[1]Ghada Yousif Ismail
[2]Shaymaa Alhayali
[3]Shahab Wahhab Kareem
[4]Zozan Saadallah Hussain

Secure Data in the Cloud with a Robust Hybrid Cryptographic Approach

Journal of Electrical Systems

Abstract: - Cloud security combines hybrid symmetric encryption and key management to protect user privacy. Our approach can be easily scaled to meet growing cloud data security needs. Cloud computing's basic tenet is resource sharing, which is used for data storage, analysis, and management. Since many people use cloud services and are spread out across the internet, they present many security risks. Hybrid clouds, which can be accessed from anywhere, provide numerous advantages. The security solution (infrastructure as a service) is compatible with many PaaS, SaaS, and even IaaS cloud services. Furthermore, it is consistent with the vast majority of existing cloud solutions. Cloud computing security can be strengthened by using hybrid public key cryptosystems. Concerns about data security have made many businesses wary of cloud computing. The study aims to secure cloud computing by combining the Rabin and Rivest-Shamir-Adleman (RSA) cryptographic models. Analyzing how well a combination of methods generates secure encryption and decryption keys for data. The pure RSA system has longer response times and requires fewer computations compared to the hybrid system.

Keywords: Rivest Shamir Adleman (RSA), Storage Security, Cloud Computing, Cryptographic, Rabin.

I. Introduction

Data completeness and unauthorized access are both protected by computer security. Security issues made operating systems for multiple concurrent users, like the ones created at Massachusetts Institute of Technology's Multics and Cambridge University, the target of criticism in the 1960s. Up until the 1970s, computer security mechanisms were at best in their infancy. A new era of widespread commercial security emerged in the 1990s due to the expansion of the Internet, online shopping, and Java. The security of network authentication procedures is strengthened with the aid of cryptography. Cryptography is unnecessary to construct a file permissions system similar to UNIX [1]. A secure form of long-distance communication using concealed (enciphered or camouflaged) communications that can only be decrypted (or decoded) by the intended recipient is known as cryptography. Greek speakers coined the term "cryptography," which designates a type of "hidden writing" (writing). A message's unencrypted form is called plaintext, whereas its encrypted form is called ciphertext. The final message is encrypted. The process of converting plaintext into an encrypted document is referred to as encryption. As the name suggests, converting encrypted data back into its unencrypted state is known as decryption. Cryptography plays an integral part in the study of cryptology. The study of mathematical techniques for decrypting encrypted data is known as cryptanalysis. On the other hand, cryptologists are used to decipher messages [2].

In the cloud, client computational sequences are carried out utilizing a hybrid type of cryptography. With fewer involvements by IT professionals or service companies and more excellent security and protection, cloud computing is a tried-and-true technique for quickly building a shared pool of reconfigurable computing resources [3]. Everyone's information is kept safer when encrypted and decoded in the cloud before transferring. A more secure cloud computing system can be built using hybrid cryptography [4], which includes identification aspects and ensures higher security. While offering enterprises the flexibility to meet the demands of their consumers for dependable service, the cloud must handle several security issues. Sensitive data will be stored using cloud computing in a far more secure setting by combining asymmetric cryptosystems. Elliptic curve cryptography has attracted much attention compared to RSA and other public-key cryptosystems. Two popular cryptography methods, HECC and RSA, create similar-sized keys [5]. Cryptography using public keys describes the procedures for producing data encryption keys and digital signatures. Due to their ability to serve all three of these objectives, public-key primitives are frequently used in contemporary applications. Massive data streams are often encrypted

[1] *Corresponding author: Department of Mechanical Technology, Technical Institute, Northern Technical University, Iraq

[2]Computer Center, University of Mosul, Iraq

[3] Department of Computer Engineering, College of Engineering, Knowledge University, Erbil 44001, Iraq.

