SECURING DATA PRIVACY IN CLOUD NETWORK SYSTEMS: A COMPARATIVE STUDY OF ENCRYPTION TECHNIQUES

[1]Chaitanya Kanth Tummalachervu
[1]RingCental Inc, Denver, Colorado, United States
[1]Tummalachervu@gmail.com

Abstract: This research presents a novel and efficient public key cryptosystem known as the Enhanced Schmidt Samoa (ESS) cryptosystem, proposed to safeguard the data of a single owner in cloud computing environments. Data storage is a one-time process in the cloud, while data retrieval is a frequent operation. Experimental results demonstrate that the ESS cryptosystem offers robust data confidentiality in the cloud, surpassing the security provided by traditional cryptosystems. The research also introduces a secure cloud framework designed to accommodate both individuals and organizations accessing applications and data in the cloud. While individual users may generate and share data, organizations often involve multiple users in data sharing to support their business processes. In these scenarios, multi-user data ownership and access management become critical, requiring secure sharing of cryptographic keys among the authorized users. To address these issues and ensure data confidentiality in multi-user cloud environments, the Improved Secure Cloud Data Storage Framework (ISCDSF) is introduced. This research not only enhances data security but also provides a comprehensive framework for secure data sharing in the cloud, catering to the needs of both individual users and organizations.

Key words: Data security, Cloud computing, Encryption techniques, Comparative analysis, Key management.

Introduction:

Cloud computing offers end users and IT organizations large-scale data storage with suitable remote access. In most personal and business contexts, there is a single owner context. You won't disclose your private information, photographs, videos, or documents with any other user. No personnel will be given access to confidential business documents, personnel information, or sensitive data. In a situation when there is only one owner, maintaining data privacy is crucial. The main problem with cloud storage, though, is that the

Corresponding Author: *Chaitanya Kanth Tummalachervu*
RingCentral Inc, Denver, Colorado, United States
Mail: tummalachervu@gmail.com

data cannot be administered by a single owner, or individual. Rather, the administrative controls over the data will be held by the Cloud Service Provider (CSP)[1]. Issues with data security, such as loss of confidentiality and illegal access, are highlighted by this situation. As a result, a secure framework is required to safeguard private and corporate information. A cloud service provider will assume accountability for data security in the event that a suitable framework is put in place, replacing a single owner.Privacy is one of the most important things. Significantly, sensitive personal data and documents belonging to a single owner must be protected when it comes to privacy. Upon obtaining sensitive data information, an intruder may encounter multiple issues. This information can only be encoded using a straight forward way[2] . The majority of the current queries, which do not employ encoded data, make this assignment perplexing.Using a cryptographic encryption system, cloud data capacity can keep up with its confidentiality. There are two sorts of cryptography: public key cryptography and shared key cryptography. For safe data transmission and capacity, remarkable cloud service providers (CSPs) like Google, Amazon, and Microsoft use the business standard Undeniable level Encryption Standard (AES). AES, which has a 256-bit key length, is used to shield data from unwanted accessAggressors can get the accreditations and keys expected to access cloud data accepting they sort out some way to infiltrate the CSP.Investigators' employment of public key cryptosystems is a calculated move toward ensuring the security of private information under their control[3] . Crucial to this endeavor is public key cryptography, a type of cryptography that makes use of number-theoretic ideas like discrete logarithms and factorization. safe cloud data storage and recovery, as well as safe sender-receiver communication, are two important use cases for this approach, which makes use of two separate keys: the public key and the private key.Public key cryptography is used in the context of cloud data storage and recovery to ensure that data is encrypted and safe from prying eyes both in transit and at rest within the cloud architecture. With this configuration, data can be securely transmitted to the cloud while both the Single Owner (SO) and the Cloud Service Provider (CSP) have access to the public key. The data is encrypted, and only the SO has access to the private key necessary to decrypt it. If an adversary has access to the encrypted data or intercepts the transmission, they will still be unable to decrypt the information without the private key.

