Comparative Analysis of Public Cloud Security Based Schemes and Cryptographic Algorithms

1st G Nagarajan
AssistantProfessor
School of Computing Science and Engineering
Galgotis University
nagarajanite@gmail.com
2nd Dr K.Sampath Kumar
Professor
School of Computing Science and Engineering
Galgotias University
ksampathkumara@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: Cloud computing has been established as the next renewable technology in the IT world. While numerous cloud protection assessments are now prevalent, there is still some disparity between the accurate mapping of problems and their related solutions. Cloud data storage is fast, but the information we store must be safe, and the information stored in the cloud-managed the cloud service providers or the cloud caregiver. The data owner is worried about the integrity and trustworthiness of data stored in the cloud. In this article, a detailed comparative examination of different schemes and "cryptography algorithms" used to protect information over the public cloud will be carried out and provided a clear review of various methods and their limitations in tabular format.

Keywords: Public cloud storage, CIA, cloud system, Cryptographic algorithms, Schemes, NIST

I. INTRODUCTION

Cloud illustrates the idea of a distributed infrastructure containing a collection of virtual computers dynamically supplied to satisfy a customer's particular resource requirements. The SLA (Service Level Agreement) controls the entire context of this cloud-customer partnership [1]. The NIST has been defined as a model of easy internet access over to a customizable computer resource such as servers, records, apps, applications, etc. The cloud is easily distributed, measured and generated with limited downtime or intervention of service providers[2]. Cloud technology has been one of the most changing phenomena and offers multiple services to its clients at low cost. For cloud storage and computer protection, cloud data security is the only challenge solved by implementing the concepts of secrecy, verification, message integrity, non-repudiation, intrusion detection, and efficiency [3].

There are three ways to use cryptography to protect public cloud storage. (1) Symmetric key algorithms and asymmetric key algorithms have been used to transform the original text into ciphertext. (2) Switching original text into ciphertext is possible using replacement techniques where every other character, number, or symbol will replace a direct text character. (3) "The techniques of transposition being used secure the actual document by permutations". Cryptographic algorithms are used to maintain the confidentiality and integrity of public cloud data. Confidentiality means that only the sender and the intended receiver exchange the information. It ensures that the sender requires such techniques, through which the information can be identified only by the recipient and not by any untrusted person. Stored information integrity maintained for data integrity on the cloud infrastructure. Unauthorized users do not have access to misappropriate data or even a mass of viewpoints, and the cloud storage service provider maintains data integrity and data accuracy. Availability ensures that consumers have access to the systems, applications, and information they need. A denial of service, which impedes access to contents, systems, devices, and other network resources, is another common assault on availability.

A. Cloud Computing

The term "Cloud" is used in cloud computing as a cloud service. Today, the computer world has been able to imagine a transition to the cloud computing era thanks to the significant developments in computing and information technology over the past three decades[5]. The advances include the construction of the Internet backbone, the mass implementation of wireless Internet connectivity, a strong network of servers and data center storage, innovations in high-performance and flexible computing technology for data centers and the Web, etc.

According to International Data Corporation (IDC), The profits of cloud computing products, such as a server, public cloud storage, and private cloud, increased by 8.1% year over year to $8.4 billion for the third period of 2016. Public cloud annual growth rate will be seven times the overall IT spending growth and this growth rate will reach $53.1 billion by 2019 and $203.4 billion worldwide. Amazon, Google, in designing the cloud computing platforms and growing the facilities for a vast number of customers, Microsoft and several businesses are going quickly. The success of such companies gives boost to many other companies to step in to the cloud such as MediaTemple, Mosso, Joyent and so on. Cloud computing utilizes three delivery models SaaS, PaaS and IaaS which provide infrastructure, platform, applications and software as a service to the consumers. In SaaS, customers run applications on the infrastructure provided by the cloud service providers. Customer can access these applications using web browsers. The service supply models of PaaS allow the customers to lease their current applications or build or test new ones from hardware, operating systems, store and network. The IaaS provides control to consumers to manage storage, network, and other computing resources to manage arbitrary software.

B. Types of Service Models in Cloud

Cloud service providers provide their services based on three basic models[6]. It consists of "software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS)".

