Journal of Namibian Studies, 33 S2(2023): 346–360 ISSN: 2197-5523 (online)

A Strong Combination of Cryptographic Techniques to Secure Cloud-Hosted Data

Khalid Altarawneh

Assistant professor, Faculty of Information Technology, Data Science Department, Mutah University, Jordan.

Abstract

In Hybrid Cloud Security, we combine symmetric encryption with key management to ensure anonymity. Our method provides a flexible and scalable deployment solution for cloud-based data security. To store, analyse, and deal with data, cloud computing relies on a core concept: sharing resources. Since cloud services are utilized by many individuals and are dispersed across the Internet, they provide a number of security vulnerabilities. Due to their worldwide accessibility, hybrid clouds open up a wide range of opportunities. The security solution works with a wide variety of PaaS, SaaS, and even IaaS cloud services (Infrastructure as a Service). It also works with most Cloud services out there. Hybrid public key cryptosystems can improve cloud security. Businesses are wary about cloud computing due to security concerns. The primary goal of this research is to strengthen the security of cloud computing by fusing the cryptographic models of Rabin and Rivest-Shamir-Adleman (RSA). Evaluating the efficacy of a hybrid approach to producing secret keys for data encryption and decryption. The purely RSA-based system has higher latency and is less computationally intensive than the hybrid system.

Keywords: Rivest-Shamir-Adleman (RSA), Rabin, storage security, network security, and Cryptography.

I. Introduction

Computer security ensures that data is both complete and accessible only to authorized users. Operating systems for several users at the same time, such as the one developed at Cambridge University and Multics at the Massachusetts Institute of Technology drew criticism in the 1960s due to security concerns. Security measures for computers were nascent at best until the 1970s. In the 1990s, the proliferation of the Internet, online commerce, and Java ushered in a new era of ubiquitous commercial security. Cryptography helps strengthen the security of network authentication processes. To implement a system of file permissions similar to that of UNIX, cryptography is superfluous [1].

Cryptography is the study of developing secure techniques of long-distance communication via hidden (enciphered or disguised) communications that can be decoded by only the intended receiver (or decipher it). The term "cryptography," which originated in Greek, refers to a method of "hidden writing" (writing). Plaintext refers to the unencrypted form of a message, while ciphertext refers to the encrypted version. The last message is encrypted. The term "encryption" is used to describe the procedure of changing plaintext into an encrypted form. Decryption, as the name suggests, is the process by which encrypted data is converted back into its unencrypted state. The field of cryptology depends heavily on cryptography. Cryptanalysis is the study of mathematical methods for deciphering encrypted data. Cryptologists on the other side utilize cryptanalysis [2] to decipher messages.

Client computational sequences in the cloud are executed using a hybrid form of cryptography. Cloud computing is a proven method for rapidly deploying a shared pool of reconfigurable computing resources with reduced involvement from IT staff or service providers and enhanced safety and security [3]. When data is encrypted and decrypted before being shared in the cloud, everyone's information is kept safer. Hybrid cryptography [2], which integrates identification elements and assures a better level of security, can be used to create a more secure cloud computing system. The cloud must address a variety of security concerns while simultaneously offering the ability for enterprises to meet the expectations of their customers for reliable service. As a result of integrating asymmetric cryptosystems, cloud computing aspires to keep sensitive data in significantly more secure locations. In comparison to other public-key cryptosystems like RSA, elliptic curve cryptography has attracted a lot of interest. HECC and RSA, two of the most widely used cryptographic algorithms, produce keys of nearly the same size [8]. In public-key cryptography, the algorithms for key generation, digital signatures, and data encryption are defined.

