International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST52310246

Comparative Study of Color Image Authentication and Encryption in Cloud

Mamta Khanchandani*[1], Dr. Sanjay Buch[2]
*[1]Research Scholar, Bhagwan Mahavir University, Surat, Gujarat, India
[2]Dean, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India

ARTICLEINFO

Article History:

Accepted: 05 March 2023
Published: 22 March 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
295-301

ABSTRACT

Cloud computing is the provision of computing and storage capacity to users as a service. Cloud storage is a type of networked online storage where data is stored in virtualized storage pools as a subservice of infrastructure as a service (IaaS) in cloud computing. Cloud computing plays a significant role in the efficient use of resources and in the utilization of service. Regardless of the cloud category (e.g., private, public, hybrid or inter-cloud), all service providers rely on domain server data. As a rapid development and deployment of cloud computing and cloud storage, users are increasingly concerned about security and privacy issues involved in these techniques. This paper provides a summary of basic security problems that consist of conventional security issues. It also addresses the additional challenges resulting from the cloud computing paradigm being used by cloud system providers and consumers. In addition, solutions suggested by some researchers are presented with a focus on cryptographic techniques which support secure storage of the cloud.

Keywords: Cloud Computing, Cryptography Techniques, Encryption, Cloud Security, Cloud Storage, Security, Privacy

I. INTRODUCTION

While considered a productive or non-profitable enterprise, the concentrated use of capital increases the economic impact and creates tremendous losses. To address this shortcoming, each consumer is hunting for a new technology to solve their demand with minimal effort. The cloud computing provides an excellent platform over the network for resource seekers in this way. The cloud service providers are not considered by most groups to be the secure way of data processing within the public cloud. Yet, at the same time, private cloud is paying more attention to ensuring that the data remains in its cloud servers as well as keeping sensitive cloud data secure. The general framework for cloud storage consists of two main components, such as data and its applications. Both data and applications are handled with the help of cloud data proprietors and cloud service providers (L, Prateelk, & Singh, 2014).

Cloud computing is an evolving technology but it has drawn significant attention from cloud users and cloud providers to its security and privacy risks. One of the main reasons for this is that cloud users must trust the security mechanisms and configuration of the cloud provider and cloud client themselves. Cryptographic technique is currently being treated in the industry and academia community as one of the primary techniques for solving security and privacy problems in the cloud computing environment. In recent years, many types of cryptography-based cloud computing solutions have been proposed in Ref., focusing primarily on secure storage , secure computing, and secure service usage (Sheik & Komati, 2018).

II. METHODS AND MATERIAL

2.1 Cloud computing security

A. Trust: Trust is described as the "act of trusting and relying on someone or something to behave as promised". In computing science, faith goes through many fields, such as computer network protection and access control, distributed device reliability, etc. The fact that data and software are outsourced in a cloud environment assigns their power to the cloud provider out of the strict owner control. Consequently, Trust is based on both the delivery model and the cloud provider (D & D, 2012)

B. Cloud security issues: Most conventional security issues are effectively countered because of the innovative architecture of cloud computing. However, the unique characteristics of its infrastructure have brought in a range of distinctive security challenges. In general, security is related to the AIC triad, namely, Availability, Integrity, and Privacy. In particular in the case of cloud computing architecture, these three properties have become key aspects used in the design of secure systems.

1) Confidentiality: This only applies to approved parties or systems with the ability to access protected data. Outsourcing data, delegating power to a cloud provider and making it accessible to various parties increases the risk of data breaches. A variety of questions arise concerning multi-tenancy problems, data remanence, security of application and privacy. Multi-tenancy refers to the resource sharing feature in the cloud. The cloud computing architecture consists of sharing different kinds of resources to allow multiple clients to concurrently use the same resource which poses a number of threats to privacy and confidentiality (Cloud Security Alliance, 2010).

2) Integrity: It means that only approved parties may change assets in the manner permitted and refers to data, software and hardware. Data Integrity refers to protecting data against unauthorized deletion, modification or manufacture. Authorization is the system's mechanism to decide what level of access a single authenticated user should have to protected resources. Because of the growing number of parties involved in a cloud environment, authorization is important to ensure the integrity of the data.

3) Availability: This refers to the property of a device that is available and usable by an authorized individual upon request. The availability of the system includes the ability of a system to carry on operations even if certain authorities misbehave [6]. The device has to be able to operate even when there is a security threat to ensure availability. The user of a cloud environment, which is discharged from the requirements of hardware infrastructure, depends on the ubiquitous network available.

2.2 Existing Security Frame Work

For cloud data centres, the most challenging task is the management of residing data under the protection of the private and confidential sectors. Apply encryption on the storage sector and decryption on the authenticated receiving sector to ensure secure data in cloud storage by using a cryptographic method.

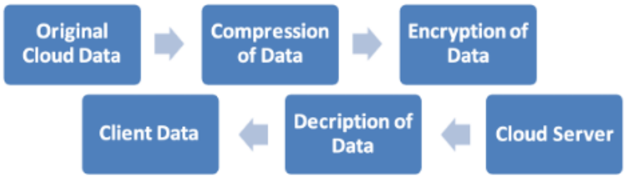

Figure 1 Existing Data Security Model

In most cases, data compression is used to minimize the original size of the data or information, without reducing both its originality and the number of bits.

2.3 Cloud security challenges

Cloud computing is becoming so popular nowadays that it is in the limelight of the present era. Cloud computing, along with its enormous benefits, poses many security issues that need significant attention to be dealt with in order to improve this technology. These are the main concerns listed below (F, 2014);

Outsourcing: Consumers may lose control when outsourcing the data. It takes some sort of appropriate mechanism to prevent the cloud service provider (CSPs) from using the data against their clients ' consent.

Multi tenancy: Cloud is a shared resource pool. Data protection must be considered when providing the multi-tenant environment.

Service Level Agreements: A specific Consumer-Provider contract is required. The main objective of the agreements is to build the confidence.

Heterogeneity: Different cloud providers have different data protection mechanisms which present challenges for integration. vendors should try to keep a minimum of data redundancy.

2.4. Factors Involved in Cloud Security

Various key factors can affect the efficiency of cloud computing because it is surrounded by various technologies such as load balancing, network, competition control, virtualization, operating system, database, memory management, etc. (Qadiree & M, 2016) Figure 2.

Such technologies' security factors affecting cloud computing are important, e.g. network that links the cloud computing to the outside world must be secured. The definition of virtualization must be done safely

Server Downtime: Downtime is the time the machine stops reacting to the customer after a failure of some operation. The downtime should be kept to a minimum and power backups should be installed to minimize downtime.

Backup: In case of any service failure, data uploaded by the customers should be backed up. Cloud Seller should mention, in SLAs, what the remedy or solutions to such problems should be in the event of any disaster. There are very small risks of system wide failure such as flooding etc.

Data Redundancy: Data redundancy is a condition in which two different places carry the same data. In the case of cloud computing, it can be understood as providing the clients with copies of the same data, systems or equipment. Cloud while mapping with the physical systems. Load balancing involves the handling of incoming traffic requests that sometimes overload the server. Algorithms to data mining can be used to deal with malicious attacks.

While cloud computing can be seen as a new phenomenon that is going to revolutionize how we use the Internet, there's a lot to be careful about. Many new technologies are emerging at a rapid rate, each with advances in technology and the potential to make life easier for humans. Several other security issues are present including virtualization security aspects. We assume that attaining end-to-end protection will be difficult due to the complexity of the cloud. The challenge we face, however, is to maintain more stable operations, even when some parts of the cloud fail.

III. LITERATURE REVIEW

Table 1 Literature Reviews

Author	Year of publication	Title	Algorithms/ Methods	Outcome

ABDALBA SIT MOHAMM ED AND NURHAYAT VAROL	2019	A Review Paper On Cryptography	Hash Algorithms	Here the concept of cryptography was discussed with its history and ever-changing need of algorithms and their need in digital security. some historical algorithms were also discussed here like Caesar cipher, simple substitution ciphers, transposition ciphers, stream ciphers and modern hash algorithms
Dr. R.K Gupta	2020	A Review Paper On Concepts Of Cryptograph y And Cryptograph ic Hash Function	DES.RSA, MD5 and SHA	Here we observed different properties, characteristics of different hashing algorithms. we observed DES,RSA,MD family and SHA family. we also observed the basic concept of cryptography and different type of keys used for encryption. Shortcomings or limitations of different algorithms were also discussed here as DES is not viable for encrypting sensitive data while in RSA it is difficult to decide large p and q.Time complexityis high because it is a one by one process
ARADHAN A SAHU AND SAMAREN DRA MOHAN GHOSH	2017	A review paper on secure hash algorithms with its variants	SHA-O,SHA-1,SHA-2,SHA-3	Different secure hash algorithms from the SHA family were compared on different parameters and how they differ from each other in respect of their construction and working was observed. SHA-O,SHA-1,SHA-2,SHA-were compared here.SHA-256 and SHA-512 novel hash algorithms were also discussed here. Working of hash algorithms differ from each other and they work on different principles
PIYUSH 0GARG AND NAMITA TIWARI	2012	Performance Analysis of SHA Algorithms (SHA - 1 and SHA-192): A Review	SHA-160 and SHA-192	Here after comparison between SHA-160 and SHA- 192 it was concluded that they are better in their respective field. SHA-192 is more secure when it was tested against the number of brute force attacks that were needed to break it and SHA-160 was proven to be fast when it was compared with other SHA algorithms
PIYUSH GUPTA AND SANDEEP KUMAR	2014	A Comparative Analysis of SHA and MD5 Algorithm		After doing comparison here it was found that SHA provided more security than MD5 but MD5 was faster than SHA on 32 bit machines
Garima and Naveen [8]	(2014)	"Triple Security of Data in Cloud Computing. "	DSA, AES AND Steganography.	Proposed a system for securing the cloud by using three algorithms: DSA (Digital Signature Algorithm), AES (Advanced Encryption Standard) and Steganography step by step. In order to encrypt the data, DSA is Applied for authentication purpose followed by AES for encryption and then finally concealing data within audio file using Steganography by for utmost security. time complexity is high because it is a one by one process.
RS Bhale et.al	(2016)	“Achieving Cloud Security using Third Party Auditor, MD5 and	MD5	Overcome security tradeoff and improve the performance of data transmission and increase the security MD5 hashes are no longer consider cryptograph by secure.

		Identity-Based Encryption”		
ElGaman and	Sarah and Depali (2016)	“Secure Cloud Auditing over Encrypted Data”	SHA-256	Improve integrity verification strategy for outsourced data. It resolve security issue in implicit cloud by applying cryptography techniques. The security in implicit cloud is provided in three cases. RSA requires more time decryption process.
Punam V Maitri, Aruna Verm	(2016)	“Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm“	AES, RC6, Blowfish	Provide block wise security to data. AES, DES, Blowfish provide low delay for data encode decode but provides low security
.Swathi and Bhaludra	(2017)	Secure file storage in cloud computing using hybrid cryptography Algorithm	Blowfish and SRNN public key	Information Security and protection issues existing all levels in SPI benefit conveyance models. Srnn increases the time performance
Rohini and Er Tejinder Sharma	(201 8)	Proposed hybrid RSA algorithm for cloud computing	RSA AND HMAC	Proposed a framework to alleviate security issues at the level authentication and storage level in cloudcomputing.
Richa S. and Richa D.	(2017)	Hybrid Algorithm for Cloud Data Security	MD5 and AES	Tackle four phases (Registration of Cloud User to Cloud Service Provider), Storing of Data in Cloud Storage, User Authentication on Data Retrieval Request and RETRIEVAL OF DATA AND INTEGRITY VERIFICATION. Uses only one cryptograph hic algorithm and hashing algorithm. And MD5 hashes are no longer consider cryptography secure
Yoshita et.al	(2019)	A Security Model for the enhancement of Data Privacy in cloud Computing	AES AND RSA	Provide multi-level encryption. Data linage and Remanence

IV. RESEARCH GAP

After review of the literature, it is found that to substantiate the augmented security in the cloud storage there is need to derive an ideal authentication scheme and it can be clearly visible that the use of hybrid cryptography is going on increasing day by day. Based on the review the following research gap are identified.

Research Gap 1: User Authentication is being neglected by most of the researchers. Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Authentication is important because it enables individual/organizations to keep their files secure by permitting only authenticated users (or processes) to access its protected resources. Without taking care of the user authentication the intruder using password guessing or other hacking method can easily have access to the un-encrypted data. Adding authentication factors to the authentication process typically improves security. Multi-dimensional encryption is not performed on nonstandard grayscale images and nonstandard color images. then it will be extended to the real-time different sector's image application usage to maintain the image security and privacy on the cloud storage.

Research Gap 2: Most of these researches suffer from practical implementation. The main focus on is the theoretical and partial implementation of the research. The full cloud and programming implementation is neglected.

V. CONCLUSION

Cloud computing is growing as a new trend and many companies and organizations are moving to the cloud, but many of them are lagging behind due to some security issues. Cloud protection is an overarching principle that removes the drawbacks of major MNC, business and organization adoption of the cloud. A lot of encryption algorithms can be used in the cloud. Some of the symmetrical algorithms and some are asymmetrical algorithm. But for cloud computing, that takes care of data security, the security algorithms that allow the linear search on decrypted data are required. In this area of research, there is a large amount of change. In order to secure the web, cryptography can be used in many ways. Crypto graphing, for example, can be used for monitoring cloud access, maintaining cloud data trust, verifiable computing, approving cloud data and authentication. In addition, Cryptography and ID based Cryptography based in Lattice are two key sectors that provide the security of the cloud data in today's world.