1) Software as a Service (SaaS):

It sometimes referred to as an Application or a Service Cloud. SaaS is the model hosting the software as a service over the Internet to its multiple cloud users. The application accessed via a web browser from a variety of client devices.

2) Platform as a Service (PaaS):

It is a virtual framework that enables applications to be created, deployed, and managed through concepts interconnected with a cloud based architecture. It is a computer platform web-based distribution. CSP is responsible for managing the underlying cloud infrastructure, as well as the network, servers, operating systems or Storage. At the same time users are required to supply certain controls for the application-hosting environment over installed software and possible configuration settings. The PaaS model promises increased safety improvement and consumer access, but less than the IaaS model[37].

3) Infrastructure as a Service (IaaS):

It provides clients with the resources (storage space, server, etc.) as the name suggests, allowing them to have greater leverage of their software development environment. IaaS needs physical capital as well. On the other hand, the vendor addresses all of the device needs related to virtualization, storage, servers, and networking. In plain terms, in the type of operation, infrastructure is given.

II. Cloud Deployment Models

NIST is again split into four implementation models based on the consumer cloud's suitability and exact intent.

Public Cloud: The infrastructure opened to the general public in this kind of cloud. A corporation, educator, government agency, or any combination can control, own, and run it. It helps all people who wish to make use of the resources of computation. Public clouds are used most widely for application development etc.

Private Cloud: It is the type of cloud computing that a single company or many users may utilize (e.g., business units). It may be handled on the premises or off-site by a service provider. They are costly regardless of the investment they are spending on it. They are fantastic for secrecy and authentication. Eucalyptus, VMware, and IBM Cloud Burst are private cloud vendors.

Community Cloud: The cloud should only be accessed by a single user group focused on general concerns (e.g., mission, security requirements, policy, etc.). It can only be used by the group members. It can be searched on or off site[6].

Hybrid Cloud: The cloud framework involves two or three independent cloud networks (private, group, or public) that are uniquely related to structured or proprietary technology (e.g., cloud load-balancing explosion)[6]. Hybrid clouds are inexpensive and scalable as public clouds. In comparison, private cloud security and control are also being tracked. Data security and integrity are problems that affect the hybrid cloud. It is scalable and cost-effective as well. Ex Microsoft, Amazon Online Services, VMware, Government agencies, for example, opt for Private Clouds when classified information is involved. They often use public clouds to store datasets for the general public. Here, we will build a cloud. [6].

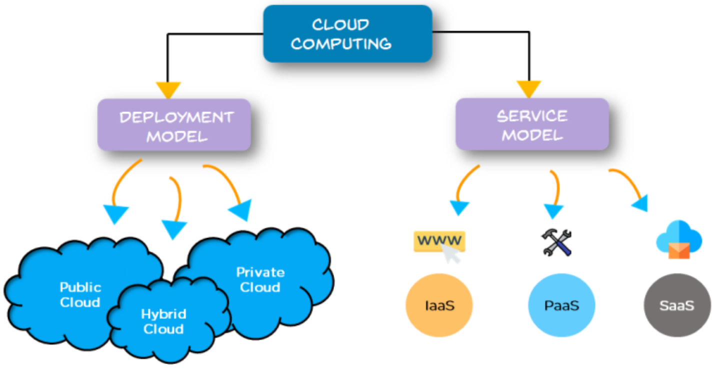

Figure 1: Cloud-computing models

The rest of paper is organized as follows: In Section 3, we review the related work of public cloud security. We classify the security issues/requirements of public cloud storage in Section 4. In Section 5, we discuss the public cloud storage schemes and their security limitations in table form. In Section 6, we analyze cryptographic security algorithm and their strength and weakness. Finally, we summarize and discuss the future work in Section 7.

III. Literature Review

The researches proposed various public cloud security schemes and algorithm to secure data storage with the help of cryptographic concepts. Morea et al., [7] have used eventual methods to secure data in the cloud. They have used AES Algorithm for data privacy, and data audit used TPA. This not specified which type of AES algorithm applied, whether 128bit, 192bit, or 256bit, and they also not specified which types of SHA2 algorithm applied like 224bit, 256bit, or 512bit. Not mentioned how the data split. Meenakshi et al.,[8] They have used Merkle hash tree to audit data in TPA and supports data dynamic operations like insertion, deletion, and update. The proposed approach not maintained privacy but ensured the integrity of data. Batch auditing is not supported. D. Dhaivat et al.,[9] Deliberated cloud deployment models and service models different risks and challenges. They identified problems such as risk multi-tenancy, risk of information encoding, and risk of information exposure depending on the implementation. The risk associated with the service model is data security, network security data integrity.