Public-key primitives are widely used in modern applications because they provide all three of these purposes. More efficient than public-key algorithms, hybrid-key algorithms are commonly utilized to encrypt and authenticate massive data streams. There has been a dramatic increase in the deployment of public-key algorithms because of digital signatures. They prevent message forging, ensure the integrity of the data being sent, and guarantee the validity of the information being sent. This implies the sender has no recourse to challenge the authenticity of the communication, which might be game-changing in certain circumstances. In the years following the publication of the first factorization-based public-key cryptosystem in 1976, two other viable systems have been developed. Cryptographic procedures like digital signature algorithms and the Diffe-Hellman key exchange rely on the resolution of the discrete logarithm (DL) problem in finite fields. They have a DL problem involving algebraic curves over a finite field. Read this paper with the help of the outline provided below. This literature review's structure is presented in Section 2. This third segment will discuss cloud security, including both problems and potential answers. Section 4 analyzes the results of a comparison between the suggested optimized hybrid encipherment approach and traditional public-key cryptosystems. A discussion of the simulation results is included in Section 5. Section 6 presents a summary of the findings.

II. A REVIEW OF THE WORKS

There are some who believe that security worries are the biggest obstacle to the mainstream use of cloud computing. The cloud security community has been busy recently, presenting a plethora of research papers. To what extent does Kamara S. In addition, Lauter K. has released a security paradigm [6] that relies on cryptographic primitives to ensure data integrity and may be used in public cloud environments. A user must generate a public key in order to encrypted data with another user. When sending sensitive information, you can use your own unique decryption key to keep it safe. Symmetric and asymmetric searchable encryption allows for the indexing of encrypted data.

It is recommended that anyone using a model developed by Wang C and others that relies on cryptographic techniques for security read up on the topic beforehand [11]. Order-preserving symmetric ciphers and symmetric searchable encryptions have been used together (OPSE). Although the analysis provides proof of the model's effectiveness keyword search case rankings, it provides no data on attacks, authenticity, or privacy. Therefore, it might not be fit for use in a protective role. Using incremental encryption [12], data can be encrypted twice: once before being stored in the cloud, and again before being shared with other authorized users.

Researchers Ashish Agarwal and Aparna Agarwal [13] address potential security risks associated with the cloud. The MD5 algorithm and RSA cryptography are used in a suggested architecture for cloud-based data exchange. The RSA technique allows for the secure encryption of large data files on the cloud. When using static data, the model performs admirably. However, most data stored in the cloud is dynamic in nature[14]. Information stored in the cloud is encrypted using 128-bit Secure Sockets Layer technology and message authentication codes [15].

The Diffie-Hellman and Advanced Encryption Standard (AES) algorithms, along with a digital signature, are recommended for use in securing data in the cloud [16]. Alternatively, we're going to employ a connection-establishing protocol to generate a shared secret key. The mobile e-commerce scenario is connected to the identity-based plaintext-checkable encryption (IBPCE) system, which was proposed by Diffie Hellman key exchange and data-encryption. In this system, users can verify the authenticity of their cipher text by providing their personal identification information without needing to know the secret key. An identity encryption scheme using the cloud and a third-party equality test was proposed in [17]. (IBEET). Using the equality test, the provider can read the encrypted messages of many customers. The bilinear map and hash to point operation render this technique applicable to real-world applications. The first five steps involve encrypting the data, while the final stage, Test, involves verifying its equality. By inputting IDA, CA, and tdA or IDB, CB, and tdB, a binary number is generated.

[19] advocated for a patient-safety-focused identity-based healthcare encryption system. Patient data is encrypted and stored securely in the cloud. In this work, IBE is combined with a signature method to safeguard data in transit against the adversary. It makes sure the user is who they say they are by using their public key.

Colaco and Krishna [20] were the first to propose using IBE with a random orientation to encrypt user communications. In this work, the totient function of Euler is used to construct the user ID, global parameter, and master private key. A CA is optional. Boneh and Franklin introduced Diffie-Hellman-protected IBE in [21]. The paired-key cipher created by Sakai and Kasahara [22] is secure and unbreakable in the presence of a colluder. This research reduces the amount of time needed to calculate private and public keys.

Safeguarding their customers' information should be the cloud provider's top priority. Using an asymmetric cryptosystem based on hyper elliptic curve cryptography [3] is the best way to ensure the security of your cloud-stored data. From the perspective of the user, it is essential to have quick and secure access to large amounts of data stored on the cloud. Although security considerations warrant careful consideration, insufficient focus has been placed on the complexity of the cryptographic algorithm employed. The proposed model sidesteps the issues with the offered method by rapidly enhancing competent, quick, and secure data access.

