Journal of Theoretical and Applied Information Technology
29th February 2024. Vol.102. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING CLOUD SECURITY BASED ON THE KYBER KEY ENCAPSULATION MECHANISM

IBRAHIM ALTARAWNI[1], MOHAMMED AMIN ALMAIAH[2,3], ANAS ALBADAREEN[4], KHALID ALTARAWNEH[5], , TAYSEER ALKHDOU[6], ABDALWALI LUTFI [7,8] AND MAHMAOD ALRAWAD[7]

[1]Faculty of Information Technology, Dept. of Computer science/Artificial Intelligence, Aqaba University of Technology.
[2]King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan
[3]Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
[4]Faculty of Information Technology, Dept. of software engineering, Aqaba University of Technology.
[5]Faculty of Information Technology, Mutah University, Det. of Data Science and Artificial Intelligence.
[6] Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[7] College of Business, King Faisal University, Al-Ahsa, 31982, Saudi Arabia
[8] MEU Research Unit, Middle East University, Amman, Jordan

E-mail: Corresponding authors: talkhdour@kfu.edu.sa and m.almaiah@ju.edu.jo

ABSTRACT

Due to its ability to provide flexible data processing and storage, cloud computing has become a crucial component of today's technological infrastructure. However, there is still serious concern about the security of data transferred and kept on the cloud. By integrating the Kyber Key Encapsulation Mechanism (KEM) into the cloud architecture, this article offers a revolutionary method of improving cloud security. A post-quantum cryptography method renowned for its strong defenses against quantum assaults is the Kyber KEM. The possibility of quantum threats to conventional encryption techniques is becoming more and more significant in cloud environments where sensitive data is exchanged and stored. Cloud service providers can strengthen their encryption protocols and guarantee that data is secure and private even in the face of developing quantum computing capabilities by including Kyber KEM. The application of Kyber KEM in a cloud security architecture is covered in this study, with a focus on how it may offer secure key exchange, data secrecy, and defense against quantum assaults. To further illustrate the usefulness and efficacy of Kyber KEM, its performance and efficiency in a cloud environment are assessed. Securing sensitive data processed and stored on the cloud requires the integration of cutting-edge cryptographic algorithms like Kyber KEM, especially in this day and age when data security is of utmost importance. This study is an important step in guaranteeing the integrity and privacy of cloud-based data since it clarifies how Kyber KEM can improve cloud security and defend against changing cyberthreats.
Keywords— *Cloud Security; Encapsulation Mechanism; Kyber Key; cryptographic algorithms.*

1. INTRODUCTION

Cloud computing has altered the way businesses and individuals store, analyze, and retrieve data. Its cost-effectiveness, scalability, and flexibility have made it an essential component of today's technological environment. But there are also serious privacy and data security issues raised by the use of cloud services. It is crucial to guarantee the privacy, availability, and integrity of data stored in the cloud. As a result, experts in the field and scholars have been investigating several strategies and tactics to protect sensitive data. Cloud security has gained significant attention in recent years, particularly with the growth of big data and the growing dependence on cloud infrastructures. Potential risks and vulnerabilities also increase with the amount of data generated and handled on the cloud. A multidisciplinary effort involving several areas, such as cryptography, behavioral modeling, and information security approaches, is required to address these issues and improve cloud security. Innovative solutions to strengthen cloud security have been offered by recent research efforts, based

on techniques like the NTRU Encrypt method [1], user behavioral models for CAPTCHA implementation [2], and effective Hadoop information security tactics [3]. Furthermore, the literature has explored the complexities of big data security problems and challenges [4], how to improve data confidentiality in cloud-based systems [5], and how to use safe cryptographic systems like Okamoto-Uchiyama Cryptosystem in cloud environments [6]. This introduction lays the groundwork for a thorough examination of the changing cloud security landscape. The aforementioned sources act as pillars, demonstrating the depth and breadth of this field's research. The following sections of this article will focus on particular facets of cloud security, drawing on these research and other pertinent contributions to create a thorough grasp of the difficulties, fixes, and best practices associated with protecting data in the cloud. The cloud components that may give rise to security concerns are depicted in Figure 1. Every component, including the network, policies, clients, and cloud infrastructure, is vulnerable to specific security threats and needs techniques for attack prevention, detection, and response [7].

