Journal of Theoretical and Applied Information Technology
15th April 2024. Vol.102. No 7

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

A HYBRID MODEL OF RSA AND NTRU FOR SECURING OF CLOUD COMPUTING

KHALID ALTARAWNEH[1], IBRAHIM ALTARAWNI[2], MOHAMMED ALMAIAH[3,4], MUSTAFA HAMMAD[5], TAYSEER ALKHDOUR[6], ROMMEL ALALI[7], ABDALWALI LUTFI[8,9], MAHMAOD ALRAWAD[9]

[1]Faculty of Information Technology, Mutah University, Det. of Data Science and Artificial Intelligence.
[2]Faculty of Information Technology, Dept. of Computer science/Artificial Intelligence, Tafila Technical University.
[3] King Abdullah the II IT School, the University of Jordan, Amman 11942, Jordan
[4] Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
[5]Faculty of Information Technology, Dept. of software engineering, Mutah University.
[6] College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[7]Associate Professor, The National Research Center for Giftedness and Creativity, King Faisal University, Saudi Arabia.
[8] College of Business, King Faisal University, Al-Ahsa, 31982, Saudi Arabia.
[9] MEU Research Unit, Middle East University, Amman, Jordan
Corresponding authors: talkhdour@kfu.edu.sa and m.almaiah@ju.edu.jo

ABSTRACT

Cryptographic techniques are essential in guaranteeing the security and confidentiality of data in cloud computing, which is a critical concern. In order to provide a strong and secure solution for cloud computing environments, this study presents a novel hybrid cryptographic architecture that combines the characteristics of RSA for key exchange with NTRU for data encryption. The suggested hybrid paradigm places an emphasis on effective cloud key management and the safe implementation of cryptographic operations. The approach creates a secure framework for cryptographic key distribution by using RSA for key exchange, guaranteeing the confidentiality of data while it is being transmitted. Data encryption using NTRU, a quick and effective encryption method, improves the security of data processed and stored on the cloud. Because of its strong encryption capabilities, NTRU is a good fit for the requirements of cloud computing, where security and performance are critical factors. This hybrid model's RSA and NTRU synergy provides a well-rounded solution to the security issues associated with cloud computing. With RSA's key exchange capabilities and NTRU's robust data encryption, the model offers a comprehensive solution that secures data in the cloud during its entire lifecycle. In conclusion, this work presents a secure, effective, and flexible hybrid paradigm combining NTRU and RSA cloud computing security. This approach helps enterprises safeguard their data while making use of cloud computing technologies by highlighting the critical components of secure cryptographic operations and cloud key management.

Keywords: *Cryptography, Security, RSA, NTRU, Cloud Computing.*

1. INTRODUCTION

Cloud computing has completely changed how we handle, share, and store data. It is a desirable option for both individuals and businesses due to its unmatched flexibility, scalability, and cost-efficiency. But this ease is accompanied by a serious worry: the security and privacy of the data stored in the cloud. Protecting data from breaches and unauthorized access is crucial when data is transferred and stored remotely [1]. A solid way to improve data security in cloud computing is public key encryption, which is a basic cryptography approach. Two keys are needed for this method: a private key for decryption and a public key for encryption. A key component of cloud computing security is data encryption, which protects private data from breaches and illegal access. Public key encryption is one of the many cryptographic algorithms that is essential for guaranteeing data integrity and secrecy in the cloud. Using a public key for encryption and a private key for decryption, this technique provides a strong mechanism to safeguard data at every stage of its lifetime. on this digital age, public key encryption is essential for protecting the data processed, transferred, and stored on the cloud. Data is the lifeblood of both individuals and organizations. By employing

public key encryption, researchers in the fields of cloud computing and cryptography have significantly improved data security in the cloud. They have made modifications to cryptographic systems, effective security algorithms, and sophisticated encryption frameworks. These contributions address the particular security requirements faced by cloud and IoT contexts, while significantly strengthening data protection. Furthermore, the development of keyword search and dual-server public-key encryption improves data retrieval while upholding strong security. Together, these developments strengthen the security of data handled and stored in the cloud and provide all-encompassing solutions for the changing cloud computing environment. Figure 1 shows the security of cloud computing [2].