III. CHALLENGES WITH CLOUD SECURITY

The popularity of cloud-based services and solutions is expected to increase further in the coming year. As the need for cloud-based services continues to grow at an unprecedented rate, so too do the number of reported security breaches. Threats to and opportunities for 2022 in the area of cyber security in cloud infrastructure.

Enterprises are rapidly adopting cloud applications to make the most of cloud output, sometimes making use of third-party apps and code snippets as starting points. Businesses are rushing to build cloud infrastructure to handle old workloads. That's why there's been such a surge in popularity for code libraries and generators built by third-parties. While not inherently risky, deploying companies should be cognizant of the potential hazards and perform thorough checks anyhow. Ninety-six percent of the containerized software in a recent research had security flaws. In order to speed up the development process, many businesses turn to third-party code templates; nevertheless, 63% of these templates contained exploitable configurations. The Rise of the Hybrid Workforce: Implications for the Management of Cloud Access Rights and Governance Managing security and privacy risks is more challenging in a hybrid environment that has elements of both paradigms. As a result, the most difficult aspect of cloud deployment will be implementing comprehensive access controls that are sensitive to context. Authentication of Users in Zero Trust Network Architectures (ZTNA). Businesses that rely heavily on the Cloud should keep records of who has access to what on the cloud and why. Job function, not job title, should be the deciding factor in who has access to what cloud resources. As more and more information is stored in the cloud, businesses need to maintain a strong compliance posture. A company's compliance needs may vary substantially if it operates in more than one country. Organizations should also monitor the locations of the data centers used by their Cloud Service Provider. Second, do different countries have different rules for data storage? Businesses need to respond to these kinds of queries because a strong compliance stance impresses regulators, investors, partners, vendors, and, most importantly, customers. The "owners" of data have greater say over the collection, use, and deletion of their information in the cloud every day. The rules of data management are currently being revised. That's why it's so important for businesses to be cautious when handling private information. They must now take responsibility for preventing unauthorized access to private information. As a result, businesses need strategies to protect private information and make ethical use of it. The current trend in data management could open the door to the use of "false data." [3].

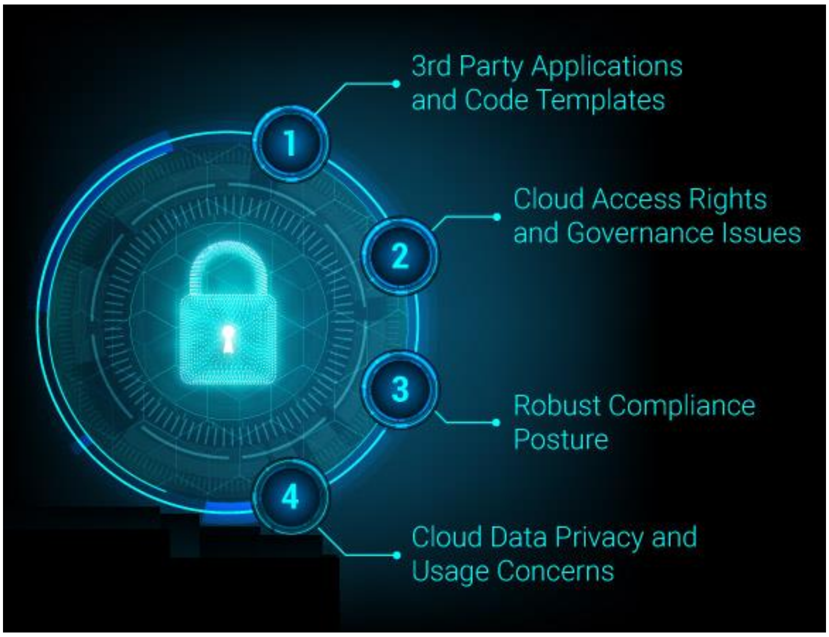
1
3rd Party Applications and Code Templates
2
Cloud Access Rights and Governance Issues
3
Robust Compliance Posture
4
Cloud Data Privacy and Usage Concerns

Figure 1: Security Challenges with the Cloud

There are a few distinct issues with cloud computing, and we can classify them as follows.