The purpose of this study is to use the Kyber Key Encapsulation Mechanism (KEM) to improve cloud security. Although cloud computing has completely changed how services and data are handled and accessed, it also poses serious security risks, especially with regard to encryption and data protection. Since the also poses serious security risks, especially with regard to encryption and data protection. Since the Kyber KEM cryptographic algorithm is post-quantum secure, it offers a high degree of protection against attacks utilizing quantum computing. The purpose of this study is to deploy Kyber KEM and assess its efficacy within the framework of cloud security. We hope to improve the security and privacy of data kept on cloud servers by using this system, which would shield private data from new threats like quantum computing and other cutting-edge attack methods. This research makes a valuable contribution by offering a workable and efficient way to strengthen cloud security against changing cybersecurity threats. Our goal is to strengthen the security of private information in cloud environments by putting the Kyber Key Encapsulation Mechanism into practice. This study advances the fields of cloud security and cryptography by providing insightful information about the performance and applicability of Kyber KEM in a cloud security setting. The results of this study will give cloud service providers, businesses, and organizations a strong security framework to protect their data, guaranteeing information integrity and confidentiality in the face of new security threats. This will increase consumer confidence in and adoption of cloud computing technologies. The remaining portion of the study is a review of the literature that explores earlier studies and important discoveries about cloud security. The methodology, result, and discussion portions of the study are its main body, providing an explanation of the experimental design, methodology, and analytical conclusions regarding the effectiveness of Kyber KEM. In order to inspire confidence in cloud technologies, the Conclusion section concludes by succinctly summarizing the most important findings and highlighting the possible effects on cloud stakeholders.

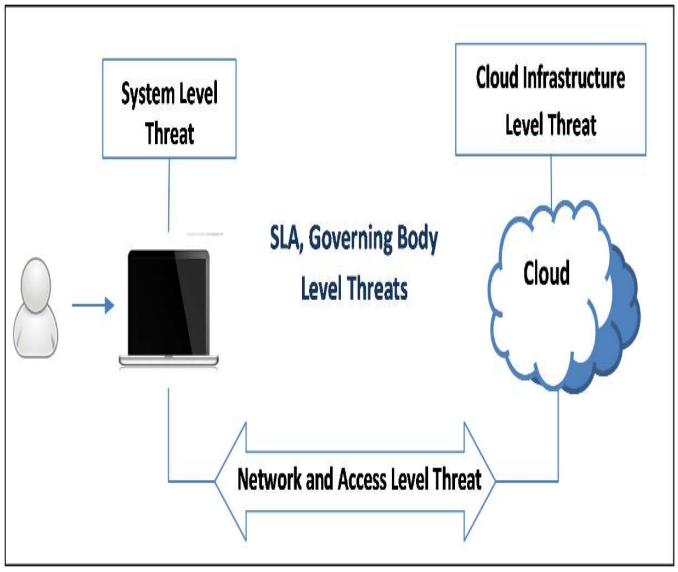

Figure 1. Cloud Components That Are Prone To Security Threats [7].

2. LITERATURE REVIEW

The introduction highlights the mounting issues caused by developing cyber threats and the crucial relevance of data security in cloud computing. It highlights how interdisciplinary approaches are needed to handle these problems and presents novel solutions like secure Hadoop data, user behavioral models for CAPTCHA [2], and the NTRU Encrypt technique [1]. The literature review then delves into previous academic contributions that tackle issues related to cloud computing security, cryptography systems such as the Okamoto-Uchiyama Cryptosystem, and big data security[5]. These key publications establish the framework for this study and offer a thorough grasp

of the changing cloud security landscape. The next sections explore particular facets of cloud security, referencing these foundational and pertinent publications to provide a thorough analysis of the problems, fixes, and industry best practices for cloud data protection. introduce a novel strategy in [6] with the goal of improving Hadoop's data secrecy, a crucial component in the big data space. This study, which was published in the Indonesian Journal of Electrical Engineering and Computer Science, highlights how crucial it is to protect data privacy in the setting of large-scale data processing and storage. The research tackles this issue by putting out a unique strategy to support data confidentiality in Hadoop systems, making a significant contribution to the big data security sector. a comparative analysis with an emphasis on cloud security ontologies [8]. The purpose of this study is to shed light on several ontological frameworks related to cloud security as shown in Figure 2.