[3]Information System Engineering Department, Erbil Technical Engineering College, Erbil Polytechnic University

[4]Department of Electrical Technology, Technical Institute, Northern Technical University, Iraq

and authenticated using hybrid-key algorithms because they are more efficient than public-key methods. Digital signatures have significantly boosted the use of public-key methods. They ensure the accuracy of the data being communicated, the accuracy of the transmitted data, and the prevention of message forgery. This suggests that the sender needs a way to contest the communication's legitimacy, which could be crucial in some situations. In 1976, a paper describing the first public-key cryptosystem based on factorization was released, and two different functional systems were created in the following years [6]. For cryptographic operations such as digital signature algorithms and the Diffe-Hellman key exchange to operate, the discrete logarithm (DL) in finite fields must be addressed. They have algebraic curves over a limited field DL [7]. Use the outline below to help you read this essay.

II. Review of the work

Some people think that safety concerns are the most significant obstruction in the widespread adoption of cloud computing. The community for cloud security has recently been highly active., highlighting several studies. Exactly how much Kamara S. Additionally, Lauter K. has published a security paradigm [8] that may be applied in public cloud environments and depends on cryptographic primitives to guarantee data integrity. To encrypt data with another user, a user must create a public key. You can utilize your unique decryption key to transfer confidential data securely. Encrypted data can be indexed thanks to symmetric and asymmetric searchable encryption. It was advised to use a model by anybody created by Dinesh et al. that depends on cryptographic safety methods to do their research first [9]. (OPSE) has combined symmetric searchable encryptions with order-preserving symmetric ciphers. The investigation reveals that the system prioritizes keyword search instances efficiently but offers no information on attacks, authenticity, or privacy. As a result, employing them in a protective capacity might not be appropriate. Data that uses incremental encryption can be double-encrypted before being uploaded to the cloud or distributed to other authorized users [10–11].

Ahmed et al. [12] examined the security needs for cloud computing while highlighting the threats and difficulties associated with the various cloud computing models (SaaS, PaaS, and IaaS). An architecture for cloud-based data interchange using the MD5 algorithm and RSA cryptography is suggested. The RSA method can securely encrypt large data files in the cloud. The model functions admirably with static data. Meanwhile, most data kept in the cloud is dynamic [13]. Utilizing message authentication codes and 128-bit secure sockets layer technology, data saved in the cloud is encrypted [14]. Safeguarding data in the cloud is advised using the Advanced Encryption Standard (AES) approach [15]. However, building a connection protocol creates a shared secret key. Diffie-Hellman created the identity-based plaintext checkable encryption technique to exchange keys and encrypt data in a way that is related to the mobile e-commerce scenario. With this approach, users can authenticate their cipher text without having access to the secret key by giving personal identity information.

In [16], a third-party equality test and a cloud-based identity encryption technique were presented. The supplier can read many customers' encrypted messages using the equality test. This method can be used in practical situations due to the hash-to-point procedure and the bilinear map. Mahalle et al. proposed a Hybrid (RSA & AES) encryption technique to maintain cloud data security. The most crucial aspect of cloud computing, security, must be handled carefully. Using the two corresponding keys facilitates the secure upload and download of the data. The key generation method is also considered special in its own right. This has made it easier to prevent the possibility of redundant or repeated keys [17]. They suggested revocable-storage identity-based encryption (RS-IBE), which can introduce user revocation and ciphertext update functionalities to provide ciphertext's forward/backward security. The user whose access has been revoked cannot access shared data from the past [18].

A practical implementation of identity-based encryption over NTRU lattices by McCarthy et al. [19]. Demonstrates how identity-based encryption permits key distribution in a multi-user system, which is frequently helpful in a resource-constrained context. A completely functional identity-based encryption method (IBE) was proposed by Boneh et al. [20]. Using a version of the computational Diffie-Hellman problem, the system has chosen ciphertext security in the random oracle model. Bilinear maps between groups form the foundation of our system. We define safe identity-based encryption techniques precisely and list numerous uses for these systems. Abdalwahid et al. [21] paired-key cipher is safe and impenetrable in the presence of a colluder. This study speeds up the process of calculating private and public keys. The cloud provider's primary concern should be to protect their clients’ data. The ideal method to ensure your cloud-stored data's safety is to use an asymmetric cryptosystem based on hyperelliptic curve cryptography [22]. Large amounts of data saved in the cloud must be easily and securely accessible from the user's point of view. Although security issues demand careful thought, the complexity of the cryptographic method has yet to receive enough attention. The proposed model fixes issues with the procedure and enhances competent, speedy, and secure data access.