VI. REFERENCES

[1]. Cerda, V., Estela, J. M., Forteza, R., Cladera, A., Becerra, E., Altimira, P., & Sitjar, P. (1999). Flow techniques in water analysis. Talanta, 50(4), 695-705.

[2]. Postolache, O., Girao, P., Pereira, M., & Ramos, H. (2002, May). An IR turbidity sensor: Design and application [virtual instrument]. In IMTC/2002. Proceedings of the 19th IEEE Instrumentation and Measurement Technology Conference (IEEE Cat. No. 00CH37276) (Vol. 1, pp. 535-539). IEEE.

[3]. K. Ranjit, and R.P. Singh, "Enhanced cloud computing security and integrity verification via novel encryption techniques," In IEEE Advances in Computing, Communications and Informatics, pp. 1227- 1233, Sep 2014.

[4]. P.V. Maitri, and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," In IEEE International Conference Wireless Communications, Signal Processing and Networking, pp. 1635- 1638,Mar 2016.

[5]. S. Singh, and K. Vinod, "Secured user's authentication and private data storage-access scheme in cloud computing using Elliptic curve cryptography," In IEEE 2nd International Conference on Computing for Sustainable Global Development, pp. 791-795, 2015.

[6]. G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications, vol. 67(19), pp. 33-38, 2013.

[7]. J.D. Bokefode, A.S. Bhise, P.A. Satarkar, and D.G. Modani, "Developing a secure cloud storage system for storing IoT data by applying role based encryption," Procedia Computer Science, vol. 89,pp. 43-50, Jan 2016.

[8]. Tirthani, Neha, and R. Ganesan. "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography." IACR Cryptology ePrint Archive 2014 (2014): 49.

[9]. G.P. Kanna, and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," In IEEE International Conference on Electrical, Electronics, and Optimization Techniques, pp. 3688-3693, 2016.

[10]. H. Tange, and B. Andersen, "Attacks and Countermeasures on AES and ECC," In IEEE 16th International Symposium on Wireless Personal Multimedia Communications, pp. 1-5, June 2013.

[11]. Tong A, Zhang M, Wang Z,Ma J (2016) A joint color image encryption and compression scheme based on hyper-chaotic system. J Nonlinear Dyn 84(4):2333–2356

[12]. S. Garima, and S. Naveen. "Triple Security of Data in Cloud computing". International Journal of Computer Science and Information Technologies. 5(4), 2014

[13]. P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm", International Conference on Wireless Communications, Signal Processing and Networking pp. 1635-1638. doi:10.1109/WiSPNET.2016.7566416,2016.

[14]. Y. Sharma, H. Gupta & S.K Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing", Amity International Conference on Artificial Intelligence pp.898-902. doi:10.1109/AICAI.2019.8701398, 2019.

[15]. B. Swathi, S.D Bhaludra, S. Raveendranadh, "Secure File Storage In Cloud Computing Using Hybrid Cryptography Algorithm", International Journal of Advance Research in Science and Engineering 6(11), 2017.

[16]. Abdalbasit Mohammed, Nurhayat Varol.2019. A review paper on cryptography. DOI:10.1109/ISDFS.2019.8757514,.

[17]. Dr. RK. Gupta. 2020 . A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function. European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 07, Issue 07, 2020.

[18]. Aradhana sahu, Samarendra Mohan Ghosh.2017.A review paper on secure hash algorithms with its variants https://www.researchgate.net/publication/326009898_Review_Paper_on_Secure_Hash_Algorithm_With_Its_Variants.

[19]. Piyush Garg, Namita Tiwari. 2012. Performance Analysis of SHA Algorithms (SHA -1 and SHA-192):A Review . http://www.ijctee.org/.

[20]. Piyush Gupta and Sandeep Kumar. 2014. A Comparative Analysis of SHA and MD5 Algorithm. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 4492-4495.

[21]. ALGORITHM SHA-512. Jai Verma*1, Md Shahrukh*2, Mukul Krishna*3, Ruchi Goel*4. *1,2,3,4MAIT Department Of Computer Science Engineering, Delhi, India..

[22]. Li, H., Yu, C. & Wang, X. A novel 1D chaotic system for image encryption, authentication and compression in cloud. Multimed Tools Appl 80, 8721–8758 (2021). https://doi.org/10.1007/s11042-020-10117-y

Cite this article as :

Mamta Khanchandani, Dr. Sanjay Buch, "Comparative Study of Color Image Authentication and Encryption in Cloud", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 2, pp. 295-301, March-April 2023. Available at doi : https://doi.org/10.32628/IJSRST52310246
Journal URL : https://ijsrst.com/IJSRST52310246