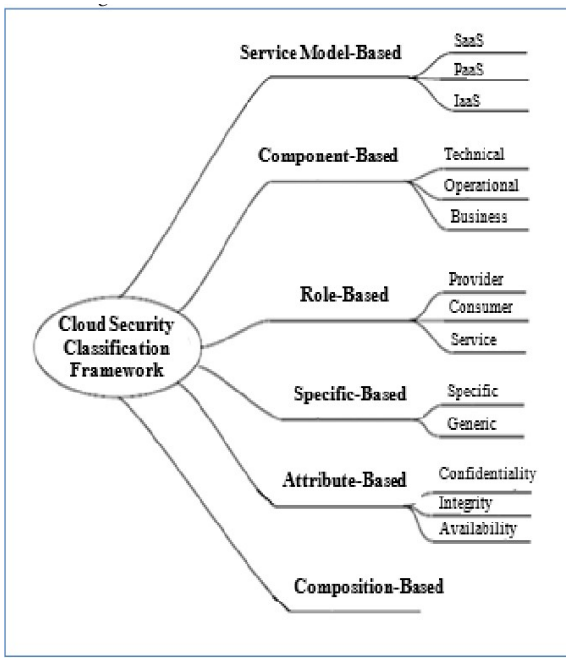

Figure 2. Cloud Computing Security Classification Framework [8]

Through comparison and analysis of various ontologies, the writers illuminated the complex field of cloud security, which is becoming more and more important in today's technological environment. The research outcomes provide significant insights for scholars and professionals, enabling a more profound comprehension of cloud security ontologies and their possible uses. Provide a novel strategy for improving information security in the context of big data in [9]. They use a hybrid cryptographic method to strengthen the security of sensitive data in the big data space by fusing the RSA and Paillier encryption approaches. Through the combination of these two encryption techniques, the authors hope to solve the complicated security issues brought on by the growing amount and complexity of big data. This study offers a novel approach that has the ability to effectively protect data integrity and privacy, contributing vital insights into information security in the big data era. In [10], a comparison of ontologies for cloud security, the analysis and comparison of several cloud security ontologies is the main goal of the work. The writers hope to improve their knowledge of cloud security concepts and how they relate to one another by looking at current ontological models. By offering a thorough comparison of various ontological approaches and illuminating the challenges of safeguarding cloud-based systems, the research makes a valuable contribution to the subject of cloud security. Difficulties and concerns regarding cloud security in their addition to the "Encyclopedia of Cloud Computing" [11]. The writers summarize the important issues and factors related to cloud security. They explore a number of cloud security topics, including compliance, privacy, and data protection. Researchers and practitioners in the field of cloud computing will find this paper to be a useful resource for comprehending the complex nature of cloud security challenges. The goal of this effort [12] is to enhance Hadoop, a well-known big data platform, in terms of information security. The writers talk about a cutting-edge strategy meant to improve data security in Hadoop deployments. They cover important topics on the privacy and security of data. In order to make a contribution to the rapidly developing field of big data security, the authors have proposed and implemented their security strategy, which is depicted in Figure 3.