III. Cloud Security Challenges

Services and products offered via the cloud are anticipated to become even more popular in the upcoming year. The requirement in the case of cloud services is still increasing at a never-before-seen rate, as are security breaches. Threats and opportunities for cloud infrastructure for 2022 are reported cyber security in cloud infrastructure. To maximize cloud output, businesses quickly adopt cloud applications, occasionally employing third-party apps as starting points. Cloud-based services and solutions are anticipated to become even more popular in the upcoming year. Security breaches and the demand for cloud-based services are increasing at previously unheard-of rates. Cloud infrastructure security has been cited as a threat and an opportunity for 2022. To maximize cloud output, businesses quickly adopt cloud applications, periodically using start-up apps and code snippets from other parties. Companies are scrambling to create cloud infrastructure to handle older workloads. As a result, third-party code libraries and generators have become more well-liked. While deployment is not intrinsically risky, organizations should be aware of the risks and perform careful checks. Recent research found that 96% of containerized software has security issues. Many companies use third-party code templates to speed development; however, 63% have unsafe settings. Effects of the rise of the hybrid workforce on cloud access rights management and governance in a hybrid system containing elements of both paradigms, managing security and privacy issues is more complicated. Implementing thorough access controls responsive to users' context and authentication in zero-trust network architectures (ZTNA) will be the most challenging component of cloud deployment [23].

Businesses that use the cloud frequently should record who has access to what and for what purposes. It should be a job function, not a job title, determining who can access which cloud resources. Businesses must maintain strict compliance as more data is hosted in the cloud. A Company's conformity requirements may differ significantly if it works in several nations. Organizations should monitor where their cloud service provider's data centers are located. Second, are there variations in data storage regulations between countries? Businesses must react to these inquiries to satisfy regulators, investors, partners, suppliers, and consumers, which are most essential. Every day, the "owners" of data have higher control over gathering, using, and deleting their data in the cloud. We're actively updating the data management guidelines. Because of this, businesses must exercise extreme caution while handling sensitive data. They are now in charge of guarding against illegal access to personal data. Companies, therefore, require policies to safeguard sensitive data. The usage of "fake data" may become more common due to the present trend in data management [24]. We can categorize a few specific problems with cloud computing according to. People who try to tamper with private Information about clients have broken the law and could face consequences under the data protection laws. Keeping track of client data transfers is crucial in an attack or leak. The authentication features of the supplier's virtual systems should be shared with other physical networks, including two-factor authentication and a central authorization database. The strategy for implementing one-time passwords and biometric authentication is the same. Using all encrypted data across different clouds requires authentication for this reason. When moving data in the cloud, it is advisable to use a hybrid cryptosystem to implement this laborious and unique authentication method.

The integrity of the underlying physical infrastructure is necessary for cloud data security. Therefore, it is the service provider's responsibility to ensure they are truthful. Other authentication methods to access your cloud storage include biometrics and the Irish cryptographic challenge. The suggested approach establishes data verification as simple. Customers' stored information and software will always be accessible in real time, thanks to cloud service providers. Network infrastructure threats Figure 1 illustrates some of the worst possible outcomes for a network, including invasions. These attacks result in a temporary or permanent loss of service, theft or unauthorized exposure of sensitive information, or the erasure of vital information [25].

