these employees will act maliciously and misuse their access to information.
- Data breaches: Attackers frequently target cloud services in an effort to steal data. This might be accomplished in a number of ways, including by deceiving users into disclosing their credentials or taking advantage of security holes in cloud software.

1.4 Some Basic Terms in Cryptography

- Encryption: The practice of encoding data using various encryption algorithms to transform it from its original representation to a new representation in order to conceal it from unauthorized users is known as encryption.
- Decryption: The process of restoring the encrypted data to its original form is known as decryption. It is the encryption process done in reverse.
- Algorithm or cipher: An algorithm, often known as a cipher, is a mathematical procedure that is well-defined and used in both encryption and decoding.
- Plain Text: This is the original text message that Alice, the sender, wishes to deliver to Bob, the recipient. The simple text may be in the form of a picture, audio file, video, etc.
- Cipher Text: The text that is encoded and results from the encryption process cannot be read.
- Avalanche effect: Certain specific properties of the encryption algorithm are defined by the utilization of the avalanche effect. Multiple bits of a ciphertext message should alternate if one bit or a little change in the plaintext is made, or vice versa.

II. APPROCHES TO ENSURE DATA SECURITY IN CLOUD COMPUTING

The following categories contribute to cloud computing data security approaches:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

A. Encryption

Certain encryption methods are used to transform plain text into cipher text; To guarantee cloud data security, a digital signature system utilizing the RSA algorithm is suggested in [5]. The program employs a "hashing algorithm" to generate a condensed representation of the data sheets in the form of a message digest. This digest is then encrypted using the user's private key, creating a digital signature. The program also generates its own message digest using the data sheets. When verifying the integrity of the data sheets, the program decrypts the digital signature with the sender's public key, producing a second message digest. If both message digests match, the integrity of the data sheets is confirmed.

The combining of the fundamental components of the Data Encryption Standard (DES) and the Simplified Data Encryption Standard (SDES) with the Playfair and Vigenere cipher algorithms is detailed in [6]. This process entails the division of a fixed 64-bit plaintext block size into two halves through the utilization of a "black box." The left half comprises six bits, while the right half consists of two bits. Subsequently, the six bits undergo processing in a block designated as the "superior function," where they are further partitioned into two segments: the initial two bits denote the rows, and the concluding four bits signify the columns. By discerning the rows and columns, the corresponding value is determined. Following the application of this function to all 8 octets of the Vigenere block's output, the black box yields a 64-bit result once more. These bits are then segregated into 4 additional octants, with the right 4 bits being consolidated to form the right halves. Finally, the left half of this configuration is derived by performing an XOR operation on the left and right halves. This technique undergoes three iterations.

In [7], encryption of data was implemented using the RSA technique, and the security of the key exchange was ensured through Bilinear Diffie-Hellman. The proposed method introduces a message header to each data packet, facilitating secure and direct communication between the client and the cloud without relying on a third-party server. The cloud server generates the public key, private key, and user identifier upon receiving a data storage request from the user. Prior to submitting the file to the cloud, the user is required to perform two tasks: append a message header to the data and utilize a secret key to encrypt both the data and the message header. Upon receiving a user's data request, the cloud server examines the message header, extracting the Unique Identification for Server in the Cloud (SID) data. If SID information is identified, the user's request is fulfilled; otherwise, it is rejected.
In [8], a technique is outlined to ensure the availability, integrity, and confidentiality of data in the cloud. This method employs Secure Socket Layer (SSL) 128-bit encryption, with the potential for enhancement to 256-bit encryption. To gain access to the encrypted data, users must strictly provide a valid user identity and password.

In [9], when data is transmitted to the cloud by the user, the cloud service provider generates a key, employs the RSA algorithm for encrypting the customer's data, and subsequently stores the encrypted data within its data center. Upon a user's request for data retrieval from the cloud, the cloud service provider verifies the user's identity and furnishes the encrypted data, which the user can decipher using their private key.

Additionally, [10] introduces a three-tiered model for data security, where each layer performs a distinct function to protect data in the cloud. The first layer oversees authentication, the second layer encrypts data, and the third layer manages data recovery functions.

The RC5 technique is used in [11] to secure cloud data. Data that is encrypted is transferred, and even if it is stolen, there won't be a matching key to unlock it. In [12], the proposition of role-based access control (RBAC) cloud architecture and the utilization of role-based encryption (RBE) are suggested methods for enhancing cloud data security. These approaches empower organizations to securely store data in public clouds while maintaining the confidentiality of their organizational structure in private clouds.