Securing Single Owner Cloud Data Using Proposed Enhanced Schmidt Samoa Cryptosystem:

The Schmidt Samoa cryptosystem's concerns are the primary focal point of the proposed ESS approach. General society and confidential keys created by ESS are produced utilizing four different indivisible numbers. The ESS framework is introduced utilizing four enormous indivisible numbers rather than two huge indivisible numbers,which expands the trouble level of savage power assaults and the time complexity of whole number factorization. Within the ESS cryptosystem are five modules:i.ESS_Keygen() -key generation

module is used to generate Public and Private Keysii.ESS_Encrypt_X() -encryption module, if public key is {N,X}iii.ESS_Encrypt_Y() -encryption module, if public key is {N,Y}iv.ESS_Decrypt_X() -decryption module, if public key is {N,X}v.ESS_Decrypt_Y() -decryption module, if public key is {N,Y}In order to facilitate communication or access to resources in the cloud, the key must be generated once and used for encryption or decryption as frequently as feasible. Figure 1 displays the suggested architecture for protecting data belonging to a single owner[11].The critical matches —a public key and a confidential key —are produced by a solitary proprietor. The data should be scrambled and kept on cloud capacity by a solitary proprietor. Subsequent to getting the ciphertext from the cloud, a solitary proprietorwill translate the data as indicated by the need.Figure 1 Suggested Framework for Ensuring the Security of Single Owner (SO) Data1.4.1.ESS Key Generation AlgorithmAlgorithm 3.2 presents the suggested ESS key creation (ESS_Keygen()) algorithm for single owner cloud data. It utilizes four huge prime numbers: p, q, r, and s. It has been determined that the least common multiplier is L between (p-1), (q-1), and M between (r-1), (s-1). Multiply p, q by X and r, s by Y to get the two prime numbers. The requirement that the greatest common divisors of X, L, and Y, M be 1 is required. Finding X mod L's multiplicative inverse yields the value of X'. Similar to this, Y mod M'smultiplicative inverse is found in order to calculate Y'. To find Z's value, multiply X' and Y' together.Since Z and L have exactly one common divisor, we may calculate N as the residual after dividing by L, and then find the multiplicative inverse of N modulo L, denoted by d. Therefore, N and X stand for the public keys, and d for the private one. If Z and Mhave the same greatest common divisor, then the process is repeated to find d, the multiplicative inverse of N modulo M. This is done in the same way as when Z and M have different greatest common divisors[12]. As a result, we set up the public keys as N and Y and keep the secret key as d. Due to the uncertainty of L and M, attempts to compromise the private key will include breaking the public key cryptosystem

Performance Analysis -Variable file size:

Performance evaluation of the ESS (Enhanced Schmidt Samoa) cryptosystem was performed on an owner's cloud data, analyzing its effectiveness for different input file sizes. The study compares the encryption and decryption execution times of the ESS encryption system with the traditional Schmidt Samoa (SS) encryption system, which uses a consistent key size of 32 bits. Here, compares the durations of two different cryptographic systems in the setting of single-owner cloud data; these are the Schmidt Cryptosystem Samoa (SS) and the Enhanced Schmidt Cryptosystem Samoa (ESS). The SS system uses a simpler set of key values (p=73529) whereas the ESS system employs a more complex set (p=73529) that also includes r=73553, s=73561, N=2391448019, and d=1564100563. Cloud computing settings place a premium on data safety and privacy, therefore these cryptographic methods are essential for assuring secure data transfer and storage.The private key (d), which is used both for encryption and decryption, is also calculated. There is a need for additional

improvements to SS's robustness and scalability because its relatively simple key structure may limit its power to handle increasingly sophisticated security challenges and larger data collections.In order to overcome some of the shortcomings of the SS system, the Enhanced Schmidt Cryptosystem Samoa (ESS) employs a more complex key configuration by adding two more prime numbers (r and s) to the already present p and q. This expansion of the key space helps to improve the encryption process's security and resilience by making it harder for adversaries to break into the system via mathematical assaults or brute force techniques. More importantly for the arena of secure cloud data management, the biggermodulus N and private key (d) in the ESS system indicate an increased capacity to handle larger datasets and increased security demands. This table includes detailed data on the duration of the encoding and decoding processes in these specific configurations, providing insight into potential performance differences between the two encoding systems in the field. Cloud data security.