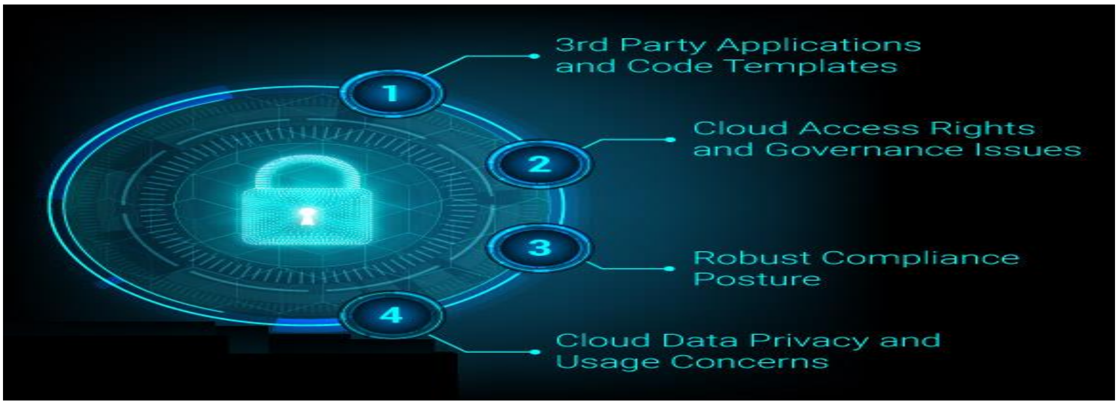

1
3rd Party Applications and Code Templates
2
Cloud Access Rights and Governance Issues
3
Robust Compliance Posture
4
Cloud Data Privacy and Usage Concerns

Figure 1. Security challenges with the cloud

IV. Utilizing An Asymmetric Key Cryptosystem for Cloud Security

Utilizing an asymmetric key cryptosystem for cloud security is crucial in safeguarding sensitive data stored and transmitted over the cloud. Public-key cryptography, commonly called asymmetric key cryptography, employs a pair of keys: a public key for encryption and a private key for decryption. This approach provides several benefits for cloud security [26].

The first is that asymmetric key encryption offers confidentiality because during data transmission, even if the intruder has access to that data, the content will be unreadable, as it is encrypted without the respective private key of the data. This protects the data from breaches and access to classified information by people who are not authorized to do so. The second part is the integrity of the. The digital signature, generated with the private key, can be seen as the means through which one provides the recipient with assurances that the data remains genuine and has not been changed in the course of its transmissions or while resident at rest—i.e., guarding against tampering or modification by an unauthorized entity. Besides, this technique ensures that the property of authentication and non-repudiation is possible. These would allow the cloud service being accessed to be both valid and reliable in the sense of being a real entity, from the public key of the service provider. Digital signatures would also provide the origin of data, so its integrity can save a user from data repudiation. However, several challenges and considerations have to be dealt with to implement an asymmetric key cryptosystem for cloud security. These include the potential performance overhead due to computational complexity, proper practices of key management ensuring long-term security, and possible quantum computing affecting asymmetric key algorithms [27-28]. Actual cloud security, however, contains a huge scope of real-life applications for an asymmetric key cryptosystem. It does find its applications in securing data exchanges between clients and service providers in such a way that end-to-end encryption is assured. This would also safeguard data at rest in cloud storage systems from unauthorized access. Other applications of asymmetric key cryptography in cloud computing are authenticated users and secure access control mechanisms. The use of an asymmetric key cryptosystem, therefore, further enhances a more secure cloud. This protects threats, hence ensuring there are no data breaches, unauthorized access, or tampering. Such research and development efforts are needed to answer the emerging challenges of long-term cloud computing security [29].

V. THE PROPOSED SYSTEM

The system is a cascade of the RSA and Rabin public key cryptosystems. Using a hybrid cryptosystem aims to increase security beyond what is feasible with a single cryptosystem. It is expected that all data on the cloud has already been encrypted. Users who use the cloud are eligible to create specific keys (both public and private keys). After that, the file is encrypted while being buffered on the cloud using the suggested hybrid method. The cloud transmits the encrypted data sets to the knowledge nodes.

A. The proposed method's Key Generation is displayed below:

INPUT: Randomly choose the prime p and q numbers and their sizes.

OUTPUT: A private key (p, q, d) and a public key (n, e). Communication with User B is started by User A.

1. Produce two equal-sized prime numbers, p, and q, randomly (and in different ways).
2. Next, determine n = p*q and n = p*q-1.
3. choosing an integer e in such a way that the gcd (e ;) is one.
4. Using the extended Euclidean algorithm, identify the single number d, 1d, such that ed1 (mod).