Furthermore, [13] delineates four authorities—data owner, data consumer, cloud server, and N attribute authorities. The attributes for each authority are categorized into N distinct groups. Prior to transmitting data to the cloud server, the data owner encrypts it using a public key, which can be acquired from any authority. Upon the data request, the authorities generate a private key and transmit it to the data consumer, who gains access to the file only after verification by the cloud server.

In [14], two approaches to securing cloud computing are introduced, one involving a trusted third party and the other operating without such a requirement. Both approaches rely on symmetric bivariate polynomial-based secret sharing and Elliptic Curve Diffie Hellman (ECDH) to ensure data security in cloud environments. Another method outlined in [15] employs location-based encryption, utilizing the user's location and geographic coordinates. This technique equips both the cloud and the user computer with a geo-encryption method, associating data with the business name or employee identities. Retrieving information involves searching for a similar label in the cloud, which then retrieves the corresponding data.
To protect the privacy of data stored in the cloud, [16] introduces a method that combines Diffie Hellman key exchange and digital signature with the Advanced Encryption Standard encryption algorithm. Recognized as a three-way mechanism, this approach provides simultaneous data security, verification, and authentication.

B. Homomorphic Token

A technique is devised to enable direct comparison of an encrypted token with the data without the need for key decryption, ensuring data security. In [17], the implementation of a homomorphic token method is proposed, utilizing homomorphic tokens and distributed data erasure-coding verification. This method facilitates secure and efficient

dynamic operations on data blocks, including appending, updating, and deleting data. Additionally, [18] introduces a model that integrates storage accuracy assurance and identifies misbehaving server(s) through the use of a homomorphic token scheme and token pre-computation method.

C. Guidelines

Various studies have proposed criteria to ensure cloud data security. [19] presents a novel cloud system design methodology encompassing three aspects: data obfuscation, data concealing, and the separation of infrastructure and software service providers. These features establish guidelines for cloud data security. To safeguard data in cloud architecture, [20] introduces the agent's technique, which utilizes three agents – the file agent, the authentication agent, and the key managing agent – to secure data. [21] provides guidelines on six key data technologies: cloud resource access control, trustworthy cloud computing, data privacy protection, data evidence of existence and usability, and trusted access control. [22] offers guidelines by conducting a meta-analysis of four distinct encryption algorithms, aiding in the selection of an appropriate method for a specific scenario.

D. Harmonizing Scheme

To establish a data repository, a privacy-preserving repository was introduced in [23]. This repository focused on reconciling operations to ensure data confidentiality while preserving harmonizing relationships in the cloud. The proposed scheme allows data owners to offload most computation-intensive tasks to cloud servers without revealing the data's contents.

E. Data Concealment Component

[24] proposed a data concealment architecture comprising three components: a data generator, a data concealment component, and a data marking component. The evaluation of this component demonstrates its effectiveness in concealing sensitive user data from potential threats.

F. Token

A proposed solution for enhancing cloud computing data security involves a versatile and effective distribution verification technique. Unlike the conventional approach of employing pseudorandom data for verifying the integrity of erasure-coded data, this method utilizes token pre-computation based on Sobol sequence. The recommended paradigm unfolds through three stages: the challenge-response protocol, token pre-computation, and file distribution.

G. Framework

A framework called TrustCloud is presented in [26], with the goal of encouraging the adoption of file-centric and data-centric logging mechanisms to improve the security and confidentiality of data in cloud computing. The framework proposes a detective and data-centric approach to increase data security. In [27], a multi-tenant system is constructed to provide a framework. The three layers of the developed solution are the data access layer, the business logic layer, and the display layer. User data is extremely secure because of these levels.

A framework is presented in [28] and includes the SecCloud protocol, which is the first protocol to cover secure computing and storage in a cloud environment through batch authentication, probabilistic sampling processes, and designated verifier signatures. A three-stage methodology is described in [29]. The first phase involves indexing data and metadata to guarantee total data privacy and prevent unethical cloud service providers. To maintain the confidentiality of searches and the generated files from the cloud service provider, multi-user private keyword searchable encryption is applied to encrypted data in the second phase. The last phase uses policy to enable user data sharing through the use of encryption and metadata.