Snoopers who attempt to tamper with the personal information of other customers are breaking the law and are subject to penalties under data protection legislation. It is important to keep an eye on client data transfers in case of an attack or a leak [5].

Two-factor authentication and a centralized authorization database are two examples of authentication characteristics that the provider's virtual systems should have in common with other physical systems. Biometric authentication and one-time passwords can be implemented using the same strategy. This is why it is crucial for all encrypted data to have authentication before being used across various clouds. This laborious and one-of-a-kind authentication approach is best done using a hybrid cryptosystem when transporting data in the cloud.

The security of cloud data depends on the integrity of the underlying physical infrastructure. As a result, it is up to the service provider to guarantee their honesty. You can gain access to your cloud storage by using a variety of authentication methods, including biometrics, digital signatures, the Irish cryptographic challenge, and one-time passwords. The proposed method makes data verification easy.

Cloud service providers guarantee their clients seamless, real-time access to all of their stored information and software. Threats to Network Infrastructure Some of the worst things that can happen to a network are intrusions, attacks resulting in a temporary or permanent reduction of service, the theft or unauthorized disclosure of sensitive data, or the destruction of critical records.

IV. USE OF ASYMMETRIC KEY CRYPTOSYSTEM FOR CLOUD SECURITY

RSA public key algorithm is a cryptographic hash function that relies on the intractable nature of factoring primes. Like the majority of other public key password features, RSA passwords are encrypted using a block cipher. Block encryption is used by secret-key algorithms like DES (Data Encryption Standard), however these techniques offer more leeway in terms of plaintext and key lengths. So, a secure and reliable system can employ a larger key length, while an efficient method demands a shorter one. The message is encrypted using the recipient's public key during the RSA operation, and then decrypted using the recipient's private key. When a sender uses its private key to sign communications and a receiver uses the sender's public key to validate the signed message, the RSA-based signature approach guarantees an authentication service.

Safe and quick data transfers are crucial in many business domains. Companies use public-key cryptography techniques to make sure their apps are secure (PKCS). To organize RSA systems, the PKCS standard is commonly applied. In the last decade, RSA encryption has become one of the most widely used public-key techniques. The RSA algorithm is utilized in a wide variety of software. The security provided by RSA is unquestionably infallible. However, the necessary key length has grown as computational power has progressed. The performance features of RSA can be examined using the aforementioned numerical methods. The RSA cryptographic protocols supported keys of varying sizes during encryption and decoding. Over the past decade, public-key cryptosystems have seen increased adoption due to the increasing demand for secure communication [4]. For good reason, the RSA cryptosystem developed by Rivest, Shamir, and Adelman is widely used for protecting sensitive information.

When it comes to public-key cryptography, RSA is one of the first and most popular methods to use. It was one of the early significant advances in public key cryptography because it was the first method determined to be appropriate for signing and encrypting. As long as the keys are sufficiently long, RSA continues to see widespread use in e-commerce protocols. Integers and one-way factorization are crucial to RSA's operation. Both the public and private keys can be derived from one another. When given a public key and encrypted text, decrypting it can be a computationally intensive process. The most frequent form of asymmetric encryption is RSA, which is also the most popular public key encryption standard. The RSA public key is meant to be distributed widely, but the private key must be kept secure.

Today's organizations can choose from several different cloud access points. Cloud services consist of the hardware, software, and programs that are made available online. Potential benefits and downsides may be misunderstood by many people due to the complexity of the options and the language used to describe them. Interface vulnerabilities were also a topic of discussion and exploitation within the application security field. Recommendations for improving PaaS, SaaS [18], and Inter-host communication, message transfer, data processing, key management, the software development life cycle (SDLC), tools and services, metrics and economics, and software development life cycle (SDLC) were all covered by the IaaS security that was provided.