K. Patel et al., [10] done a reasonable analysis of symmetric algorithms based on Ten lesser file sizes and Ten larger file sizes. The authors conclude based on memory usage and execution time. In terms of execution time, DES is better, and blowfish is better for memory usage. Finally, the authors specified DES is better for a lesser file size. The performance of all algorithms is equal. The cryptographic algorithms have been studied in comparative terms by Advani et al. [11]. The analysis revealed that AES is a strong algorithm of symmetric, RSA is a better asymmetric algorithm, that the differences between blowfish and rock are more fragile and twistedfish are less guarded than AES. Mazhar et al [12] Proposed a technique called protected cloud data sharing that gives secrecy, access management, data sharing without extensive computational encryption, threatened inside protection, and backward access control that uses a trusted reencryption-based cryptographic server to symmetrically encrypt cloud data before putting it in the cloud to guarantee faith. The cluster generated by the cryptographic server is split into two parts to ensure each component is retention by the cryptographic server and by the user in the cluster who wants data access to ensure data integrity. The model has been tested based on time usage for key creation, encryption, and file upload/download.

M. A. Al-Shabi [29] performed a comparison of symmetric and Asymmetric algorithms based on different parameters such as battery usage, processing time, block size, number of iterations, and algorithm strikes. According to the analysis, the AES algorithm takes less time than RSA and the D-H algorithm outperforms it.

Xin et al. [30] suggested a secrecy and efficient data sharing system in cloud computing by integrating Cipher text Law –Attribute Dependent Encryption with the Identity Based Encryption technique. The proposed system guarantees fine-grained shared data management, backward confidentiality, and protection against device collusion with the cloud, as well as user extension, revocation, and attribute updates. The disadvantage discovered is the use of computational overhead requiring pairing processes.

Guiyi et al [31] suggested that data secrecy can be achieved using a system that uses initial pairing secure, private, and multi - directional proxy re-encryption. Data are protected utilising symmetric key encryption, and the keys for symmetric encryption are explicitly encrypted using the suggested proxy reencryption process, ensuring the anonymity of the data sharer without the need for a fully-trusted group. The scheme has little impact on the data holder's workload.

Mohta et al. [33] are looking for a way to protect cloud data in the public audit systems used in the work suggested. Data security and data auditing are used in their solution by the RSA algorithm. You used the SHA algorithm to digest the post. You did not specify which RSA edition (1024,2048,3072,15360). Data dynamics, including convergence, elimination, and upgrading, are also clarified.

Zhu et al. [34, 35] proposed dynamic cloud-based audit services. They used the nominal framework to decrease the storing of signatures, used index hash tables continue providing complex data processing service and used regular sample audits to improve information completeness. Wang et al. [40, 41] have developed a scheme called Panda that will verify the integrity of shared information in the cloud by revoking users. The proxy resignation was used by the revoked user to change their signed results.

Li et al. [42] found the resource-restricted device of the customer to be straightforward and lightweight. Consequently, a client suggested the scheme to assign TPA to run high-end computer and overcome the bottleneck of the client prior to transferring data from the user to the cloud server.

Erway et al.[43] suggested a complex, evidence-based data ownership applying to entirely dynamical data the PDP model. You need another authenticated data structure to prove and update them remotely stored data using authenticated skip lists from ranks. Their scheme cannot, however, accept public authentication, since only dynamic data are achieved.

IV. SECURITY ISSUES/REQUIREMENTS IN PUBLIC CLOUD STORAGE

Cloud computing faces two main challenges Security and Reliability. As client's data can be accessed by any other client in cloud, this arises security issues in cloud. Hackers could attempt to steal client data by authenticate using authorized user name and password and can modify the data and make changes. So many techniques are available to achieve security in cloud such as Encryption, Authorization, and Authentication. Cloud security risks can be categorized in to cloud user and cloud service provider. Some of the cloud security risks are Data leakage, Data breaches and loss, Hacking, Denial of Service, malicious insiders attack, and some shared technology issues. Authentication, authorization, data protection etc., are some of the security aspects that cloud service provider must cover and basic security goals that needs to constitute as basic security principles and it became more crucial as data move to cloud.