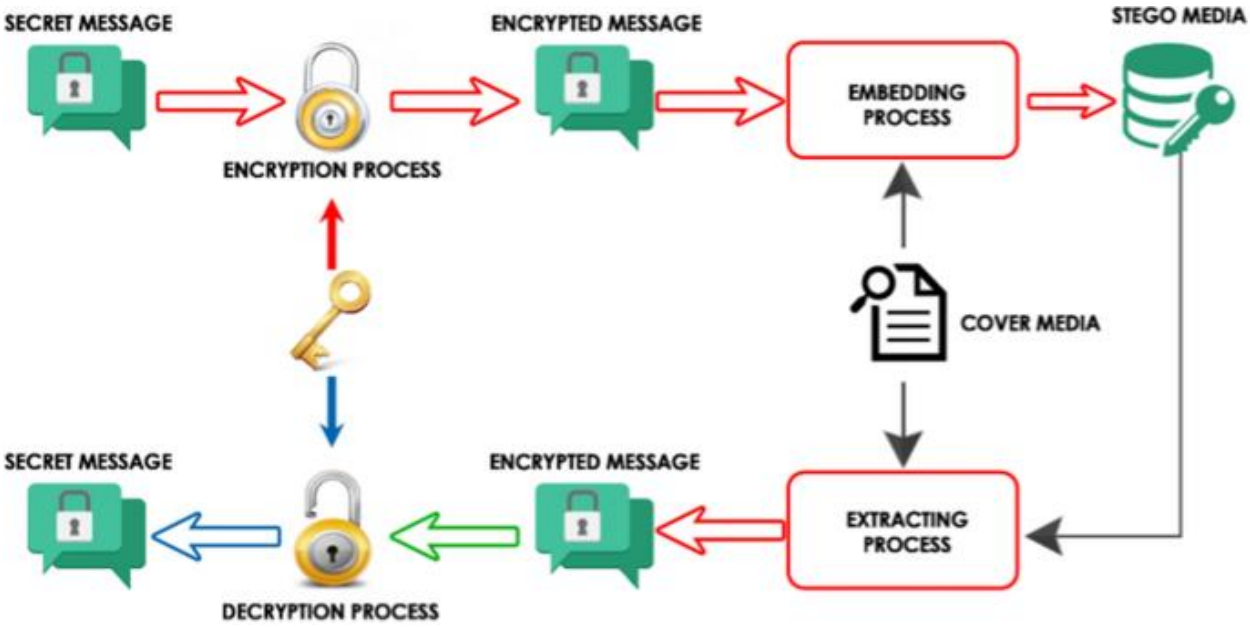

Fig.1. Enhancing Data Security of Cloud Based LMS:

Brute force Attack:

A brute power assault is a broadly utilized classic cryptanalysis method. The objective of the assault is to interpret the given ciphertext by endeavoring each possible blend of keys. This approach gives the time expected to think twice about cryptosystem.How long it takes an interloper to break the cryptosystem concludes how secure it is. The algorithm's most significant strength is that it gives breaks additional time. The ESS takes additional opportunity to break the key than other cryptanalysis systemssince it looks for every conceivable mix of the key. The vital size of the RSA, Paillier, and Schmidt-Samoa cryptosystems is exclusively subject to the two prime qualities, p and q. In any case, in

the better Schmidt Samoa cryptosystem, p and q (or r and s) are the two prime qualities that decide the key size. Thus, tracking down p and q (or) r and s gives off an impression of being a difficult part of the interruption in the ESS cryptosystem.The correlation of brute power assault times for single proprietor cloud data with various key sizes of 16, 32, 64, 128 and 256 bits and fixed plaintext document size of 512 MB is displayed. The data was gotten from the SS, Paillier, RSA, andESS cryptosystems. Seconds (s) have been utilized to gauge the length. The chart makes it apparent that Enhanced Schmidt Samoa demands more investment to finish cryptanalysis than RSA, Paillier, and Schmidt-Samoa. Subsequently, it is trying for an assailant to break the key, and ESS has been demonstrated to be an all the more remarkable algorithm.