V. THE PROPOSED SYSTEM

Two different public key cryptosystems are cascaded to create the system (RSA and Rabin). The goal of utilizing a cryptosystem hybrid is to increase security beyond what would be possible using a single cryptosystem. All cloud-related data is expected to have already been encrypted. When using the cloud, a user is eligible for certain key generation (public and personal keys). The file is then encrypted using the suggested hybrid approach while being buffered on the cloud. The encrypted data sets are sent from the cloud to the knowledge nodes. Figure 2 depicts these actions. One component of cloud computing is a storage node, or "node," where metadata is stored and used to manage the directory's and who may access encrypted files. One or more blocks from a large group of knowledge nodes are used to create the encrypted file.

a- The Key Generation of the proposed method is shown below:

INPUT: Take the prime numbers p and q at random and their sizes.

OUTPUT: A public key, denoted by (n; e), and a private key (p,q,d) User A initiates communication with User B.

1. Create two random (and different) prime numbers, p and q, of about equal size (1).

2. Then, find n = p * q and = p * q -1.

3. Pick an integer e, 1 e , where the gcd (e;) equals 1.

4. Determine the one and only integer d, 1d, such that ed1 (mod), by employing the extended Euclidean algorithm.

5. Public key of the user is (n; e), and the private key is (d, p, q).

b- The encryption process of the proposed methods as shown below:

INPUT: To encrypt the user's public key, plaintext must be sent to them (n; e).

OUTPUT: Encrypted cipher text.

The message is sent from user A to user B. B should perform the following steps to encrypt:

1. Obtain the real public key for A. (n; e).

2. Next, place the message's integer representation, m, in the range [0, n1].

3. Third, find C = (m2e) mod n.

4. Have c, the encrypted message, sent to A.

c. Decryption process of the proposed algorithm as shown below

INPUT: The recipient's private key and the encrypted message were received.

OUTPUT: Original plaintext.

Following this procedure will allow B to extract plaintext m from c:

1. With d as the private key, calculate W=cd mod n.

2. Get the four square roots m1, m2, m3, and m4 of W modulo n.

3. The message delivered was one of the square roots m1, m2, m3, and m4.

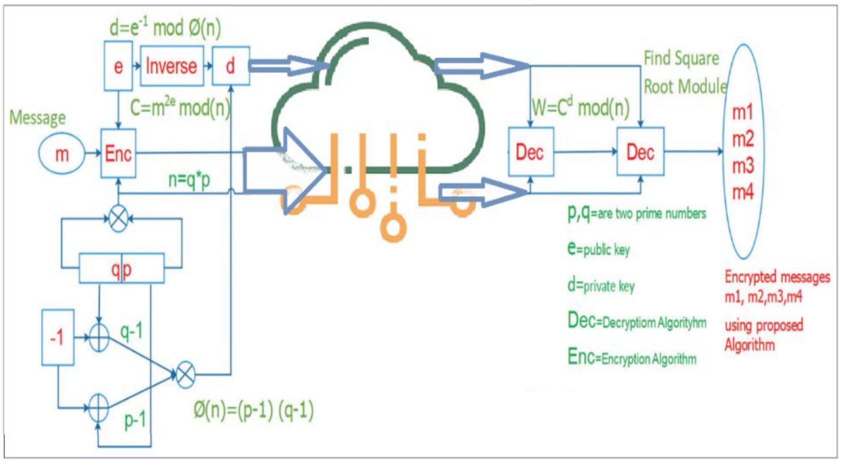

Figure 2 Model for cloud security.

VI. RESULT AND ANALYSIS

The foundation of cloud computing is virtualization-based data transport. You should, therefore, be concerned about data storage. When using cloud services, users should use the same caution they would with any other type of information system [16]. It's recommended practice for consumers to know where the storage host is located, for instance. Consumers have a right to know where their data is held and, if possible, the origins of any data that may have been collected and stored alongside it [2]. The four tenets of data security—confidentiality, authentication, integrity, and availability—must be ensured by cloud service providers [20]. In spite of the high demand for their offerings, service providers have significant difficulties in securing their consumers' private information. There is no way to justify the cost of keeping sensitive customer information hidden. To ensure that sensitive data is stored securely in the cloud, a more robust cloud security system was developed in response to this demand. Engineers employ both symmetric and asymmetric critical approaches to maximize safety.