Trust of the cloud service provider (CSP) and its services is among the principal drivers of a customer deciding to migrate to a cloud platform or conform to the legacy framework. Trust relies upon deciding whether the provider is responsible for all risks such as data protection, VM security, and other regulatory and regulatory concerns. "Confidentiality, Integrity and availability" are the three considerations considered during the cloud system security review (CIA). This section's primary objective is to generalize security requirements for the modern cloud infrastructure since the CIA domain is the commonly used method for defining security vulnerabilities in the conventional information system.

A. Confidentiality and Privacy

The security of some business properties from exposing unauthorized users implies secrecy. In a cloud world, consumers like unauthorized access to data stored in the same database as the CSP data may be clients. The CSP itself can even include unethical or nefarious representatives who may access or even tamper with confidential, sensitive consumer data. Besides client info, the network of virtual computers, virtual picture, etc. ultimately need secrecy.

Certain confidentiality concerns related to cloud data include:

1. A variety of cloud storage services send content to customer data-containing web folders.
2. Another aspect that impacts data security is the whole geographical area of the client's information [13].

Cloud service services are believed to be reliable but odd in some cases. They want to hear more about the details of personal data files and user privilege data. They want to hear more about the contents of user data files and user privilege data. Appropriate access management procedures should be formulated by the owners to prevent specific scenarios.

B. Integrity

Integrity applies to an asset's security property that ensures that it has not been changed by third-party employees who are not allowed to do so. Consequently, the accuracy and correctness of the asset concerning its owner are ensured by this property. Typically, inserting, removing or modifying operations is assumed to alter the integrity of any support. With the user accessing Cloud resources through web browsers, all web attacks in the Cloud environment are widespread, causing user file contents, database, virtualized storage or indeed WSDL files to be changed [39].

The following problems of data security were addressed here under the separate integrity specifications of the public cloud:

Data outsourcing: The outsourcing of data at the CSP end constitutes a direct challenge to its credibility. CSP will be able to erase any legitimate consumer data tuples, which the customer could never create. [14].

Insecure API: The web developer has used the insecure API from Obscure sources for a lot of time, where the API key can leak to the attacker.

Collision Attack: A collision attack is an operation that can merge several copies of media or other files to create a new copy. The tasks that include, but are not limited to, are data averaging, substitution, linear data mix, etc.

Wrapping attack: is another common network attack that is naturally extremely likely to occur for cloud systems. The text and signature is duplicated and sent to the server as an authentic user during SOAP translation in TLS (Transport Layer service) layer[15].

C. Availability

Demand is one of the most critical protection factors to be maintained by a CSP. Multiple business organizations who utilize cloud-based technology to support their consumers should guarantee that these services remain available as a minor downtime will result in a significant irrecoverable financial loss. A standard service-level agreement lays out what the supplier has promised to supply and respond to demand. For, e.g., the service level could state that 99.999 per cent of the time, if more than 80% of the support given is used, the programs will be utilizable, and more resources will be dynamically available.

Date	**Organization**	**Issue**
Oct-07	Salesforce.com	Attack on phishing and client list leaked.
Mar-09	Google	Flaw exchanges consumer information in Google Docs unintentionally
Mar-09	Epic.com	FTC complain about its policies in terms of privacy
Jun-12	Amazon	Amazon web services downtime
Sep-12	T-Mobile	Unauthorized Party access
Dec-13	Excellus	Data Breach
Mar-15	Premera	Data Breach
Jun-15	Kaspersky	Data Breach affected multiple customer
Nov-15	Vtech	Information exposed including accounts, Encrypted passwords, etc
May-17	Ransomware/ WannaCry attack	locks down all the files on infected computer and ask computers to pay to regain control

Table1. Security and privacy issues

V. Summary of Reviewed Schemes Based on Public Cloud Security

In this segment, presented mentioned research paper in table based on confidentiality and integrity of public cloud storage proposed by various authors.