Integer Factorization:

Number factorization, or reducing a composite number to its indivisible prime elements, is a central topic in number theory. Several encryption and decryption techniques are based on this process, making it crucial in the disciplines of cryptography and security. One special case of number factorization is called prime factorization, and it entails locating the prime numbers that, when multiplied together, give rise to the original number. Finding these prime factors reveals the fundamentals of the original number, which can then be used to analyze it mathematically.When working with huge numbers, the search for prime factors, also known as the great elements of the number, presents a considerable computational difficulty. In 2014, Shah Muhammad Hamdi et al. presented the number field sieve (NFS) method, a potent algorithm used for factoring big integers, particularly those with more than 100 digits. To ensure the safety of today's communication networks, which rely on intricate encryption methods, this technique has had a profound impact on both number theory and cryptography.The number field sieve algorithm shows improved efficiency and scalability when applied to changeable private key sizes between 4 and 32 bits, in compared to other techniques such as the Schmidt Samoa and Enhanced Schmidt Samoa methods. For the purpose of maintaining the security and reliability of cryptographic systems, its capacity to efficiently process enormous numbers makes it an indispensable instrument. In the context of digital security, where the secrecy and privacy of sensitive data significantly depend on the efficacy of encryption techniques, this flexibility is of paramount importance.The number field sieve method has greatly improved our grasp of number theory and its practical applications by making it possible to find prime factors in complicated and huge numbers. Its application in contemporary cryptography has been crucial in creating trustworthy channels of communication and safeguarding private data in our increasingly linked digital environment.Arithematic analysis in accordance with the guidelines outlined in [26].

Conclusions:

A novel and efficient public key cryptosystem -Enhanced Schmidt Samoa cryptosystem has been proposed for protecting the single owner data in the cloud. Data storage will be done in the cloud once, and most of the time, data retrieval will be performed. The experimental results proved that the ESS cryptosystem could be utilized to ensure data confidentiality in the cloud. From the cloud setup and experimental results, the proposed ESS cryptosystem is highly secured and not easily breakable, compared to the traditional cryptosystems[23].In this research, a secure cloud framework has been developed for the individuals, who are accessing the applications and data in the cloud. Individuals may generate and share the data among multiple users with reading/writing access. In organizations, mostly data will be shared among multiple users for supporting the business process. In these scenarios, multi-user (i.e.) data owner and data user, the concept needsto be adapted in the framework. If the data need to be shared, cryptographic keys need to beshared among the owners securely[24]. Improved Secure Cloud Data Storage Framework (ISCDSF) framework needs to be enhanced by addressing key management issues and ensuring the data confidentiality for multi-user data in the cloud.

Reference:

1. Prasad, B. S., Gupta, S., Borah, N., Dineshkumar, R., Lautre, H. K., & Mouleswararao, B. (2023). Predicting diabetes with multivariate analysis an innovative KNN-based classifier approach. Preventive Medicine, 174, 107619.

2. Prasad, B. V. V. S., and Sheba Angel. "Predicting future resource requirement for efficient resource management in cloud." International Journal of Computer Applications 101, no. 15 (2014): 19-23.

3. Prasad, B. V., and S. Salman Ali. "Software–defined networking based secure rout-ing in mobile ad hoc network." International Journal of Engineering & Technology 7.1.2 (2017): 229.

4. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Veeneetha, S. V., Srivalli, N., ... & Sahitya, D. (2022, November). Prediction of Flight-fare using machine learning. In 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP) (pp. 134-138). IEEE.

5. Kumar, B. R., Ashok, G., & Prasad, B. S. (2015). Tuning PID Controller Parameters for Load Frequency Control Considering System Uncertainties. Int. Journal of Engineering Research and Applications, 5(5), 42-47.

6. Ali, S. S., & Prasad, B. V. V. S. (2017). Secure and energy aware routing protocol (SEARP) based on trust-factor in Mobile Ad-Hoc networks. Journal of Statistics and Management Systems, 20(4), 543–551. https://doi.org/10.1080/09720510.2017.1395174

7. Onyema, E. M., Balasubaramanian, S., Iwendi, C., Prasad, B. S., & Edeh, C. D. (2023). Remote monitoring system using slow-fast deep convolution neural network model for identifying anti-social activities in surveillance applications. Measurement: Sensors, 27, 100718.