Encrypting and decrypting data utilizing the RSA and recommended approach cryptosystems is time consuming. The O-notation has been helpful for both analysts and algorithm designers due to its ability to facilitate the systematic classification of algorithms based on their performance, leading the latter to the "optimal" methods for urgent problems. T (for time complexity) and S (for space complexity) are the typical units of measurement for computational complexity (for space complexity). The quantities T and S can be written as a function of the inputs, n. The time complexity of RSA encryption is shown in Eq. 1, whereas that of decryption is shown in Eq. 2.

The time constant,

$$T(c), = O(\log n)^3 \ (1)$$

$$T\ (m) = O(\log n)^3 \ (2)$$

We compare the encryption and decryption times of the suggested methods to those of the traditional public key cryptosystem (RSA) using randomly generated plaintext of varied lengths. FIGURE 3: Outcomes for Files of Formats for Various Sizes of Regular Text (100, 200, 300, 400, 500, 700, 900, and 1000 GB). Time requirements for encryption and decryption using RSA and the suggested methods are shown in Figures 3 and 4, respectively. See Figures 3 and 4 to see how the proposed method encrypts and decrypts data more quickly than the RSA cryptosystem.

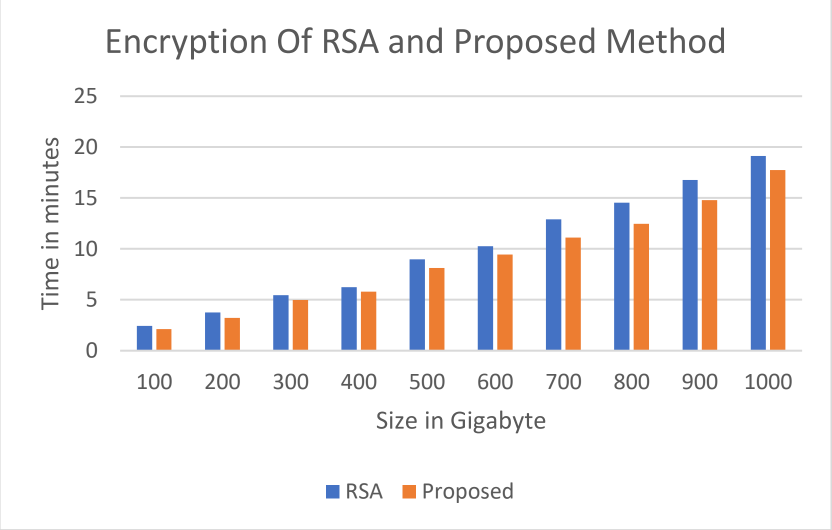

Figure 3 Time of encryption Process the file size in MB

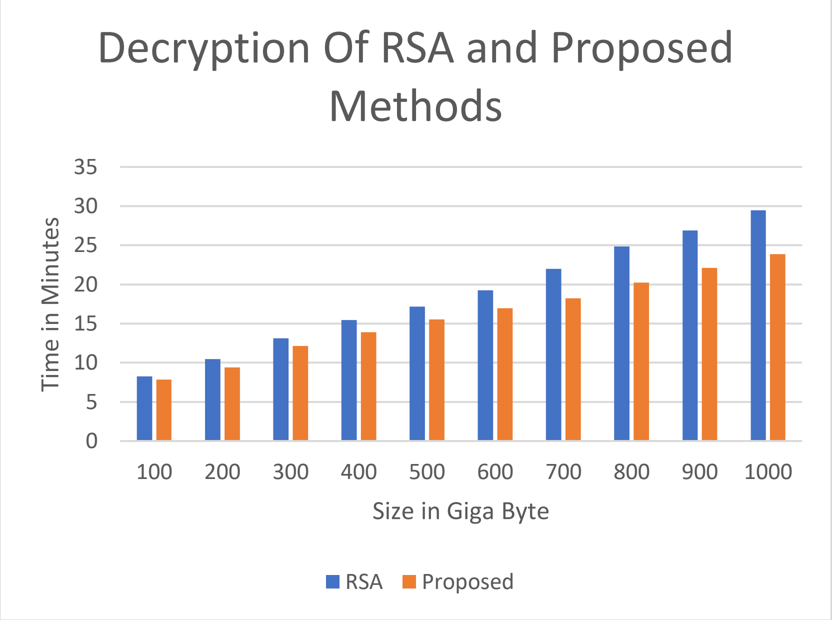

Figure 4 Time of Decryption Process the file size in MB

VII. CONCLUSION

Many concerns about the safety of cloud computing have been raised. The lack of strict privacy and security measures is one of cloud computing's drawbacks. The proposed model, which adapts RSA asymmetric key techniques, is built in Java and deployed in the wild.