H. Stripping Algorithm

In [30], a stripping algorithm is utilized to enhance the security of image data in the cloud. The approach comprises three modules: image analysis, data separation, and data distribution.

I. Modern Cryptography

Contemporary encryption algorithms, including RC6, AES, DES, 3DES, and Blowfish, continue to be crucial for ensuring data security in cloud computing. An assessment of these encryption algorithms has been conducted through randomness testing, employing NIST statistical testing in a cloud computing environment (Amazon EC2) [31].

J. Searchable Encryption

A type of encryption known as "searchable encryption" allows data to be searched for or retrieved from encrypted files without requiring complete decryption. Through the use of encryption and searchable encryption technologies, cloud-secure architecture [32, 33] enables safe data retrieval and the search process for encrypted data.

K. Homomorphic Encryption

Homomorphic encryption is a type of encryption technology wherein ciphertext is subjected to a computation, and the resultant output, when decoded, corresponds with the outcome of an operation done on plaintext [34, 35]. Homomorphic techniques are typically used to preserve data integrity over cloud networks.

L. Attribute Based Encryption

A public-key one-to-many encryption called attribute-based encryption (ABE) [36] enables users to encrypt and decode data according to their own attributes. Key-policy ABE and ciphertext-policy ABE are the two types of ABE systems.

m) Hybrid Encryption - To leverage the benefits of various encryption methods, hybrid encryption [37, 38] integrates two or more encryption systems.

III. SECURITY TECHNIQUES AND APPROACHES FOR DATA IN THE CLOUD

TABLE I. SECURITY TECHNIQUES AND APPROACHES

Sl. No	*Author*	*Proposed Method*	*Approaches*	*Security For*	*Source*
1.	Somani, U., Lakhani, K., & Mundra, M. (2010, 28- 30 Oct. 2010).	Digital Signature with RSA algorithm	Encryption	Data	Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing
2.	Vamseek and sriramr,(2011)	Playfair and vigenere cipher techniques were merged with structural aspects of Simplified Data Encryption Standard (SDES) and Data Encryption Standard (DES).	Encryption	Data	Data Security in Cloud Computing
3.	Shuai, H., & Jianchuan, X. (2011, 15-17 Sept. 2011)	RSA	Encryption	Data	Ensuring data storage security through a novel third party auditor scheme in cloud computing
4.	Sood, S. K. (2012)	Secure Socket Layer (SSL)	Encryption	Data	A combined approach to ensure data security in cloud computing
5.	Parsi Kalpana & Sudha Singaraju (2012)	RSA	Encryption	Data	Data Security in Cloud Computing using RSA Algorithm
6.	Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012,14 -16 May 2012)	Three layered data security model	Encryption	Data	Enhanced data security model for cloud computing
7.	Singh, J., Kumar, B., & Khatri, A. (2012, 6-8 Dec. 2012).	RC5	Encryption	Data	Improving stored data security in Cloud using Rc5 algorithm
8.	Lan, Z.,	Role Base	Encrypt	Data	Achieving
	Varadharajan, V., & Hitchens, M. (2013).	Encryption	ion		Secure Role-Based Access Control on Encrypted Data in Cloud Storage
9.	Taeho, J., Xiang-Yang, L., Zhiguo, W., & Meng, W. (2013, 14-19 April 2013).	Four authorities are defined i.e, data owner, data consumer, cloud server and N attribute authorities	Encryption	Data	Privacy preserving cloud data access with multi-authorities
10.	Ching-Nung, Y., & Jia-Bin, L. (2013, 2-5 July 2013).	Elliptic Curve DiffieHellman (ECDH) and symmetric bivariate polynomial	Encryption	Data	Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing
11.	Abolghasemi, M. S., Sefidab, M. M., &Atani, R. E. (2013, 22-25 Aug. 2013).	Location based encryption	Encryption	Data	Using location based encryption to improve the security of data access in cloud computing
12.	Rewagad, P., & Pawar, Y. (2013, 6-8 April 2013).	Digital signature and Diffie Hellman key exchange in combination with Advanced Encryption Standard encryption	Encryption	Data	Use of digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing
13.	Cong, W., Qian, W., Kui, R., & Wenjing, L. (2009, 13-15 July 2009).	Homomorphic token with distributed verification	Homomorphic token	Data	Ensuring data storage security in Cloud Computing
14.	Tribhuwan, M. R., Bhuyar, V. A., &Pirzade, S. (2010, 16-17 Oct. 2010).	Token pre-computation	Homomorphic token	Data	Ensuring Data Storage Security in Cloud Computing through Two-Way Handshake Based on Token Management
15.	Yau, S. S., & An,	Guidelines are provided for data	Guidelines	Data	Protection of users' data

Sl. No	*Author*	*Proposed Method*	*Approaches*	*Security For*	*Source*
	H. G. (2010). ting	security			confidentiality in cloud compu
16.	Feng-qing, Z., & Dian-Yuan, H. (2012, 24-26 Aug. 2012).	Agents method	Guidelines	Data	Applying agents to the data security in cloud computing
17.	Zhongbin, T., Xiaoling, W., Li, J., Xin, Z., & Wenhui, M. (2012, 27-30 May 2012).	Guidelines about six key data technolo	Guidelines	Data	Study on Data Security of Cloud Computing
18.	Rachna, A., and Anshu, P.(Jul-Aug 2013).	Guidelines are provided by giving the meta analysis of Four Different Encryption Algorithms	Guidelines	Data	Secure User Data in Cloud Computing Using Encryption Algorithms
19.	Mishra, R., Dash, S. K., Mishra, D. P., & Tripathy, A. (2011, 8-10 April 2011).	Harmonizing Operations	Harmonizing scheme	Data	A privacy preserving repository for securing data across the cloud
20.	Delettre, C., Boudaoud, K., &Riveill, M. (2011, June 28 2011-July 1 2011).	Data Concealment Component	Data concealment	Data	Cloud computing, security and data concealment
21.	Syam Kumar, P., Subramanian, R., & Thamizh Selvam, D. (2010, 28-30 Oct. 2010).	Token Pre-computation using Sobol Sequence	Token	Data	Ensuring data storage security in cloud computing using Sobol Sequence
22.	Ko, R. K. L., Kirchberg, M., & Bu Sung, L. (2011, 3-5 Aug. 2011).	Framework is provided; known as TrustCloud	Framework	Data	From system-centric to data-centric logging Accountability, trust & security in cloud computing
23.	Gawali,	Framework is	Frame	Data	Enhancement

Sl. No	*Author*	*Proposed Method*	*Approaches*	*Security For*	*Source*
	M. B., & Wagh, R. B. (2012, 6-8 Dec. 2012).	provided by building a multi-tenant system	work		for data security in cloud computing environment.
24.	Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., et al. (2014).	Framework is provided that consists of protocol named SecCloud	Framework	Data	Security and privacy for storage and computation in cloud computing
25.	Rashid, F., Miri, A., &Woungang, I. (2013, June 28 2013-July 3 2013).	Framework it consist of three steps	Framework	Data	Secure Enterprise Data Deduplication in the Cloud
26.	Leistikow, R., &Tavangarian, D. (2013, 25-28 March 2013).	Stripping Algorithm	Stripping	Data	Secure Picture Data Partitioning for Cloud Computing Services
27.	El-etriby, S., Mohamed, E. M., & Abdul-kader, H. S. (2012, March).	RC6, AES, DES, 3DES and Blow-Fish	Modern cryptography	Data	Modern encryption techniques for cloud computing
28.	Hamdan M. Al-Sabri, Saleh M. Al-Saleem (2013)	Cloud Storage Encryption (CSE) Architecture	Searchable encryption	Data	Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security
29.	Mao-Pang Pang Lin, Trend Micro, Taiwan, Wei-Chih Hong, Chih-Hung Chen, Chen-Mou Cheng , (2013)	Multi-user Secure Indices for Encrypted	Searchable encryption	Data	Design and Implementation of Multi-user Secure Indices for Encrypted Cloud Storage
30.	Shivani Gambhir, Ajay Rawat, Rama	Fully Homomorphic Encryption	Homomorphic encryption	Data	Cloud Auditing: Privacy Preserving using Fully

Sl. No	*Author*	*Proposed Method*	*Approaches*	*Security For*	*Source*
	Sushil, (2013)				Homomorphic Encryption in TPA
31.	Cong Wang, S.-M. Chow, Qian Wang, Kui Ren , Wenjing Lou , (2013)	Privacy-Preserving Public Auditing	Homomorphic encryption	Data	Privacy-Preserving Public Auditing for Secure Cloud Storage
32.	ShuaishuaiZhu ;Xiaoyuan Yang ; Xuguang Wu , (2013)	Attribute Based Encryption	Attribute based encryption	Data	Secure Cloud File System with Attribute Based Encryption
33.	Chao Yang ; Weiwei Lin ; Mingqi Liu, (2013)	Novel Triple Encryption Scheme	Hybrid encryption	Data	A Novel Triple Encryption Scheme for Hadoop-Based Cloud Data Security
34.	Sengupta , N., Holmes J.	Cryptography Based Security	Hybrid encryption	Data	Designing of Cryptography Based Security System for Cloud Computing

IV. Conclusions and Future Directions

Utilizing cloud computing has several advantages, including increased accessibility, rapid deployment, and cost effectiveness. Still, there are a lot of real-world issues that need to be resolved. One of them is the secrecy of the data. Numerous researchers have made contributions to reduce the data security risk in this field using various strategies that are detailed in this paper. A study of the literature is done on the studies that have been done on cloud computing data security. We were able to comprehend many authors' contributions to the subject of cloud data security, algorithm kinds, and methods for data security.

Even though the cloud's data security ideas have been examined in our assessment, further research is required to fully understand data security. Future work will expand on this review by adding other sources (workshops, journals, and conferences). In the future, we hope to investigate other security algorithms in the context of cloud computing and create a security model that uses encryption to hide data in the cloud.

References

[1] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., &Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision support systems*, *51*(1), 176-189.

[2] Shaw, S. B., & Singh, A. K. (2014, March). A survey on cloud computing., International conference on green computing communication and electrical engineering (ICGCCEE) (pp.1-6). IEEE

[3] Pearson, S. (2013). *Privacy, security and trust in cloud computing* (pp. 3-42). Springer London.

[4] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

[5] Somani, U., Lakhani, K., & Mundra, M. (2010, 28- 30 Oct. 2010). Implementing digital signature with RSA ncryption algorithm to enhance the Data Security of cloud in Cloud Computing. Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on.

[6] Vamsee k and sriramr,(2011) "Data Security in Cloud Computing,"in Journal of Computer and Mathematical Sciences Vol. 2, pp.1-169.

[7] Shuai, H., &Jianchuan, X. (2011, 15-17 Sept. 2011). Ensuring data storage security through a novel third party auditor scheme in cloud computing. Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on.

[8] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing, Journal of Network and Computer Applications, 35(6), 1831- 1838.

[9] Parsi Kalpana&SudhaSingaraju (2012), Data Security in Cloud Computing using RSA Algorithm. International Journal of Research in Computer and Communication technology(IJRCCT), vol 1, Issue 4.

[10] Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012,14-16 May 2012). Enhanced data security model for cloud computing. Paper presented at the Informatics and Systems (INFOS), 2012 8th International Conference on.

[11] Singh, J., Kumar, B., & Khatri, A. (2012, 6-8 Dec. 2012), Improving stored data security in Cloud using Rc5 algorithm. Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on.

[12] Lan, Z., Varadharajan, V., & Hitchens, M. (2013), Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage. Information Forensics and Security, IEEE Transactions on, 8(12), 1947-1960.

[13] Taeho, J., Xiang-Yang, L., Zhiguo, W., & Meng, W. (2013, 14-19 April 2013). Privacy preserving cloud data access with multi-authorities. Paper presented at the INFOCOM, 2013 Proceedings IEEE.

[14] Ching-Nung, Y., & Jia-Bin, L. (2013, 2-5 July 2013), Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing. Paper presented at the Biometrics and Security Technologies (ISBAST), 2013 International Symposium on.

[15] Abolghasemi, M. S., Sefidab, M. M., &Atani, R. E. (2013, 22-25 Aug. 2013). Using location based encryption to improve the security of data access in cloud computing. Paper presented at the Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on.

[16] Rewagad, P., & Pawar, Y. (2013, 6-8 April 2013), Use of digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. Paper presented at the Communication Systems and Network Technologies CSNT), 2013 International Conference on.

[17] Cong, W., Qian, W., Kui, R., & Wenjing, L. (2009, 13-15 July 2009), Ensuring data storage security in Cloud Computing. Paper presented at the Quality of Service, 2009. IWQoS. 17th International Workshop on.

[18] Tribhuwan, M. R., Bhuyar, V. A., &Pirzade, S. (2010, 16-17 Oct. 2010). Ensuring Data Storage Security in Cloud Computing through Two-Way Handshake Based on Token Management. Paper presented at the Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference on.

[19] Yau, S. S., & An, H. G. (2010). Protection of users' data confidentiality in cloud computing. Paper presented at the

Proceedings of the Second AsiaPacific Symposium on Internetware.

[20] Feng-qing, Z., & Dian-Yuan, H. (2012, 24-26 Aug. 2012). Applying agents to the data security in cloud computing. Paper presented at the Computer Science and Information Processing (CSIP), 2012 International Conference on.

[21] Zhongbin, T., Xiaoling, W., Li, J., Xin, Z., & Wenhui, M. (2012, 27-30 May 2012). Study on Data Security of Cloud Computing. Paper presented at the Engineering and Technology (S-CET), 2012 Spring Congress on.

[22] Rachna, A., and Anshu, P.(Jul-Aug 2013). Secure User Data in Cloud Computing Using Encryption Algorithms in International Journal of Engineering Research and Applications (IJERA), 3(4),1922- 1926.

[23] Mishra, R., Dash, S. K., Mishra, D. P., & Tripathy, A. (2011, 8-10 April 2011), A privacy preserving repository for securing data across the cloud. Paper presented at the Electronics Computer Technology (ICECT), 2011 3rd International Conference on.

[24] Delettre, C., Boudaoud, K., &Riveill, M. (2011, June 28 2011-July 1 2011). Cloud computing, security and data concealment. Paper presented at the Computers and Communications (ISCC), 2011 IEEE Symposium on.

[25] Syam Kumar, P., Subramanian, R., & Thamizh Selvam, D. (2010, 28-30 Oct. 2010)., Ensuring data storage security in cloud computing using Sobol Sequence. Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on.

[26] Ko, R. K. L., Kirchberg, M., & Bu Sung, L. (2011, 3-5 Aug. 2011). From system-centric to data-centric logging Accountability, trust & security in cloud computing. Paper presented at the Defense Science Research Conference and Expo (DSR), 2011.

[27] Gawali, M. B., & Wagh, R. B. (2012, 6-8 Dec. 2012)., Enhancement for data security in cloud computing environment. Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on.

[28] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., et al. (2014). Security and privacy for storage and computation in cloud computing. Information Sciences, 258(0), 371-386.

[29] Rashid, F., Miri, A., &Woungang, I. (2013, June 28 2013-July 3 2013). Secure Enterprise Data Deduplication in the Cloud. Paper presented at the Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on.

[30] Leistikow, R., &Tavangarian, D. (2013, 25-28 March 2013). Secure Picture Data Partitioning for Cloud Computing Services. Paper presented at the Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on.

[31] El-etriby, S., Mohamed, E. M., & Abdul-kader, H. S. (2012, March). Modern encryption techniques for cloud computing. In *ICCIT* (pp. 800-805)

[32] Hamdan M. Al-Sabri, Saleh M. Al-Saleem, "Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security" IJCSI International Journal of Computer Science Issues, Volume 10, Issue 2, 2013

[33] Mao-Pang Pang Lin, Trend Micro, Taiwan, Wei-Chih Hong, Chih-Hung Chen, Chen-Mou Cheng "Design and Implementation of Multi-user Secure Indices for Encrypted Cloud Storage" International Conference on Privacy, Security and Trust, IEEE, 2013.

[34] Shivani Gambhir, Ajay Rawat, Rama Sushil, "Cloud Auditing: Privacy Preserving using Fully Homomorphic Encryption in TPA", International Journal of Computer Applications, Volume 80, Number 14, 2013.

[35] Cong Wang, S.M. Chow, Qian Wang, Kui Ren , Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Cloud Computing, Volume 62, Issue 2, 2013.

[36] ShuaishuaiZhu, Xiaoyuan Yang,Xuguang Wu, "Secure Cloud File System with Attribute Based Encryption" IEEE International Conference on Intelligent Networking and Collaborative Systems, 2013.

[37] Chao Yang, Weiwei Lin,Mingqi Liu, "A Novel Triple Encryption Scheme for Hadoop-Based Cloud Data Security" IEEE International Conference on Emerging Intelligent Data and Web Technologies, 2013.

[38] Sengupta, N., Holmes J. "Designing of Cryptography Based Security System for Cloud Computing" IEEE International conferences on Cloud & Ubiquitous Computing & Emerging Technologies, 2013.