8. Syed, S. A., & Prasad, B. V. V. S. (2019, April). Merged technique to prevent SYBIL Attacks in VANETs. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
9. Patil, P. D., & Chavan, N. (2014). Proximate analysis and mineral characterization of Barringtonia species. International Journal of Advances in Pharmaceutical Analysis, 4(3), 120-122.
10. Desai, Mrunalini N., Priya D. Patil, and N. S. Chavan. "ISOLATION AND CHARACTERIZATION OF STARCH FROM MANGROVES Aegiceras corniculatum (L.) Blanco and Cynometra iripa Kostel." (2011).
11. Patil, P. D., Gokhale, M. V., & Chavan, N. S. (2014). Mango starch: Its use and future prospects. Innov. J. Food Sci, 2, 29-30.
12. Priya Patil, D., N. S. Chavan, and B. S. Anjali. "Sonneratia alba J. Smith, A Vital Source of Gamma Linolenic Acid (GLA)." Asian J Pharm Clin Res 5.1 (2012): 172-175.
13. Priya, D., Patil, A., Niranjana, S., & Chavan, A. (2012). Potential testing of fatty acids from mangrove Aegiceras corniculatum (L.) Blanco. Int J Pharm Sci, 3, 569-71.
14. Priya, D., Patil, A., Niranjana, S., & Chavan, A. (2012). Potential testing of fatty acids from mangrove Aegiceras corniculatum (L.) Blanco. Int J Pharm Sci, 3, 569-71.
15. Patil, Priya D., and N. S. Chavan. "A comparative study of nutrients and mineral composition of Carallia brachiata (Lour.) Merill." International Journal of Advanced Science and Research 1 (2015): 90-92.
16. Patil, P. D., & Chavan, N. S. (2013). A need of conservation of Bruguiera species as a famine food. Annals Food Science and Technology, 14, 294-297.
17. Bharathi, G. P., Chandra, I., Sanagana, D. P. R., Tummalachervu, C. K., Rao, V. S., &Neelima, S. (2024). AI-driven adaptive learning for enhancing business intelligence simulation games. Entertainment Computing, 50, 100699.
18. Nagarani, N., et al. "Self-attention based progressive generative adversarial network optimized with momentum search optimization algorithm for classification of brain tumor on MRI image." Biomedical Signal Processing and Control 88 (2024): 105597.
19. Reka, R., R. Karthick, R. Saravana Ram, and Gurkirpal Singh. "Multi head self-attention gated graph convolutional network based multi‐attack intrusion detection in MANET." Computers & Security 136 (2024): 103526.
20. Meenalochini, P., R. Karthick, and E. Sakthivel. "An Efficient Control Strategy for an Extended Switched Coupled Inductor Quasi-Z-Source Inverter for 3 Φ Grid Connected System." Journal of Circuits, Systems and Computers 32.11 (2023): 2450011.
21. Karthick, R., et al. "An optimal partitioning and floor planning for VLSI circuit design based on a hybrid bio-inspired whale optimization and adaptive bird swarm optimization (WO-ABSO) algorithm." Journal of Circuits, Systems and Computers 32.08 (2023): 2350273.
22. Jasper Gnana Chandran, J., et al. "Dual-channel capsule generative adversarial network optimized with golden eagle optimization for pediatric bone age assessment from hand X-ray

image." International Journal of Pattern Recognition and Artificial Intelligence 37.02 (2023): 2354001.
23. Rajagopal RK, Karthick R, Meenalochini P, Kalaichelvi T. Deep Convolutional Spiking Neural Network optimized with Arithmetic optimization algorithm for lung disease detection using chest X-ray images. Biomedical Signal Processing and Control. 2023 Jan 1;79:104197.
24. Karthick, R., and P. Meenalochini. "Implementation of data cache block (DCB) in shared processor using field-programmable gate array (FPGA)." Journal of the National Science Foundation of Sri Lanka 48.4 (2020).
25. Karthick, R., A. Senthilselvi, P. Meenalochini, and S. Senthil Pandi. "Design and analysis of linear phase finite impulse response filter using water strider optimization algorithm in FPGA." Circuits, Systems, and Signal Processing 41, no. 9 (2022): 5254-5282.
26. Kanth, T. C. (2024). AI-POWERED THREAT INTELLIGENCE FOR PROACTIVE SECURITY MONITORING IN CLOUD INFRASTRUCTURES.
27. Karthick, R., and M. Sundararajan. "SPIDER-based out-of-order execution scheme for HtMPSOC." International Journal of Advanced Intelligence paradigms 19.1 (2021): 28-41.
28. Karthick, R., Dawood, M.S. & Meenalochini, P. Analysis of vital signs using remote photoplethysmography (RPPG). J Ambient Intell Human Comput 14, 16729–16736 (2023). https://doi.org/10.1007/s12652-023-04683-w
29. Selvan, M. A., & Amali, S. M. J. (2024). RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE.