International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.6 January – 2022 DOI: 10.46647/ijetms.2022.v06i01.001
ISSN: 2581-4621

Enhanced Data Security in Cloud Computing: Survey

Mageto Stephen N[1], *Dr.N.V.Balaji*[2]
[1]*Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India*
[2]*Research supervisor, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India*
[1]*magetosteve@gmail.com*
[2]*nvb1977@gmail.com*

***Abstract*---The next era in the advent of the internet is internet based computing also known as cloud computing. It has been the emphasis in recent years, but security concerns are one among the most important impediments to the rise of cloud computing.. It essentially sends user data and application programs to massive data centers, i.e. a distant cloud, where consumers have little control and data management may be insecure. However, numerous security issues raised by the cloud's unique nature must be addressed and fully acknowledged.. Amongst the most critical concerns which must be tackled is the security issue. Issues with data security created by user data and software in the provider's jurisdiction. Cloud users search for cloud resources with secure data management. When sharing their personal data over public clouds, some cloud users may prefer to manage their data with more privacy. This document focuses on improving privacy-related data security in the cloud and related works that have been done to enhance data security in cloud computing. This research review work analyzes and discusses several of the security and privacy improvements evaluated in related existing systems.**

***Keywords*: Authentication, Cloud computing, Confidentiality, Data security, Encryption**.

I. INTRODUCTION

There is no single definition of cloud computing that everyone agrees on [9]. It is described as a dynamic platform that is usually easy to scale and increase transparency. Provide users with virtual resources online. There are major three levels to cloud computing services; Platform, Infrastructure and software as Service. Even though every service model contains security measures, security requirements differ based on whether the services are private, public, mixed, or public cloud [17]. The cloud is also a five-part architecture, including customers, applications, platforms, and infrastructure and the server.

- A public cloud that is owned and control by a service provider.
- Community cloud, the physical structure that an organization and association have.
- The private cloud, the structure of which is owned and created by a particular organization.
- The previous three models have been altered by the hybrid cloud.
- Using their ineternal architecture (IaaS, PaaS and SaaS) are the deployment models of the cloud.

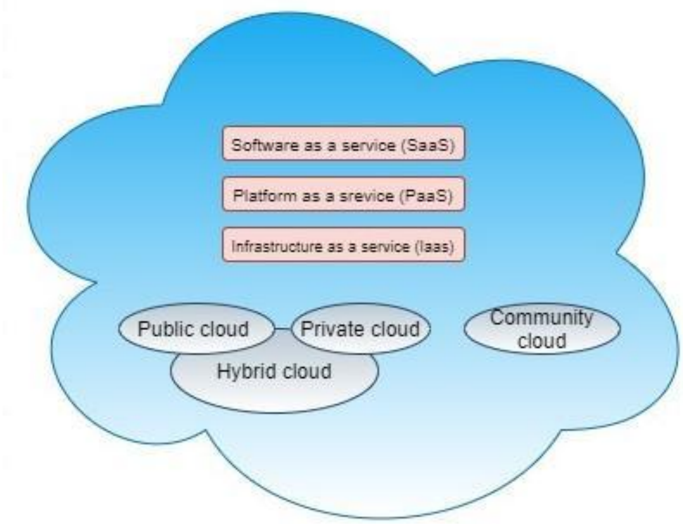

Software as a service (SaaS)
Platform as a srevice (PaaS)
Infrastructure as a service (Iaas)
Public cloud
Private cloud
Community cloud
Hybrid cloud

Figure 1: Model and services of cloud computing

Security service

Security comprises the goals of protection, restoration, and assurance. Protection of information in a computer system from numerous risks. In reality, the security service provided by the security mechanism enforces the security policy, as well as the security of computer networks and information systems. It is offered via services like as integrity, confidentiality, identity verification, non-repudiation, and availability. [12].

TABLE 1
SECURITY ISSUES IN CLOUD COMPUTING

Confidentiality	Make certain that no information is given or distributed to unauthorized persons, organizations, or operations. Indeed, data is delivered and received without unwanted objects gaining access to it during transmission. Encrypting data is an effective method of achieving privacy. It is accomplished through the use of a symmetric or asymmetric key model [16].
Integrity	Ascertain that the data received by the authorised individual corresponds to the data supplied. The data has not changed [15].
Availability	Ensure that valid users may access services and that data is produced. Available and usable at the request of authorized persons.
Authentication	Verify the sender and recipient of the message's identities. In reality, the integrity and secrecy of information are only significant when the sender and receiver's identities are fully confirmed. [14]
Non-repudiation	Ascertain that the action made will not be rejected by either the sender or the receiver. Denials are classified into two types: rejection of origin and refusal of destination. In the first instance, neither the sender nor the receiver may decline the transfer message, and neither can they refuse to deliver the message [13].

Cloud computing environments present many challenges. It's a conflict-free cloud user identity management that provides security for data-dependent applications, protects the privacy of users who do not want to expose their identities, and maintains control over the lifecycle of external data. Data outsourcing is just data that is openly shared with different users.

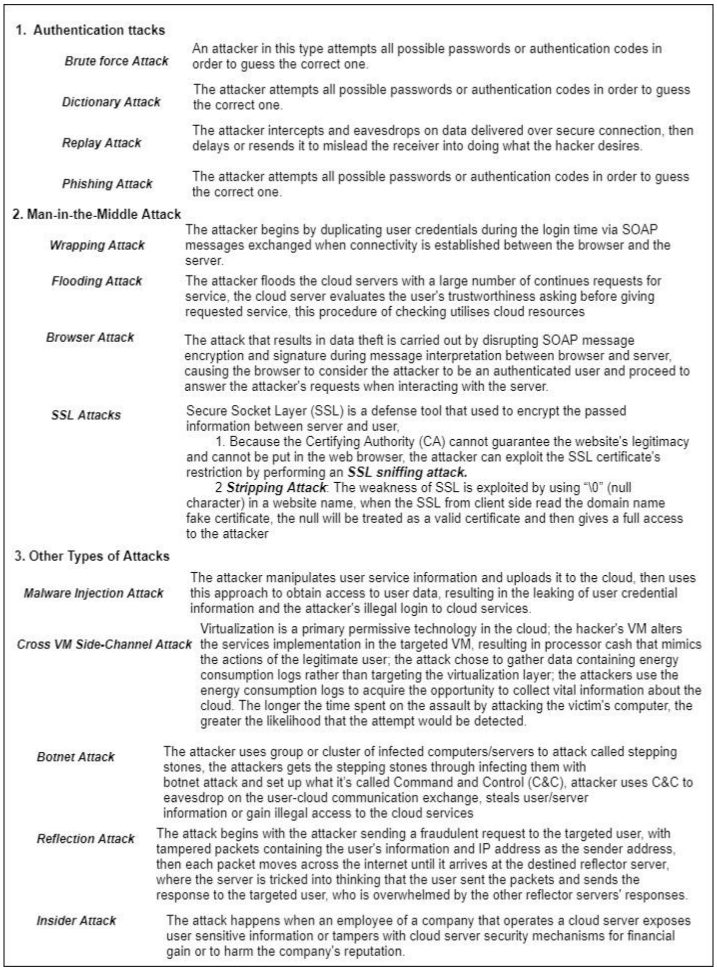
Cloud computing environments offer many benefits to the users, but users do not like to log in to the cloud. Many analyzes show that the main problem with cloud computing is the security threat. Security risks can cause conflicts with the original user data. The second most important issue in cloud computing is protecting user privacy [18].

Cloud computing provides flexible and scalable user access without the need for a large number of servers. In this case, privacy is a major issue that users should expect when they do not want to disclose their personal information to them [11]

A. *Possible Types of Cloud Security Attacks*.

When users enter the cloud to share their personal data, they need to be aware of the security threats that can attack their data. Cloud providers need to provide trust to their users in order to get the highest level of service.

TABLE II
CLOUD ATTACKS IN CLOUD COMPUTING



1. Authentication ttacks	
Brute force Attack	An attacker in this type attempts all possible passwords or authentication codes in order to guess the correct one.
Dictionary Attack	The attacker attempts all possible passwords or authentication codes in order to guess the correct one.
Replay Attack	The attacker intercepts and eavesdrops on data delivered over secure connection, then delays or resends it to mislead the receiver into doing what the hacker desires.
Phishing Attack	The attacker attempts all possible passwords or authentication codes in order to guess the correct one.
2. Man-in-the-Middle Attack	
Wrapping Attack	The attacker begins by duplicating user credentials during the login time via SOAP messages exchanged when connectivity is established between the browser and the server.
Flooding Attack	The attacker floods the cloud servers with a large number of continues requests for service, the cloud server evaluates the user's trustworthiness asking before giving requested service, this procedure of checking utilises cloud resources
Browser Attack	The attack that results in data theft is carried out by disrupting SOAP message encryption and signature during message interpretation between browser and server, causing the browser to consider the attacker to be an authenticated user and proceed to answer the attacker's requests when interacting with the server.
SSL Attacks	Secure Socket Layer (SSL) is a defense tool that used to encrypt the passed information between server and user, 1. Because the Certifying Authority (CA) cannot guarantee the website's legitimacy and cannot be put in the web browser, the attacker can exploit the SSL certificate's restriction by performing an ***SSL sniffing attack.*** 2 ***Stripping Attack***: The weakness of SSL is exploited by using "\0" (null character) in a website name, when the SSL from client side read the domain name fake certificate, the null will be treated as a valid certificate and then gives a full access to the attacker
3. Other Types of Attacks	
Malware Injection Attack	The attacker manipulates user service information and uploads it to the cloud, then uses this approach to obtain access to user data, resulting in the leaking of user credential information and the attacker's illegal login to cloud services.
Cross VM Side-Channel Attack	Virtualization is a primary permissive technology in the cloud; the hacker's VM alters the services implementation in the targeted VM, resulting in processor cash that mimics the actions of the legitimate user; the attack chose to gather data containing energy consumption logs rather than targeting the virtualization layer; the attackers use the energy consumption logs to acquire the opportunity to collect vital information about the cloud. The longer the time spent on the assault by attacking the victim's computer, the greater the likelihood that the attempt would be detected.
Botnet Attack	The attacker uses group or cluster of infected computers/servers to attack called stepping stones, the attackers gets the stepping stones through infecting them with botnet attack and set up what it's called Command and Control (C&C), attacker uses C&C to eavesdrop on the user-cloud communication exchange, steals user/server information or gain illegal access to the cloud services
Reflection Attack	The attack begins with the attacker sending a fraudulent request to the targeted user, with tampered packets containing the user's information and IP address as the sender address, then each packet moves across the internet until it arrives at the destined reflector server, where the server is tricked into thinking that the user sent the packets and sends the response to the targeted user, who is overwhelmed by the other reflector servers' responses.
Insider Attack	The attack happens when an employee of a company that operates a cloud server exposes user sensitive information or tampers with cloud server security mechanisms for financial gain or to harm the company's reputation.

B. *The issue of cloud privacy*.

Protecting the privacy of cloud users is one of the service providers' most important obligations, and the most sensitive user information is saved in cloud. If your data is published in cloud, users will not want to share their information with others. Challenges that motivate cloud service providers to ensure privacy include inadequate user control, information breaches, rogue secondary storage, uncontrolled data delivery, and dynamic provisioning.

This overview describes relevant mechanisms and technologies previously used for security and privacy. It also discusses the merits and demerits of each strategy.. Based on a review of the above mechanisms, it can be observed that the currently implemented system has more advantages.

II. RELATED WORK

D. V. Chadwick et al. proposed a scalable structure for the confidential exchange of network information (CTI) among collaborators for analysis [1]. The proposed framework establishes a five-tier trust architecture for cloud-based data transfer infrastructure at the cloud's edge. From plain text to anonymization and anonymization to symmetric cipher, data owners can choose the appropriate confidence and method for cleaning CTI data to process CTI data before sending it for analysis. CTI analysis delivers useful cyber threat intelligence to users, informing them of threats to their systems. Although standard security software have their own built-in analytic tools and notify clients of the preponderance dangers impacting their systems, due to the quickly changing nature of threats and the enormous and complicated number of CTIs handled, they seldom identify all active threats when this data is being processed. This architecture is functional because a Data Sharing Agreement (DSA) policy aligns CTI data in a Protected Data Object (DPO), and DSA is applied on the cloud-edge or the cloud, or both, to make clients trust their sensitive data. It will not spread to those who are untrustworthy or only half trusted until it is adequately trusted

To address data integrity and confidentiality challenges, M. Tahir et al. presented CryptoGA, a novel paradigm based on the genetic algorithm (GA) [12]. They used GA to create the encryption and decryption keys in this case, and encryption methods are utilized to protect the security and integrity of the cloud data. Evaluations and comparisons take into account of the common known parameters such as execution time, performance, key size, and avalanche effect. This experiment uses 10 different sets of test and validation data.

To improve cloud computing data security, Tabet et al. offer a lightweight encryption technique. A suggested technique for improving data security that may be used to safeguard cloud-based applications [3]. The algorithm is a 16-byte (128-bit) block cypher that encrypts data with a 16-byte (128-bit) key. It is built on the original architecture arrangement and substitution technologies to boost the encryption's complexity. This algorithm applies Shannon's propagation and confusion theory using logical operations (XOR, XNOR, transformation, and substitution). It is also flexible in choosing key length and number of turns. Compared with the password system, the experimental findings of the suggested method which is extensively used in cloud computing show that the algorithm has higher security, and its performance in terms of password execution time and security has been greatly improved. According to the National Institute of Standards and Technology (NIST) [19], confidentiality, availability, and integrity are basic requirements for cloud computing.

- **Authentication** Confirm the identity of the sender and recipient of the message.
- **Availability** Ensure availability of services to legitimate users and data production whenever needed.
- **Authorization** establish that the access points are reserved for clients who have provided certain information.

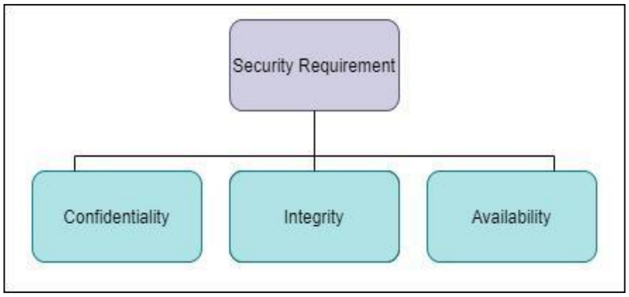


Figure 1: Basic security for cloud computing

K Kumar et al., proposed an algorithm that uses image masking and image segmentation to protect user data. In this case, image segmentation is used to mask data in different parts of the image [4]. The proposed algorithm's performance is assessed using numerous metrics such as PSNR and MSE value, and the results are compared to other existing techniques for pictures of various sizes. Steganography is the method of concealing data in a picture so that human eye cannot see the data. There are many methods of hiding information such as image masking, video masking, and audio masking. They devised a steganography and image hashing-based technique that can only conceal secrets in the original cover photo's computation or processing part. Confidential data is stored in a text file, the original message is encrypted with the RSA encryption technique, and the key is acquired. Then, copy and paste the key into the grayscale image's chosen pixels. Lastly, save a Stego image to the cloud. Stego is utilised as the input in the receiving procedure, all the stages are reversed, after which, the server receives the key from the image and uses the key to decrypt the original confidential data.

Narayanan, U. et al. Introduces a global picture of how to solve the major security challenges of big data in the cloud [5]. They proposed a new system architecture called SADS-Cloud, which supports the big data environment . It entails three processes: I big data outsourcing, (ii) big data interchange, and (iii) big data analysis. When substantial amounts of data are outsourced, the data owner scores in the trusted centre using the SHA-3 hash algorithm. The MapReduce approach is used to partition the input file into fixed-size chunks. Each block is encrypted using the SALSA20 algorithm. When vast amounts of data are exchanged, data consumers take part in safe file recovery. This is accomplished by hashing the user's credentials and comparing them to the database. Big data management incorporates three fundamental procedures for managing big data: compression, clustering, and indexing utilizing the Lemperl Ziv Markov Algorithm (LZMA), density-based application noise clustering (DBSCAN), and the usage of fractional index trees. Index of files in the cloud database, where you can perform individual searches, inserts and deletes. This work proposes four entities. Trust center (TC), data user (DU) cloud server (CS) and data owner (DO),. It solves the two main issues of user privacy and data security in the cloud that underpins big data. In order to securely authenticate users (data owners and users), they proposed the SHA-3 hash algorithm. Hash messages containing user information and saved in TC and CS. The data owner sends the data to the cloud server in a secure manner. The data is compressed using the LZMA compression method to optimize cloud storage for big data. Then data is encrypted using SALSA20 MapReduce to reduce encoding and decoding times. After the encryption is complete, send the data to CS. If the user requests the data to retrieve the data, it must be authenticated. Use the private key stream to retrieve and decrypt the required file. Consider two processes for managing big data through the cloud, such as using DBSCAN and fractal trees for clustering and indexing, respectively.

H ZHU et al. introduced a data integrity verification system based on a short signature algorithm (ZSS signature) that allows confidentiality and public inspection [6] by introducing a trusted third party whilst also reducing the burden of the hash function in the signing process, computational expenses are effectively reduced. It can withstand adaptive message selection assaults based on CDH's hard problem assumption. According to the evaluation, the circuit is more efficient and safe. The BLS signing mode must use the specific hash function, and the performance of batch signing is poor in the large data setting. .

Y Fan et al. Cloud users are given a set of permissions; duplication can only be performed if the cloud user has the appropriate permissions [7]. In addition, the solution strengthens fusion cryptography through user privileges and relies on the Trusted Runtime Environment (TEE) to manage keys securely, enabling these cryptosystems to defend against plaintext and chosen-ciphertext attacks

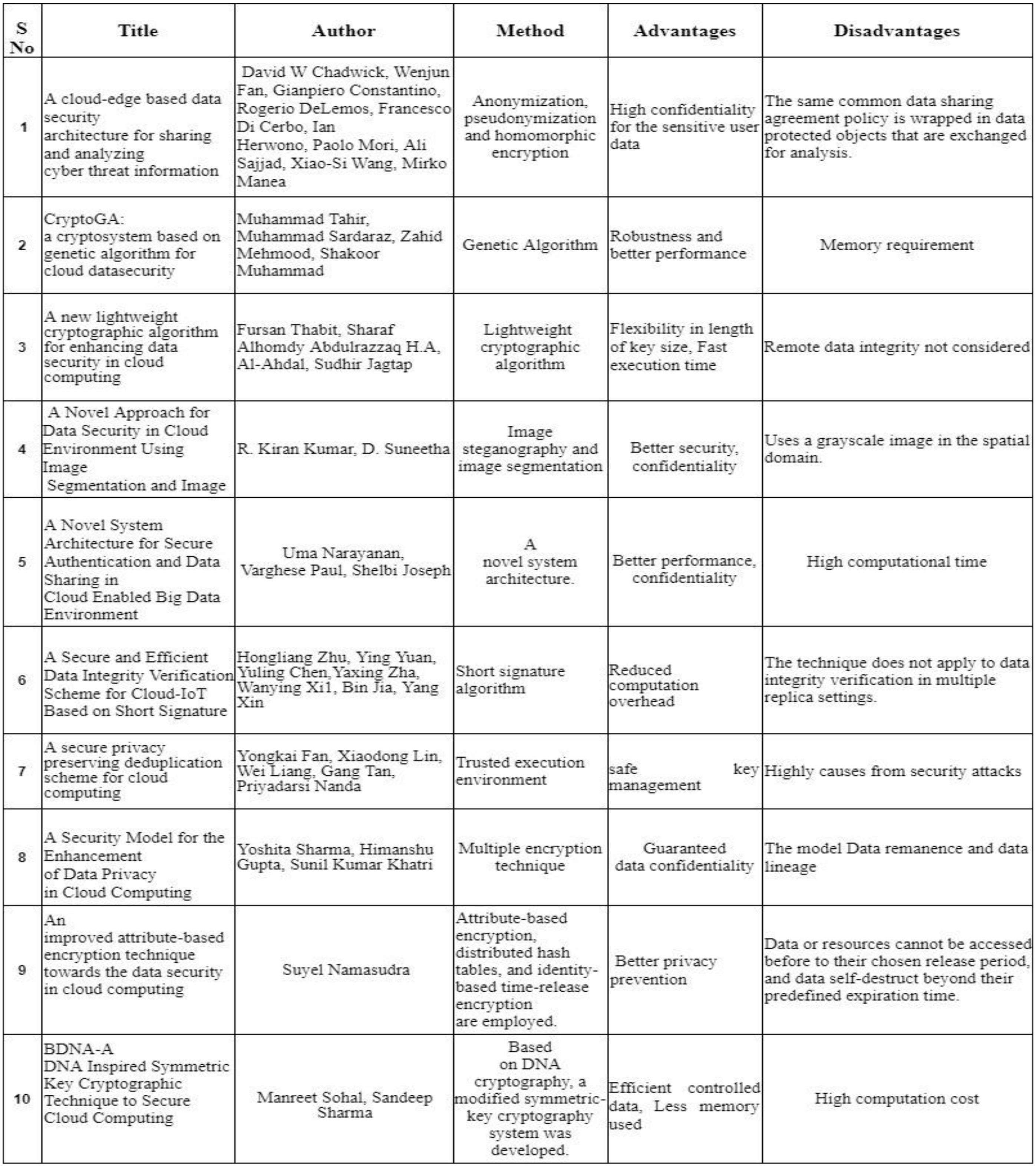
Sharma et al., proposed a security model to improve data privacy in the cloud. They used multiple encryption techniques, emphasizing the importance of data security and privacy protection [8]. They use a secure block cipher, AES and RSA, which provide higher security when storing data. The data go through a multi-layer encryption and decryption process, which effectively improves data security. To encrypt data, RSA algorithm is used, which will create the first encryption level for the corresponding file. The AES technique is then utilised in the second part of the encryption process to encrypt the encrypted files from the first stage in order to create the ciphertext. The decryption method is the opposite of the encryption procedure. The presented model includes multi-level encryption that is difficult to crack, because unauthorized users need encryption keys and decryption keys to retrieve data, which will inevitably become a complex undertaking without an effective key that cannot be completed.

The use of multi-level cryptography is projected to provide greater Cloud data security storage than single-level cryptography

Suyel Namasudra suggested a method for securing data in computer accounts using attribute-based encryption. This approach employs Attribute-based Encryption (ABE), Distributed Hash Table Network (DHT), and Identity-based Time Synchronization (IDTRE) encryption [9]. In this case, user characteristics are utilised to encrypt data or resources first, and the encrypted material is separated into encapsulated ciphertext and extracted ciphertext. Then, using the IDTRE technique, encrypt the decryption key and combine the key's cypher text with the recovered cypher text to generate a public cypher text. Finally, the cypher text is distributed throughout the DHT network, and the wrapped cypher text is kept on the cloud server.

M. Sohal et al. suggested an encryption approach that encrypts data before it is uploaded to the cloud by using data from the client side for encryption. It has a symmetrical structure multiplex encoding method based on DNA coding [10]. DNA coding has many computational flaws because it requires high-tech laboratories to actually implement the technology. It is impossible to automate the DNA process. DNA synthesis requires manual processing at each stage, this has become a drawback to its overall growth as a result, pseudo-DNA coding approaches have gained popularity to enable address DNA's flaws coding. Its mechanism of action is similar to that of DNA synthesis, but this does not involve having the laboratory synthesis of DNA bases. The method proposed in [10] is a pseudo-DNA technique, which is based on the workings of DNA coding, but does not use DNA coding. This method is an algorithm of symmetric key, especially for binary data. They mainly use a random dynamic cipher table, thus improving security.

TABLE III
ANALYSIS OF MODELS AND METHODS USED TO ENHANCE DATA SECURITY SUMMARIZED.



S No	Title	Author	Method	Advantages	Disadvantages
1	A cloud-edge based data security architecture for sharing and analyzing cyber threat information	David W Chadwick, Wenjun Fan, Gianpiero Constantino, Rogerio DeLemos, Francesco Di Cerbo, Ian Herwono, Paolo Mori, Ali Sajjad, Xiao-Si Wang, Mirko Manea	Anonymization, pseudonymization and homomorphic encryption	High confidentiality for the sensitive user data	The same common data sharing agreement policy is wrapped in data protected objects that are exchanged for analysis.
2	CryptoGA: a cryptosystem based on genetic algorithm for cloud datasecurity	Muhammad Tahir, Muhammad Sardaraz, Zahid Mehmood, Shakoor Muhammad	Genetic Algorithm	Robustness and better performance	Memory requirement
3	A new lightweight cryptographic algorithm for enhancing data security in cloud computing	Fursan Thabit, Sharaf Alhomdy Abdulrazzaq H.A, Al-Ahdal, Sudhir Jagtap	Lightweight cryptographic algorithm	Flexibility in length of key size, Fast execution time	Remote data integrity not considered
4	A Novel Approach for Data Security in Cloud Environment Using Image Segmentation and Image	R. Kiran Kumar, D. Suneetha	Image steganography and image segmentation	Better security, confidentiality	Uses a grayscale image in the spatial domain.
5	A Novel System Architecture for Secure Authentication and Data Sharing in Cloud Enabled Big Data Environment	Uma Narayanan, Varghese Paul, Shelbi Joseph	A novel system architecture.	Better performance, confidentiality	High computational time
6	A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature	Hongliang Zhu, Ying Yuan, Yuling Chen,Yaxing Zha, Wanying Xi1, Bin Jia, Yang Xin	Short signature algorithm	Reduced computation overhead	The technique does not apply to data integrity verification in multiple replica settings.
7	A secure privacy preserving deduplication scheme for cloud computing	Yongkai Fan, Xiaodong Lin, Wei Liang, Gang Tan, Priyadarsi Nanda	Trusted execution environment	safe key management	Highly causes from security attacks
8	A Security Model for the Enhancement of Data Privacy in Cloud Computing	Yoshita Sharma, Himanshu Gupta, Sunil Kumar Khatri	Multiple encryption technique	Guaranteed data confidentiality	The model Data remanence and data lineage
9	An improved attribute-based encryption technique towards the data security in cloud computing	Suyel Namasudra	Attribute-based encryption, distributed hash tables, and identity-based time-release encryption are employed.	Better privacy prevention	Data or resources cannot be accessed before to their chosen release period, and data self-destruct beyond their predefined expiration time.
10	BDNA-A DNA Inspired Symmetric Key Cryptographic Technique to Secure Cloud Computing	Manreet Sohal, Sandeep Sharma	Based on DNA cryptography, a modified symmetric-key cryptography system was developed.	Efficient controlled data, Less memory used	High computation cost

Conclusion

There are many benefits for using cloud computing, such as cost efficiency, rapid deployment, and improved availability, but there are still many practical challenges to be resolved. Data privacy is one of them. Cloud computing is a new technology used by many consumers for public storage and data exchange, one of the most important of which is security and privacy. This article analyzes the theoretical analysis of different security concerns of several forms and different issues affecting user data privacy, as well as ways to mitigate security threats that appear in cloud environments in real time. It also discusses ways to solve confidentiality problems. The detailed explanation of these methods summarizes and describes the advantages of different method used in cloud computing environment. The survey discusses the many possible ways around these problems, and discusses various encryption techniques for dealing with security risks. This survey has focused on the different proposed models, schemes and architectures that researchers have used to enhance data security in cloud computing.

Reference

[1] Chadwick, D. W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., ... & Wang, X. S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Generation Computer Systems*, *102*, 710-72

[2] Tahir, M., Sardaraz, M., Mehmood, Z., & Muhammad, S. (2021). CryptoGA: a cryptosystem based on genetic algorithm for cloud data security. *Cluster Computing*, *24*(2), 739-752.

[3] Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), 91-99.

[4] Kiran Kumar, R., & Suneetha, D. (2019). A novel approach for data security in cloud environment using image segmentation and image steganography. In *Information Systems Design and Intelligent Applications* (pp. 75-82). Springer, Singapore.

[5] Narayanan, U., Paul, V., & Joseph, S. (2020). A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. *Journal of King Saud University-Computer and Information Sciences*.

[6] Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B., & Xin, Y. (2019). A secure and efficient data integrity verification scheme for cloud-IoT based on short signature. *IEEE Access*, *7*, 90036-90044.

[7] Fan, Y., Lin, X., Liang, W., Tan, G., & Nanda, P. (2019). A secure privacy preserving deduplication scheme for cloud computing. *Future Generation Computer Systems*, *101*, 127-135.

[8] Sharma, Y., Gupta, H., & Khatri, S. K. (2019, February). A security model for the enhancement of data privacy in cloud computing. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 898-902). IEEE.

[9] Namasudra, S. (2019). An improved attribute-based encryption technique towards the data security in cloud computing. *Concurrency and Computation: Practice and Experience*, *31*(3), e4364.

[10] Sohal, M., & Sharma, S. (2018). BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. *Journal of King Saud University-Computer and Information Sciences*.

[11] Arumugam, K., (2015). Survey of Cloud Security and Privacy. Preservation. *International Journal of Advanced Information in Arts, Science & Management*, *3*(3), 7-12.

[12] Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), 9493-9532.

[13] Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, *102*, 902-911.

[14] Zaraket, C., Hariss, K., Chamoun, M., & Nicolas, T. (2021). Cloud based private data analytic using secure computation over encrypted data. *Journal of King Saud University-Computer and Information Sciences*.

[15] Choudhary, S., & Singh, N. (2020, October). Data Security in Cloud Environment Using Light Weight Secret Key. In *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)* (pp. 79-82). IEEE.

[16] Mayuranathan, M., Murugan, M., & Dhanakoti, V. (2021). Enhanced security in cloud applications using emerging blockchain security algorithm. *Journal of Ambient Intelligence and Humanized Computing*, *12*(7), 6933-6945.

[17] Singh, A., & Sharma, S. (2019). Enhancing Data Security in Cloud Using Split Algorithm, Caesar Cipher, and Vigenere Cipher, Homomorphism Encryption Scheme. In *Emerging Trends in Expert Applications and Security* (pp. 157-166). Springer, Singapore.

[18] Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 1-10.

[19] Kaushik, S., & Gandhi, C. (2019). Ensure hierarchal identity based data security in cloud environment. *International Journal of Cloud Applications and Computing (IJCAC)*, *9*(4), 21-36.