Increased security in the cloud is achieved through the use of key generation, encryption, and decryption. The suggested method offers an improved method of developing and delivering encrypted software in the Cloud that is both faster and more secure. The proposed encryption approach works with most of the popular cloud computing service paradigms, including IaaS, SaaS, and PaaS. (PaaS). The proposed method showed remarkably low processing time overhead over a wide range of file sizes and degrees of complexity (double the computational complexity in the decryption stages). As time goes on, it will be required to merge the asymmetric key cryptosystems Rabin and RSA. In the proposed hybrid system, the time it takes to decrypt a message using the Rabin algorithm, which normally generates four alternative plaintexts, is a major weakness.

Bibliography

J.B.D. Joshi and Gail-Joon Ahn. Challenges with Security and Privacy in Cloud Computing Environments. IEEE Security Privacy Magazine, Volume 8, IEEE Computer Society, 2010, pages 24–31.

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

Aparna and Ashish Agarwal. the dangers of cloud computing for security. The International Journal of Computer Applications in Engineering Sciences is available online at vol. 1, special issue onCNS, July 2011, with ISSN 2231-4946.

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

M. Venkatesh, M. R. Sumalatha, and Mr. 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.

Amin Salih Mohammed Hersh A. Muhamad , Shahab Wahhab Kareem, "A Deep Learning Method for Detecting Leukemia in Real Images," NeuroQuantology, 2022.

Kamara, S., Lauter, K, Cloud storage with encryption:. 2010's Lecture Notes in Computer Science, volume 6054:136–49

Shahab Wahhab Kareemab Roojwan ScHawezia, Farah Sami Khoshabaa, "A comparison of automated classification techniques for image processing in video internet of things," 2022.

Zhijie Jerry Shi and Hai Yan. Software Elliptic Curve Cryptography Implementations. Third International Conference on Information Technology: New Generations, April 2006.

Suresha and Ravi Gharshi. Using the ECC Algorithm to Improve Cloud Storage Security. Volume 2, Issue 7, July 2013, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

Abdalwahid, S. M. J., Yousif, R. Z., & Kareem, S. W. (2019). Enhancing approach using hybrid pailler and RSA for information security in bigdata. Applied Computer Science, 15(4).

Modares, M. T. Shahgoli, H. Keshavarz, A. Moravejosharieh, and R. Salleh H. Make a Secure Connection Using Elliptic Curve Digital Signature. Volume 3, Issue 9 of the International Journal of Scientific and Engineering Research (IJSER), published in September 2012, ISSN 2229-5518.

Wang C, Cao N, Li J, Ren K, Lou Secure ranked keyword search over encrypted cloud data.. ACM W Journal, 43(3):431–73 (2010).

Ismael, R. S., Youail, R. S., & Kareem, S. W. (2014). Image encryption by using RC4 algorithm. European Academic Research, 2(4), 5833-5839.

Aparna and Ashish Agarwal. The International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946] published an article titled "The Security Risks Associated with Cloud Computing."

Mayank Namdev, Shiv Shakti Shrivastava, Animesh Kumar Dubey, and Ashutosh Kumar Dubey. RSA and MD5-Based Cloud-User Security for Java Environment Resource Attestation and Sharing CSI's Sixth International Conference on Software Engineering (CONSEG), September 2012.

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

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

A. Sudarsono, M. Yuliana, and H. A. Darwito, “A secure data sharing using identity-based encryption scheme for e-healthcare system,” in 2017 3rd International Conference on Science in Information Technology (ICSITech), pp. 1–9, Bandung, Indonesia, 2017.

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

S. Colaco and A. Krishna, “A random oriented identity based encryption process,” International Journal of Advanced Studies of Scientific Research, vol. 3, no. 8, pp. 9–17, 2018.