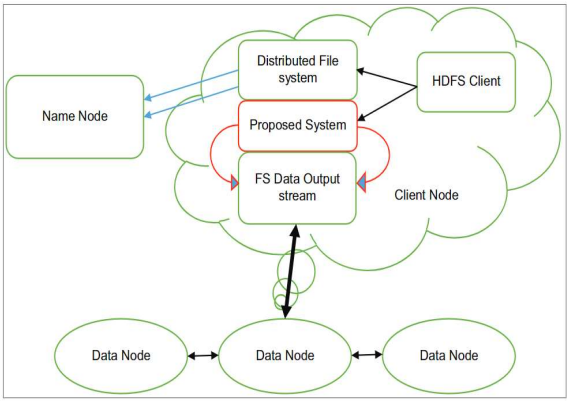

Figure 3 Security Procedure In HDFS [12]

Given the growing significance of data security in big data ecosystems, this article provides insights and methods for protecting sensitive data in Hadoop. The writers examine the ever-changing field of cloud security in [13]. They explore new vulnerabilities and threats that impact cloud environments. The study offers a thorough analysis of current mitigation strategies and responses for these security issues. Through an examination of the latest dangers and viable remedies, the article provides insightful information about cloud security. It acts as a thorough resource for learning about the security posture of the cloud today and the safeguards put in place to secure data and services hosted on the cloud. Focusing on the cloud computing paradigm and the related security issues in [14]. The writers recognize how cloud computing has revolutionized a number of industries, most notably healthcare and education. They draw attention to the serious security risks and challenges that come with implementing cloud computing. In doing so, the article provides insightful information about the issues related to cloud security and the necessity of strong security measures in cloud-based systems, particularly in settings such as healthcare and education. The authors acknowledge that cloud computing is becoming more and more important, and that this presents security issues. As a result, they methodically look at how machine learning approaches may improve cloud security. A number of topics are covered in the paper, including the use of machine learning in cloud systems for anomaly, intrusion, and threat detection [15]. This paper provides insights into the potential of machine learning to reduce security threats in cloud-based systems and is a useful resource for understanding the present state of machine learning solutions in the cloud security space. Table 1 shows the comparison of some of the related works, the table presents some of the paper's aims, contributions, and purposes of these papers.

3. RESEATCH METHODLOGY

This paper focuses on Hadoop, a top supplier of cloud-based large-scale data processing and storage, and offers a novel method for improving the security of cloud data processing and storage. The inclusion of the Kyber Key Encapsulation Mechanism (KEM) is necessary for this method to accomplish homomorphic encryption and handle cipher limitations. Here is a thorough explanation of this procedure: Hadoop is a popular technology for handling and archiving massive amounts of cloud data. Strong encryption technologies are emphasized in order to protect data.

The mechanism of Kyber Key Encapsulation (KEM): The Kyber KEM, a cryptographic method intended to protect data from quantum-based assaults, lies at the core of the procedure. Because Kyber KEM provides post-quantum security, it is resistant to the processing power of quantum computers.

Data Encryption for Hadoop: To improve security, each file written on the Hadoop Distributed File System (HDFS) needs to be encrypted beforehand.

Table 1 Comparison Of Related Works In The Cloud Security

Comparison of related works in the cloud security				
	Models Used	**Aim**	**Contribution Purpose**	**Scenario**
[16]	Not specified in the paper	Identifying cloud security threats for cloud adoption	Identify and analyze security threats in cloud computing	Cloud computing adoption framework
[17]	Virtualization	Mobile Devices	Virtualized in-cloud security services for mobile devices	Propose virtualized security services for mobile cloud computing
[18]	| Not specified in the paper	Assessing innovations in cloud security	Evaluate and assess innovative security approaches	Cloud security innovations
[19]	Supervised Machine Learning	Feasibility of supervised machine learning for cloud security	Investigate the feasibility of using supervised machine learning for security	Cloud security with machine learning

[20]	Not specified in the paper	Cloud security and privacy model	Propose a model for secure cloud services	Secure cloud service model
[21]	Not specified in the paper	Internet of cloud: Security and privacy issues	Discuss security and privacy issues in the Internet of Cloud	Internet of Cloud
[22]	Broker-Based Framework	Standardization and management of Cloud Security-SLAs	Propose a broker-based framework for managing Cloud Security Service Level Agreements	Cloud Security SLAs
[23]	Not specified in the paper	Cloud security engineering	Discuss early stages of cloud security in the System Development Life Cycle	Cloud security in SDLC
[24]	Taxonomy, Intrusion Detection	Cloud security attacks taxonomy and intrusion detection	Present a taxonomy for cloud security attacks and intrusion detection	Cloud security attacks and detection
[25]	Cloud Security Algorithms	Cloud security algorithms	Discuss various cloud security algorithms	Cloud security with different algorithms

Client Liability for HDFS: The public and private keys must be managed by the HDFS Client.
The suggested technique encrypts files while they are being written to HDFS by utilizing Kyber KEM.
Type of Data: Unstructured data is the category for the data that HDFS is used to store.
Transmission of Data: HDFS starts transferring encrypted files to data nodes once they have been encrypted.

Parts of the HDFS: HDFS is made up of several parts, such as Name Node: In charge of overseeing the file system namespace, this node handles metadata. It also manages client access to files that are encrypted. Data Nodes is A group of data nodes stores and distributes one or more blocks that make up encoded files. The stages involved in this process are illustrated clearly in Figure 4 of the article, which shows how files are encrypted before being transmitted to HDFS data nodes.
A post-quantum cryptography method called the Kyber Key Encapsulation Mechanism (KEM) is utilized for safe key exchange and data encryption. It offers a method for two parties to safely exchange a symmetric key via an unsecure channel. The following is a comprehensive process that uses Kyber KEM for both encryption (key encapsulation) and decryption (key decapsulation), with mathematical explanations provided for each step:
Key Generation: The sender (Alice) and the recipient (Bob) must each generate their unique key pairs before any data can be transferred. These key pairs are made up of a private key and a public key. While the private key needs to be kept confidential, the public key is known to everybody. The generation of key pairs can be shown as:
The key pair for Alice is (pk_Alice, sk_Alice), and Bob's Key Pair: (pk_Bob, sk_Bob).
Encryption (Key Encapsulation): Random Session Key Generation: Alice generates a random session key, K_sess, before she may send Bob a secure communication. The actual message is encrypted and decrypted using this symmetric session key. In terms of math, this is represented as: Random() is K_sess.
Alice encrypts the session key using Bob's public key (pk_Bob) in order to perform key encapsulation. The Kyber encryption algorithm, also known as Enc_Kyber, is used during the encapsulation procedure. This procedure yields the encapsulated key (ct_key): Enc_Kyber(K_sess, pk_Bob) = ct_key
Transferring the Condensed Key: Together with the encrypted message, Alice sends Bob the encapsulating key (ct_key).
Key decapsulation, or decryption: Encapsulated Key Reception: Alice sends Bob the encrypted message plus the encapsulated key (ct_key). Additionally, Bob has his private key (sk_Bob), which is the same as his public key and is utilized for key encapsulation.
Key Decapsulation: Bob extracts the session key from the encapsulated key using his private key (sk_Bob) and the Dec_Kyber Kyber decryption technique. The outcome is the session key (K_sess), which is employed in the decoding of messages:
Dec_Kyber(ct_key, sk_Bob) = K_sess
Message Decryption: Bob can now decrypt the encrypted message using the symmetric encryption algorithm, known as Dec_symmetric, using the session key (K_sess) that he acquired via the key decapsulation step. Here is the initial message (msg) as a result:
message = Dec_symmetric(K_sess, encrypted_msg)

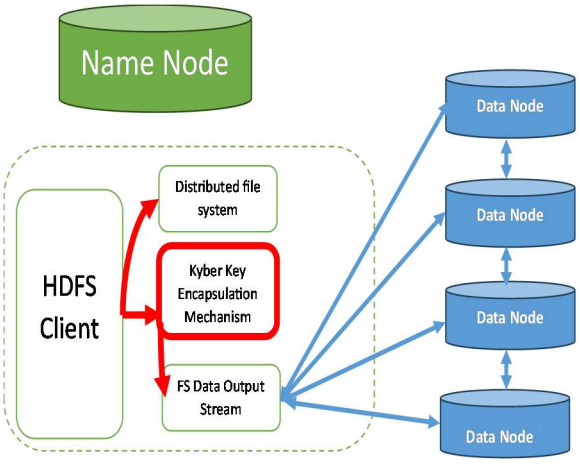

Figure 5 Proposed Model For Cloud Security Applying In Hadoop Framework As A Cloud

Exchange of Messages: Bob can view the message and reply after it has been encrypted. In a similar manner, Bob would encrypt messages securely by encasing Alice's public key in a session key in any reply to her.

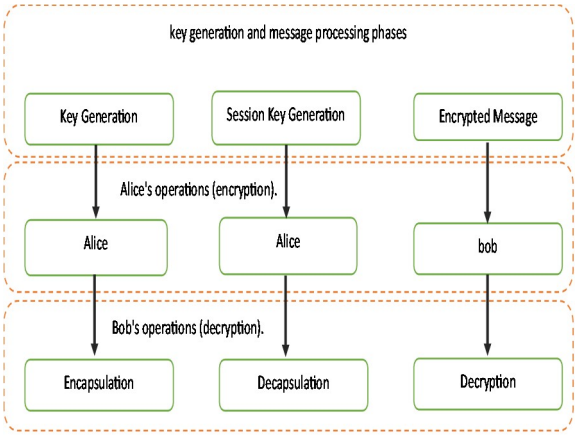

Figure 6 Text-Based Representation Of A Block Diagram For Kyber KEM

In conclusion, the Kyber Key Encapsulation Mechanism permits two parties to exchange session keys in a way that is resistant to quantum mechanics, ensuring safe communication. How the security of the key exchange and the message's confidentiality are preserved is demonstrated by the mathematical depiction of the key encapsulation and DE capsulation processes. The size of the key and particular operations are two of the elements that affect the time complexity of public key encryption systems such as ElGamal, RSA, and Kyber KEM. The time complexities for these encryption techniques are summarized as follows:

Cyber KEM, or the Kyber Key Encapsulation Mechanism: Key generation takes place in steps of O(n^2) to O(n^3), depending on the particular set of Kyber parameters (e.g., Kyber512, Kyber768, Kyber1024), where "n" is the degree of the polynomial. Similar to key generation, encryption operates between O(n^2) and O(n^3), depending on the parameter configuration. Decryption: O(n^2) to O(n^3), akin to the processes of encryption and key generation. Kyber is effective and useful for post-quantum security since its time complexity is polynomial in the security parameter.

Rivest-Shamir-Adleman, or RSA: O(k^3) is the key generation time, where "k" is the modulus's bit length. O(k^2) is the encryption algorithm, where "k" is the modulus's bit length. O(k^3) is the decryption time, where "k" is the modulus bit length. RSA's time complexity is polynomial in the modulus's bit length. In ElGaramal O(k^3) is the key generation time, where "k" is the modulus's bit length. O(k^2) is the encryption algorithm, where "k" is the modulus's bit length. O(k^3) is the decryption time, where "k" is the modulus bit length. ElGamal's temporal complexity is likewise polynomial in the modulus's bit length. It is crucial to remember that the precise implementation and optimizations employed can affect the real time complexity. These time complexities are also approximations that could change depending on different hardware and software configurations. In reality, the chosen encryption technique is frequently determined by the desired level of post-quantum security as well as the particular security requirements. Kyber KEM is a well-liked option for contemporary cryptographic applications because of its efficient design and robust post-quantum security. Although ElGamal and RSA are frequently utilized in conventional cryptography settings, they are typically less resistant to quantum attacks.

4. RESULTS AND DISCUSSIONS

The Hadoop Distributed File System (HDFS) and MapReduce have been utilized to evaluate the effectiveness of HDFS encryption on nodes that have an Intel i7-core processor, 16 TB of HDD storage, and 32 GB of RAM. The encryption time can be defined as the amount of time needed to apply the Key Encapsulation Mechanism (KEM) technique to Hadoop-separated data files; on the other hand, the decryption time is the amount of time needed to transform the ciphertext back into plaintext.

As seen in Figure 6, the study compares the effectiveness of the KEM, RSA, and hybrid

encryption methods[12] over a range of file sizes. With incremental step sizes, the suggested method showed consistently better time efficiency than RSA for all file sizes between 10 MB and 1000 MB. The findings of a comparison between the KEM, RSA, and Hybrid models in [12] for various file sizes are shown in Figure 7. The suggested method routinely beats RSA in terms of time consumption for data sizes between 100 MB and 1000 MB, with the step size growing with each repetition.

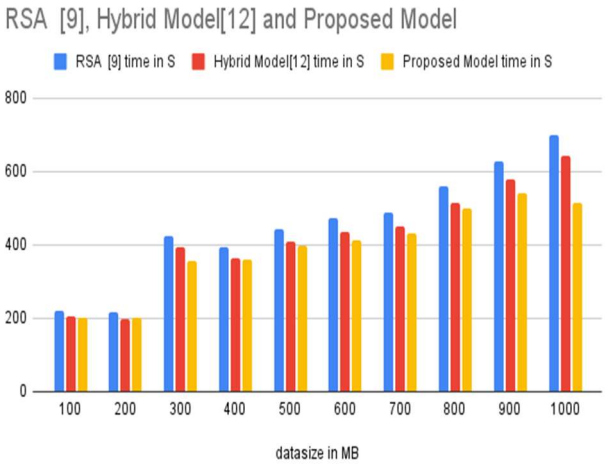

Figure 6 Encryption Running Time In Seconds

As a result, in the encoding step, the suggested method—known as the Proposed Algorithm—proves to be quicker than the RSA and Hybrid models in [12]. An illustration of the KEM, RSA, and hybrid models' performance is given in Figure 7 in [12]. We have so far worked with encoded files of different sizes, and the suggested approach shows faster decoding times than the previously discussed approaches.

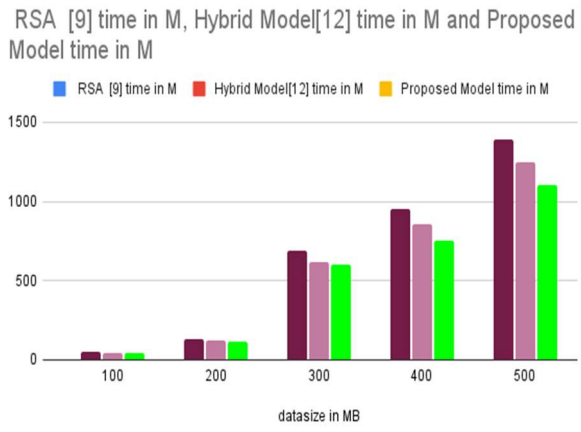

Figure 7 Decryption Running Time In Minutes

5. CONCLUSION

This study has introduced a thorough technique with a special focus on Hadoop, a well-known technology in this field, which aims to improve the security of cloud-based data processing and storage. The security of data in a cloud environment has been ensured by the use of the Kyber Key Encapsulation Mechanism (KEM), which has been crucial in accomplishing homomorphic encryption and surmounting the constraints of conventional cyphers. One of the most important post-quantum cryptography techniques for protecting data from quantum-based assaults is the Kyber KEM. The method's main components—data encryption for Hadoop, client management of public and private keys, and the encryption procedure for unstructured data in HDFS—have been clarified in this work. Key generation, encryption, and decryption are all included in the detailed application of Kyber KEM for safe key exchange and data encryption. The steps involved in facilitating secure communication have been outlined, together with the mathematical foundations that support these processes. Additionally, the study contrasted the time complexity of other encryption methods, such as ElGamal, RSA, and Kyber KEM, highlighting the effectiveness and resistance of Kyber KEM to quantum attacks. It is clear from the results and discussion section that the Proposed Algorithm—which makes use of the Kyber KEM—performs better than the Hybrid model and RSA in terms of encryption and decryption times for a variety of file sizes. The suggested method's efficacy is further supported by the graphic display of this higher time efficiency. By presenting and confirming the Kyber Key Encapsulation Mechanism as a reliable option for secure data processing and storage in cloud-based systems, this research has advanced cloud data security. The results show how much better it performs than before and emphasize how crucial post-quantum security is for modern cryptographic applications. The approach and findings discussed here provide insightful information for businesses looking to improve the security of their cloud-based data processing and storage infrastructure.

6. ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. 5920).

REFERENCES

[1] Yousif, M. K., Dallalbashi, Z. E., & Kareem, S. W. (2023). Information security for big data using the NTRUEncrypt method. *Measurement: Sensors*, *27*, 100738.

[2] Awla, H. Q., Mirza, A. R., & Kareem, S. W. (2022, February). An Automated CAPTCHA for Website Protection Based on User Behavioral Model. In *2022 8th International Engineering Conference on Sustainable Technology and Development (IEC)* (pp. 161-167). IEEE.

[3] 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.

[4] KAREEM, S., HASAN, A., HAWEZI, R., MUHEDEN, K., & KHOSHABA, F. (2021). Big Data Security Issues and Challenges. Journal of Applied Computer Science & Mathematics, 15(32).

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

[6] 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.

[7] Khalil, I., Khreishah, A., & Azeem, M. (2014). Cloud Computing Security: A Survey. Computers, 3(1), 1–35. MDPI AG. Retrieved from http://dx.doi.org/10.3390/computers3010001.

[8] Singh, V., & Pandey, S. K. (2014). A comparative study of Cloud Security Ontologies. In Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimisation (pp. 1-6). Noida, India. doi:10.1109/ICRITO.2014.7014763.

[9] 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), 63-74.

[10] Singh, V., & Pandey, S. K. (2014, October). A comparative study of cloud security ontologies. In *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization* (pp. 1-6). IEEE.

[11] Samarati, P., & De Capitani di Vimercati, S. (2016). Cloud security: Issues and concerns. *Encyclopedia of cloud computing*, 205-219.

[12] Yousif, R. Z., Kareem, S. W., & Abdalwahid, S. M. (2020). Enhancing approach for information security in hadoop. *Polytechnic Journal*, *10*(1), 81-87.

[13] Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*, *59*, 126-140.

[14] Yandong, Z., & Yongsheng, Z. (2012, August). Cloud computing and cloud security challenges. In *2012 International Symposium on Information Technologies in Medicine and Education* (Vol. 2, pp. 1084-1088). IEEE.

[15] Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. *IEEE Access*, *9*, 20717-20735.

[16] Khan, N., & Al-Yasiri, A. (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. *Procedia Computer Science*, *94*, 485-490.

[17] Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., & Jahanian, F. (2008, June). Virtualized in-cloud security services for mobile devices. In *Proceedings of the first workshop on virtualization in mobile computing* (pp. 31-35).

[18] Khansa, L., & Zobel, C. W. (2014). Assessing innovations in cloud security. *Journal of Computer Information Systems*, *54*(3), 45-56.

[19] Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2016, December). Feasibility of supervised machine learning for cloud security. In *2016 International Conference on Information Science and Security (ICISS)* (pp. 1-5). IEEE.

[20] El Makkaoui, K., Ezzati, A., Beni-Hssane, A., & Motamed, C. (2016, May). Cloud security and privacy model for providing secure cloud services. In *2016 2nd international conference on cloud computing technologies and applications (CloudTech)* (pp. 81-86). IEEE.

[21] Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K., & Janicke, H. (2018). Internet of cloud: Security and privacy issues. *Cloud Computing for Optimization: Foundations, Applications, and Challenges*, 271-301.

[22] Halabi, T., & Bellaiche, M. (2018). A broker-based framework for standardization and

management of Cloud Security-SLAs. *Computers & Security*, *75*, 59-71.

[23] Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, *74*, 385-392.

[24] Iqbal, S., Kiah, M. L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K. K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications*, *74*, 98-120.

[25] Pansotra, E. A., & Singh, E. S. P. (2015). Cloud security algorithms. *International journal of security and its applications*, *9*(10), 353-360.