Paper reviewer	**Technique/Schemes**	**Applicable to**	**Limitations**	**Security**
Alexandru Butoi et al.[1]	secret sharing scheme	Hybrid private-public cloud storage	It is not based on data flow monitoring and data replication.	It offers protection for data storage and services in the public cloud.

Yingjie Xue et al.[2]	Attribute-based controlled collaborative access control scheme	Applicable in cases where multiple users access public cloud data.	The performance of the proposed scheme only satisfactory.	Ensures confidentiality of data and resistance to user collusion on public cloud storage.
Jiaojiao Wu et al.[3]	CPDA scheme, convergent encryption and random masking techniques	Data owners audit their own TPA data individually and assist CSP in auditing the credibility of outsourced files.	The cost of measurement for CSP is not guaranteed.	Confirms the security of cloud data during file deduplication and data audit process integrity using convergent encryption and random masking techniques.
Thangavel M et al.[4]	A novel integrity verification framework based on Ternary Hash Tree(THT) and R-THT	Applicable for cloud data auditing with TPA.	Limitation of exchange of data within the user community.	Data privacy and data usability of cloud data have been checked by the proposed system.
Hendrik Graupne et al.[5]	Asymmetric convergent Encryption, partition sensitivity detection,	Enhance their Cloud RAID Multi-Cloud Broker System.	Observed deduplication rates of up to 69.83 per cent.	Minimizing the risk of breach of confidentiality of data and maximizing the use of public cloud storage.

HAL marwani, R et al.[6]	Tagging of Outsourced Data(TOD) method	Checks the authenticity of TPA results.	TOD approach is based on current methods of spot-checking.	Tackle the concerns of how TPA-managed data accuracy can be reviewed.
Yan Xu et al. [7]	Intrusion-resilient system of public cloud auditing.	Notify authenticators for auditing to prevent malicious file tampering.	If the consumer and TPA are corrupted over various time spans, an adversary may acquire an auditing hidden key.	Secure client and TPA by compromising the same period of time.

VI. COMPARATIVE ANALYSIS OF CRYPTORGRAPHIC SECURITY ALGORITHMS

Comparing various cryptographic algorithms to protect cloud data is shown in Table 02 based on different analytical parameters [16]. The key size, block size, round number, time of the run, the key used, and memory usage are the parameters considered. The advantages and disadvantages also indicated. There are both benefits and drawbacks.

Advanced Encryption Algorithm is essential for personal digital information, cyber-security and govt computer privacy. The U.S. government has developed and introduced AES to protect sensitive information. The tiny Blowfish block size (64 bits) is more vulnerable than the 128 bits used by AES for birthday attacks [17]. On various file formats such as “image, audio, video, text, document, and portable document format”, the AES algorithm tested [18, 38], and the result has proved to be stable.

Algorithms / Parameters	**AES**	**RSA**	**Blowfish**	**IDEA**	**DES**
Key used	Encryption and Decryption same key used.	Two keys, one for encryption and one for decryption, were	Encryption and Decryption same key used.	Encryption and Decryption same key used.	Encryption and Decryption same key used.

		used.			
Execution Time	Rapid	Slowest	Fast	Slow	Same as AES
Data encryption Capacity	Large quantity of data	Tiny data	Lower than AES	Tiny data	Less than AES
Security	Strong	Considered to be safe	Considered secure	Inarticulate	Inarticulate
Key size	128, 192 or 256 bits	>than 1024 bits	32-448bits	128 Bits	56 bits out of 64 bits
Block size	128,192 or 256bits	Irregularity	64bits	64bits	64bits
Rounds	10, 12 or 14 depending on key size	1	16	8.5	16
Encryption Type	Symmetric	Asymmetric	Symmetric	Symmetric	Symmetric
Benefits	Most reliable, less memory, more powerful key size, Good speed and time	Probably easier to share your public key.	Less memory, Good speed,	Complex rounds, large key size	Low encryption time, Good power consumption and It was throughput.