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

Farah Khoshaba, Shahab Kareem, Hoshang Awla, Chnar Mohammed, "Machine learning algorithms in Bigdata analysis and its applications: A Review," in International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2022, 2022.

Abdalwahid, S. M. J., Ibrahim, B. F., Ismael, S. H., & Kareem, S. W. (2022). A New Efficient Method for Information Security in Hadoop. QALAAI ZANIST JOURNAL, 7(2), 1115-1138.

R. Sakai and M. Kasahara, ID Based Cryptosystems with Pairing on Elliptic Curve, Cryptology ePrint Archive, 2003. Challenges and Security Issues in Cloud Computing, International Journal of Computer Networks, Vol. Kuyoro S. O., Ibikunle F., and Awodele O. 3, No. 5, pp. 247-255, 2011

Yogita Pawar and Prashant Rewagad are in. Enhancing Data Security in Cloud Computing through the Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm. International Conference on Network and Communication Technologies 2013, 2013.

Yousif, R. Z., Kareem, S. W., & Abdalwahid, S. M. (2020). Enhancing Approach for Information Security in Hadoop. Polytechnic Journal, 10(1), 81-87.

Larry Barret (27 July 2010). The SaaS market is expanding rapidly, according to Gartner. Computing.QuinStreet, Inc.

KAREEM, S. W. (2020). Secure Cloud Approach Based on Okamoto-Uchiyama Cryptosystem. Journal of Applied Computer Science & Mathematics, 14(29).

Tao Sun and Xinjun Wang. Data Security Model in Cloud Computing Platform for SMEs by. 2013; 7(6): 97–108; International Journal of Security and its Applications.

Luca Ferretti, Michele Colajanni, and Mirco Marchetti Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases by was published in IEEE Transactions on Parallel and Distributed Systems, Vol. February 2014. Volume 25, No. 2.

Shahab Wahhab Kareemab Roojwan ScHawezia, Farah Sami Khoshabaa, "A comparison of automated classification techniques for image processing in video internet of things," 2022.

Amin Salih Mohammed Hersh A. Muhamad , Shahab Wahhab Kareem, "A Deep Learning Method for Detecting Leukemia in Real Images," NeuroQuantology, 2022.

Farah Khoshaba, Shahab Kareem, Hoshang Awla, Chnar Mohammed, "Machine learning algorithms in Bigdata analysis and its applications: A Review," in International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2022, 2022.

Sami H. Ismael, Shahab W. Kareem, Firas H. Almukhtar, "Medical Image Classification Using Different Machine Learning Algorithms," AL-Rafidain Journal of Computer Sciences and Mathematics, 2020.

Kareem, Shahab Wahhab, Raghad Zuhair Yousif, and Shadan Mohammed Jihad Abdalwahid, "An approach for enhancing data confidentiality in hadoop," Indonesian Journal of Electrical Engineering and Computer Science, vol. 20, no. 3, pp. 1547-1555., 2020.

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

Abdalwahid, S. M. J., Yousif, R. Z., & Kareem, S. W., "Enhancing approach using hybrid pailler and RSA for information security in bigdata," Applied Computer Science, vol. 15, no. 4, 2019.

Anis S Mokhtar, Nurhayo Asib, A. R. R. . R. M. A. . (2022). Development of Saponin based Nano emulsion formulations from Phaleria macrocarpa to Control Aphis gossypii. Journal Of Advanced Zoology, 43(1), 43–55. Retrieved from http://jazindia.com/index.php/jaz/article/view/113

Faisal, H. T. ., Abid, M. K. ., & Abed, A. . (2022). Study Of Some Biochemical Parameters in Dose During Pregnancy in Goats. Journal Of Advanced Zoology, 43(1), 01–06. https://doi.org/10.17762/jaz.v43i1.109

Mokhtar, A. R. R. A. S. . (2022). Development Of Saponin Based Wettable Powder Formulation from Phaleria macrocarpa To Control Pomacea maculate. Journal Of Advanced Zoology, 43(1), 17–31. Retrieved from http://jazindia.com/index.php/jaz/article/view/111