5. The public and private keys for the user are (n; e) and (d, p, q), respectively.

B. *The approaches put forth to have the following encryption procedure:*

INPUT: To encrypt it, the recipient must provide them with the user's public key in plaintext (n; e).
OUTPUT: cipher text in encryption.
Users A and B are the recipients of the message. B should carry out the subsequent actions to encrypt::

1. Get hold of A's public key. (n; e).
2. Integer representation of the message is set, m, between [0, n1] next.
3. Find C = (m2e) mod n in step three.
4. Assemble c and send A the encrypted message.

C. *The following illustrates the suggested algorithm's decryption procedure:*

INPUT: Acquired the recipient's secret key and the encrypted message.
OUTPUT: authentic plaintext.
B will be able to distinguish plaintext m from c using this procedure:

1. Using the private key d as the input, find W=cd mod n.
2. Find the four-square roots of W modulo n for m1, m2, m3, and m4.
3. The message was contained in one of the square roots m1, m2, m3, or m4.

Fig. 2 illustrates these actions. A storage node, often known as a "node," is a component of cloud computing where metadata is kept to keep the directory up to date and manage access to encrypted files. To generate the encrypted file, a significant number of knowledge nodes contribute one or more blocks.

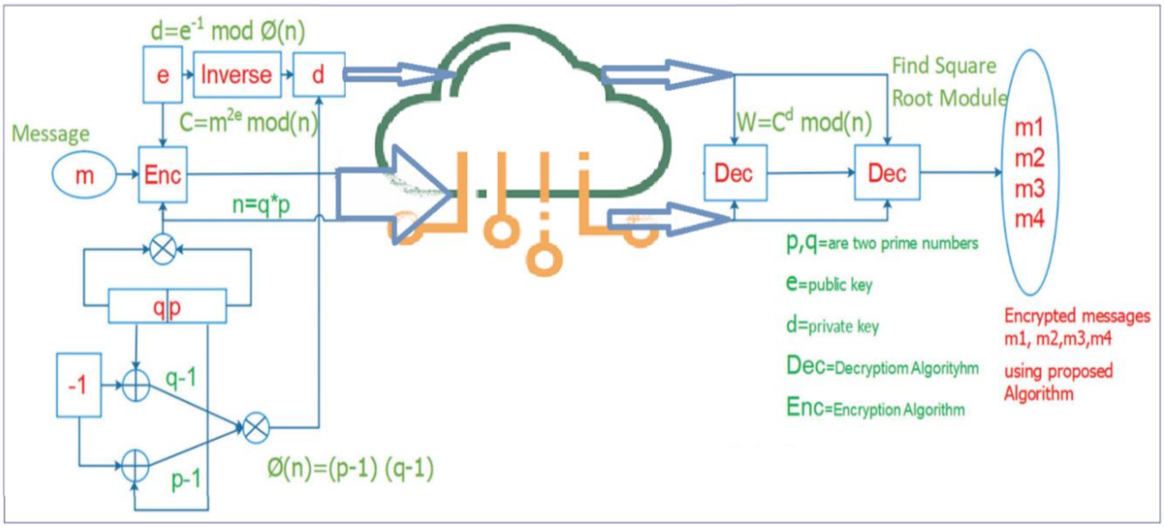


Figure 2 Model for Cloud Security

VI. Discussion Of the Results

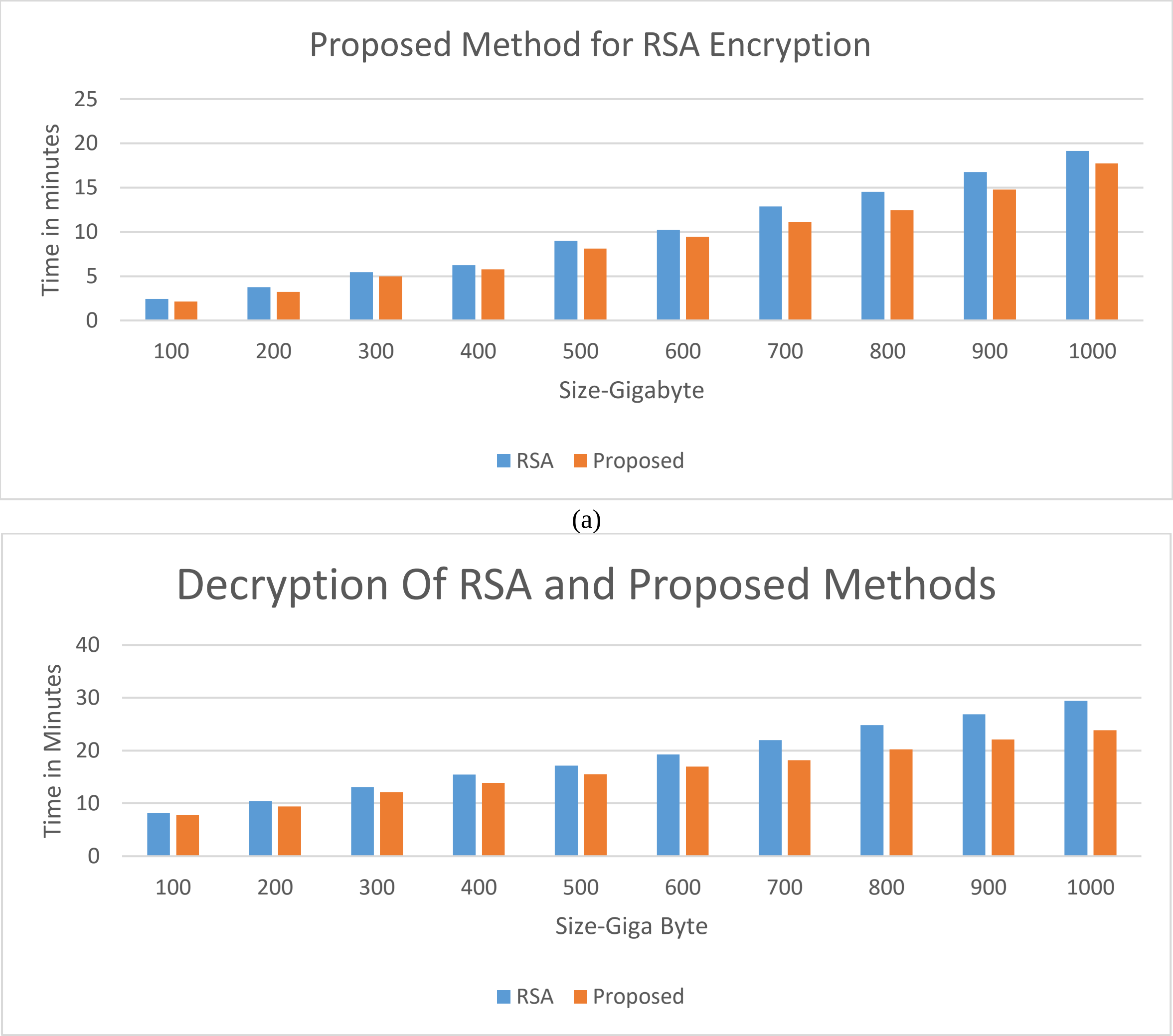
The data transport based on virtualization is the basis of cloud computing. Therefore, we need to be concerned about data storage. Users should exercise the same caution while using cloud services as any other information system. Consumers should, for example, be aware of the location of the storage host. Customers have an entitlement to know where their data is stored and where it originated if any other data is gathered and stored nearby. Confidentiality, authentication, integrity, and availability are the four cornerstones of data security that cloud service providers must ensure. Service providers struggle to secure their customers' private information despite the massive demand for their products. It is impossible to justify the expense of hiding vital consumer information. In response to this need, a more sophisticated cloud security system has emerged to guarantee the safe storage of sensitive data in the cloud. To maximize safety, engineers use both symmetric and asymmetric critical techniques. RSA is a suggested method for data encryption and decryption. Cryptosystems are time-consuming. By facilitating the systematic classification of algorithms based on their performance and guiding the latter to the "optimal" solutions for challenging situations, the O-notation has proven helpful for analysts and algorithm designers. The standardized units of measurement for computational complexity are (T) time complexity and (S) space complexity, expressed as a function of the inputs (n), which is feasible. Eq. 1 shows the time complexity of RSA encryption, while Eq. 2 shows the time complexity of decryption (i).