Drawbacks/Limitations	Brute force attack, The implementation of the software is complicated.	Challenged by man-in-the-middle attack.	Throuhput, key management	There have been so many activities.	initial and final permutation not clear

Table 2: Comparison between various cryptographic Algorithm

Each of the already mentioned encryption algorithms has a strengths and weaknesses point that has its own. The following parameters are being selected to evaluate the success of different encryption algorithms.
Encryption time, Decryption time
Avalanche effect, Memory consumption

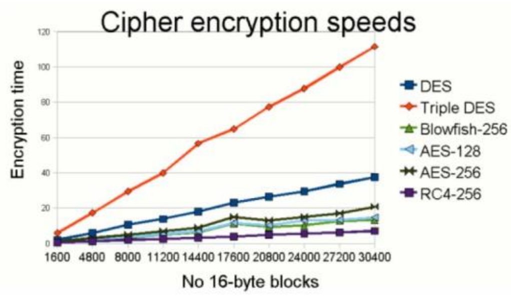

Figure 2: Encryption time Versus Plaintext of multiple symmetric encoding algorithms of different sizes [32]

Figure 2 shows the overall of [32] which indicate different algorithm encryption times.
In addition, RSA uses the highest quantity of memory and blowfish absorbs the minimum for device usage. The table 03 shows the memory for mentioned algorithms process units.

Algorithm	**Memory consumed (KB)**
DES	18.4
3DES	20.5
AES	14.7
Blowfish	9.40
RSA	30.50

Table 3: Memory consumed units operation

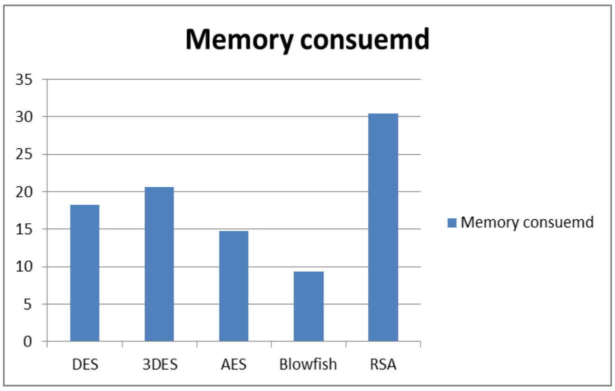

Figure 3: Memory consumed by cryptographic algorithm

The avalanche effect is another measurement parameter we have chosen. The power of every encryption algorithm is often told in cryptography diffusion. An ASCII value in plain text and ciphertext can be used to identify the difference between the source (plain text) and the output (chip text) calculated with the distance from Hamming and convert them to binary and XOR. The algorithm with more than one after XOR is known to have a strong avalanche effect.

Hamming Distance= (Binary representation of ASCII value of each character of Plain text) XOR (Binaryrepresentation of ASCII value of each character of Cipher text)

Avalanche effect= (Hamm Distance / document leenght)

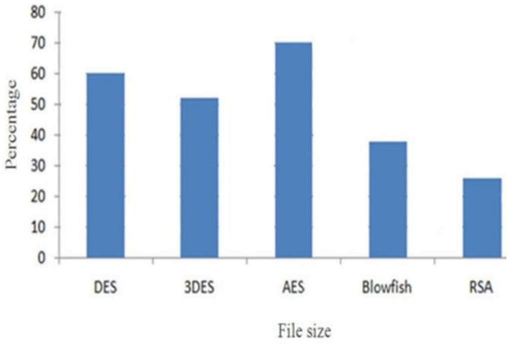

Fig.4 Shows that AES has highest Avalanche effect whereas RSA shows least Avalanche effect[44].

VII. CONCLUSION

Cloud computing has developed as a major area of research. Cloud offers users a lot of advantages by offering services such as pay-per-use, cost-effective services, and fast internet connectivity. Cloud has an immense opportunity, but many users still do not embrace clouds because of the transparent problems that have not yet been addressed. While several solutions were given by the authors, one solution did not solve all the problems. Several authors have identified a range of security risks and concerns such as data leakage, loss of data, insecure API, collusion attack, wrapping attacks, unidentified risk profile, and many more as a major obstacle stopping users from embracing cloud data security. Another big challenge is trust, as service providers frequently hack and leak sensitive data with malicious agents and losing their reputation. To maintain the confidentiality and integrity of data the cryptography algorithms are used. Several schemes and encryption methods are used to avoid internal and external threats and secure privacy and user data. This paper discusses a variety of public cloud security problems and explains the encryption algorithm and schemes used by authors in tabular format. The comparative analysis halt that symmetric algorithms are further powerful and reliable. AES and Blowfish algorithm require fewer encoding time and less memory consumption than other algorithms shown in table 3. Alternative enhancements for the security of the public cloud will continue as future work.

VIII. References

1. Buyya, R., Yeo, C., Venugopal, S., Broberg, J. and Brandic, I., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), pp.599-616.
2. P.Mell and T.Grance,"The NIST definition of cloud computing",National Institute of Standards and Technology,Tech. Rep.,2009.
3. Binita Thakkar, 2020. A Survey for Comparative Analysis of various Cryptographic Algorithms used to Secure Data on Cloud. International Journal of Engineering Research and, V9(08).
4. Popli, M. and Deep, G., 2018. A Critical Analysis on Cloud Security. International Conference on Innovations in Computing (ICIC 2018), pp:19-23.
5. Kim, W., 2009. Cloud Computing: Today and Tomorrow. The Journal of Object Technology, 8(1), p.65.
6. Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011) "Introduction to Cloud Computing". Cloud Computing : Principles and Paradigms. New York, USA: Wiley Press.pp.1–44.ISBN978-0-470-88799-8.
7. 7 More, S. and Chaudhari, S., 2016. Third Party Public Auditing Scheme for Cloud Storage. Procedia Computer Science, 79, pp.69-76.
8. 8 Meenakshi, I.K. and George, S., 2014. Cloud server storage security using TPA. International Journal of Advanced Research in Computer Science & Technology (IJARCST).
9. 9 Dave, D., Meruliya, N., Gajjar, T.D., Ghoda, G.T., Parekh, D.H. and Sridaran, R., 2018. Cloud security issues and challenges. In Big Data Analytics (pp. 499-514). Springer, Singapore.
10. 10 Patel, K., 2019. Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. International Journal of Information Technology, 11(4), pp.813-819.
11. 11 Advani, N., Rathod, C. and Gonsai, A.M., 2019. Comparative study of various cryptographic algorithms used for text, image, and video. In Emerging Trends in Expert Applications and Security (pp. 393-399). Springer, Singapore.
12. 12 Ali, M., Dhamotharan, R., Khan, E., Khan, S., Vasilakos, A., Li, K. and Zomaya, A., 2017. SeDaSC: Secure Data Sharing in Clouds. IEEE Systems Journal, 11(2), pp.395-404.
13. 13 Journal of E-Governance, 2011. Guidelines on Security and Privacy in Public Cloud Computing. 34(3), pp.149-151.
14. 14 Berger, S., Cáceres, R., Pendarakis, D., Sailer, R., Valdez, E., Perez, R., Schildhauer, W. and Srinivasan, D., 2008. TVDc. ACM SIGOPS Operating Systems Review, 42(1), pp.40-47.
15. 15 Ashokkumar, S., Karuppasamy, K., Srinivasan, B. and Balasubramanian, V., 2010. Parallel Key Encryption for CBC And Interleaved CBC. International Journal of Computer Applications, 2(1), pp.21-25.
16. 16 W. Stallings, Cryptography and Network Security Principles and Practices, 4th edition. Prentice Hall, 2005.
17. 17 NIST, "What is AES Encryption and How Does it Work?," Searchsecurity.techtarget.com. https://searchsecurity.techtarget.com/definition/AdvancedEncryption-Standard (accessed Aug. 07, 2020).
18. 18 Janakiraman, K., Baghyasree, T. and Parkavi, D., 2016. Highly secure data transmission for industrial network using blowfish algorithm in embedded processors. International Journal of Advanced Intelligence Paradigms, 8(2), p.168.
19. 19 ALmarwani, R., Zhang, N. and Garside, J., 2020. An effective, secure and efficient tagging method for integrity protection of outsourced data in a public cloud storage. PLOS ONE, 15(11), p.e0241236.
20. 20 Xue, Y., Xue, K., Gai, N., Hong, J., Wei, D. and Hong, P., 2019. An Attribute-Based Controlled Collaborative Access Control Scheme for Public Cloud Storage. IEEE Transactions on Information Forensics and Security, 14(11), pp.2927-2942.
21. 21 Wu, J., Li, Y., Wang, T. and Ding, Y., 2019. CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing. IEEE Access, 7, pp.160482-160497.