The time constant:

$$T_c = 0(\log n)^3 \quad (1)$$

$$T_m{=}0(\log n)^3 \quad (2)$$

We use randomly generated plaintext of different lengths to compare the encryption and decryption timings of the recommended approaches to those of the conventional public key encryption system. Figure 3(a) displays the results for files of various ordinary text file sizes (100, 200, 300, 400, 500, 700, 900, and 1000 GB). The suggested approach encrypts and decrypts data faster than the RSA cryptosystem, as shown in Figures 3(a) and 3(b).



(a)

(b)

Figure 3. Time for (a) the encryption procedure and (b) the decryption process of the file size in MB

VII. CONCLUSION

Cloud computing security has been the subject of numerous worries. One disadvantage of cloud computing is the need for stricter privacy and security measures. The suggested model is created in Java and used in the real world. It modifies RSA asymmetric key techniques. Key generation, encryption, and decryption are methods for enhancing cloud security. The suggested system offers a faster and more secure way of creating and distributing encrypted software in the cloud. The most widely used service for cloud paradigms, including IaaS, SaaS, and PaaS, is compatible with the suggested encryption technique. The proposed method demonstrated very little processing time overhead across various file sizes and complexity levels (decryption stages have twice as much computing complexity). Combining the asymmetric key cryptosystems Rabin and RSA will become necessary over time. The standard output of the Rabin method is four different plaintexts, which take a long time to decrypt a message, a critical problem in the proposed hybrid system.

REFERENCES

[1] J.B.D. Joshi and Gail-Joon Ahn., “Challenges with Security and Privacy in Cloud Computing Environments,” IEEE Security Privacy Magazine, vol. 8, pp. 24–31, Oct. 2010.

[2] FarzadSabahi, “Threats to and solutions for cloud computing security,” Third International Conference on Communication Software and Networks (ICCSN), IEEE, 2011.

[3] Aparna and Ashish Agarwal, “The dangers of cloud computing for security,” The International Journal of Computer Applications in Engineering Sciences, vol. 1, special issue on CNS, July 2011.

[4] Zhijie Jerry Shi and Hai Yan., “Software Elliptic Curve Cryptography Implementations,” Third International Conference on Information Technology New Generations, April 2006.

[5] Suresha and Ravi Gharshi, “Using the ECC Algorithm to Improve Cloud Storage Security,” International Journal of Science and Research (IJSR), Vol. 2, Issue 7, July 2013.

[6] Abdalwahid, S. M. J., Yousif, R. Z., and Kareem, S. W., “Enhancing approach using hybrid paler and RSA for information security in big data,” Applied Computer Science, vol. 15, no. 4, 2019.

[7] Modares, M. T. Shahgoli, H. Keshavarz, A. Moravejosharieh, and R. Salleh H., “Make a Secure Connection Using Elliptic Curve Digital Signature,” Vol. 3, Issue 9, International Journal of Scientific and Engineering Research (IJSER), September 2012.

[8] Kamara, S., Lauter, and K., “Cloud storage with encryption,” 2010's Lecture Notes in Computer Science, vol. 6054, pp. 136–49.

[9] Dinesh Nepolean, I. Karthik, Mu. Preethi, Rahul Goyal, and M. Kathirvel Vanethi “Privacy-Preserving Ranked Keyword Search over Encrypted Cloud Data,” International Conference on Security in Computer Networks and Distributed Systems, pp. 396–403, 2014.

[10] M. Venkatesh, M. R. Sumalatha, and C. Selva Kumar, “Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing,” 2012 International Conference on Recent Trends in Information Technology (ICRTIT), April 2012.

[11] Amin Salih M. H. A. M., and Shahab Wahhab Kareem, “A Deep Learning Method for Detecting Leukemia in Real Images,” NeuroQuantology, 2022.

[12] Hussam Alddin S. Ahmed, Mohammed Hasan Ali, Laith M. Kadhum, Mohamad Fadli Bin Zolkipli, Yazan A. Alsariera, “A review of challenges and security risks of cloud computing,” Journal of Telecommunication, Electronic and Computer Engineering, pp. 87–91, vol. 9, No. 1-2, 1 January 2017.

[13] Mayank Namdev, Shiv Shakti Shrivastava, Ashutosh Kumar Dubey, and Animesh Kumar Dubey, “Cloud-User Security Using RSA and MD5 Algorithm for Java Environment Resource Attestation and Sharing CSI,” Sixth International Conference, Software Engineering (CONSEG), Sept. 2012.

[14] Wang C, Cao N, Li J, and Ren K., “Lou Secure Ranked Keyword Search over Encrypted Cloud Data,” ACM W Journal, 43(3), pp. 431–73, 2010.

[15] D. Boneh and M. K. Franklin, “Identity-based encryption from the Weil pairing,” Proc. CRYPTO, LNCS, vol. 2139, pp. 213–229, 2001.

[16] S. Ma, “Identity-based encryption with outsourced equality test in cloud computing,” Information Sciences, vol. 328, pp.389–402, 2016.

[17] Vishwanath S Mahalle, et al., “Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm,” 2014 International Conference on Power, Automation and Communication (INPAC), December 2014.

[18] Kishore Babu V and R Amutha, “Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption,” International Journal of Scientific Development and Research, pp. 91–94, 2017.

[19] S. McCarthy, et al., “A Practical Implementation of Identity-Based Encryption over NTRU Lattices”,16th International Conference (IMACC), December 12-14, pp.227-246, 2017.

[20] D. Boneh and Matthew Franklin, “Identity-based encryption from the Weil pairing,” Proc. Proceedings of Crypto 2001, vol. 2139, pp. 213–229, 2001.

[21] Abdalwahid, S. M. J., Yousif, R. Z., and Kareem, S. W., “Enhancing approach using hybrid pailler and RSA for information security in big data,” Applied Computer Science, vol. 15, no. 4, 2019.

[22] Tao Sun and Xinjun Wang., “Data Security Model in Cloud Computing Platform for SMEs,” International Journal of Security and its Applications, 7(6), pp. 97–108, 2013.

[23] Joshna S1 and Manjula P, “Challenges and Security Issues in Cloud Computing,” International Journal of Computer Networks and Mobile Computing, Vol.3, Issue.4, pp. 558-563, April 2014.

[24] Luca Ferretti, Michele Colajanni, and Mirco Marchetti Distributed, “Concurrent, and Independent Access to Encrypted Cloud Databases,” IEEE Transactions on Parallel and Distributed Systems, Vol.25, No. 2, February 2014.

[25] Modares, M. T. Shahgoli, H. Keshavarz, A. Moravejosharieh, and R. Salleh H., “Make a Secure Connection Using Elliptic Curve Digital Signature,” Vol. 3, Issue 9, International Journal of Scientific and Engineering Research (IJSER), September 2012.

[26] L. Qin, Z. Cao, and X. Dong, “Multi-receiver identity-based encryption in multiple PKG environment,” IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, New Orleans, LA, USA, pp. 1–5, 2008.

[27] KAREEM, and S. W., “Secure Cloud Approach Based on Okamoto-Uchiyama Cryptosystem,” Journal of Applied Computer Science & Mathematics, vol. 14, no. 29, pp. 9-13, 2020.

[28] Larry Barret, “The SaaS market is expanding rapidly, according to Gartner, Computing Quin-Street,” Inc., July 2010.

[29] Kareem, S. W., Yousif, R. Z., & Abdalwahid, and S. M. J., “An approach for enhancing data confidentiality in Hadoop,” Indonesian Journal of Electrical Engineering and Computer Science, 20(3), pp.1547-1555, 2020.