22. 22 Thangavel, M. and Varalakshmi, P., 2020. Enabling Ternary Hash Tree Based Integrity Verification for Secure Cloud Data Storage. IEEE Transactions on Knowledge and Data Engineering, 32(12), pp.2351-2362.
23. 23 Graupner, H., Torkura, K., Sukmana, M. and Meinel, C., 2019. Secure Deduplication on Public Cloud Storage. Proceedings of the 2019 4th International Conference on Big Data and Computing - ICBDC 2019,.
24. 24 Xu, Y., Sun, S., Cui, J. and Zhong, H., 2020. Intrusion-resilient public cloud auditing scheme with authenticator update. Information Sciences, 512, pp.616-628.
25. 25 Nagarajan, G. and Kumar, K.S.,”A Security Risk on Data Storage in Cloud based System–Survey”. International Journal on Emerging Technologies 10(2): 195-199(2019).
26. 26 ALmarwani, R., Zhang, N. and Garside, J., 2020. An effective, secure and efficient tagging method for integrity protection of outsourced data in a public cloud storage. PLOS ONE, 15(11), p.e0241236.
27. 27 Popli, M. and Deep, G., 2018. A Critical Analysis on Cloud Security. International Conference on Innovations in Computing (ICIC 2018), pp:19-23
28. 28 Rama Devi, K., Prabakaran, S. An enhanced bilateral information security towards a conventional cryptographic system using DNA sequences. Indian Journal of Science and Technology, 2016, 9(39), 102067.
29. 29 M. A. Al-Shabi, “A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security,” Int. J. Sci. Res. Publ., vol. 9, no. 3, pp. 576–589, 2019, doi: 10.29322/IJSRP.X.X.2018.pXXXX.
30. 30 Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue, and Minglu Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing", Computers & Security, vol. 42, pp. 151-164, 2014.
31. 31 Guiyi Wei, Rongxing Lu, and Jun Shao,"EFADS: Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy reencryption." Journal of Computer and System Sciences 80, no. 8 1549-1562, 2014.
32. 32http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue1/Version-3/L017136269.pdf
33. 33 Abhishek Mohta, Ravi Kant Sahu, Lalit Kumar. “Robust Data Security for Cloud while using Third Party Auditor”. International journal of advanced research in CSE (IJARCSE), Volume 2, Issue 2, February 2012.
34. 34 Z. Yan, et al., “Dynamic audit services for outsourced storages in clouds”, IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227–238, 2013.
35. 35 Liu, C.W., Hsien, W.F., Yang, C.C. and Hwang, M.S., 2016. A Survey of Public Auditing for Shared Data Storage with User Revocation in Cloud Computing. IJ Network Security, 18(4), pp.650-666.
36. 37 Spoorthy, V., Mamatha, M. and Kumar, B.S., 2014. A survey on data storage and security in cloud computing. International Journal of Computer Science and Mobile Computing, 3(6), pp.306-313.
37. 38 Thakkar, B. and Thankachan, B., A Survey for Comparative Analysis of various Cryptographic Algorithms used to Secure Data on Cloud.
38. 39 Singh, P. and Saroj, S.K., 2020, March. A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 695-700). IEEE.
39. 40 W. Boyang, L. Baochun, and L. Baochun, “Public auditing for shared data with efficient user revocation in the cloud”, in Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM’13), pp. 2904–2912, Turin, Italy, Apr. 14-19, 2013.
40. 41 W. Boyang, L. Baochun, and L. Baochun, “Panda: Public auditing for shared data with efficient user revocation in the cloud”, IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92-106, 2015
41. 42 L. Jin, T. Xiao, C. Xiaofeng, D. S. Wong, “An Efficient Proof of Retrievability with Public Auditing in Cloud Computing”, in 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS’13), pp. 93–98, 2013.

42. 43 C. Erway, A. K, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” in Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 213–222, Illinois, USA, 2009.
43. 44 Semwal, P. and Sharma, M.K., 2017, September. Comparative study of different cryptographic algorithms for data security in cloud computing. In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-7). IEEE.