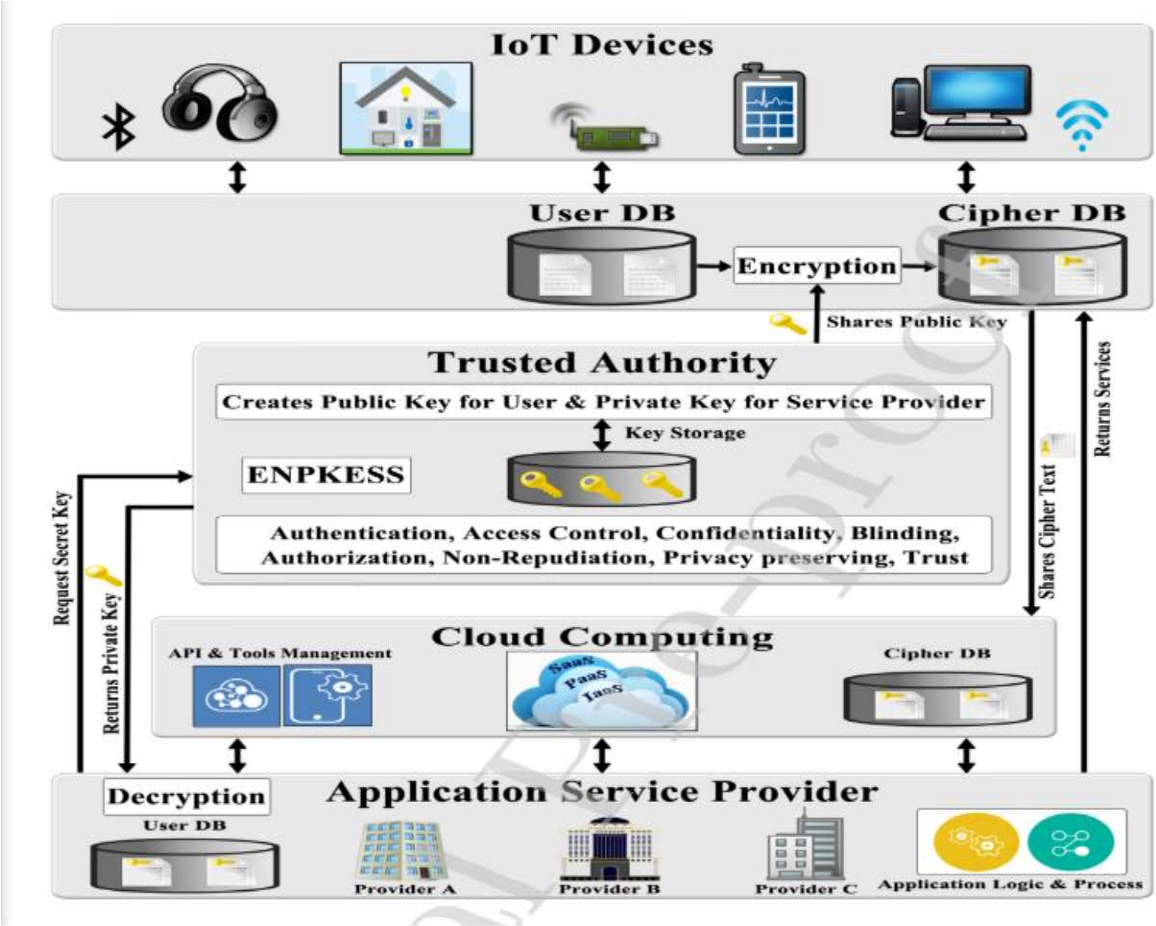

Figure 1 security of cloud computing [2].

The rest of the paper is organized as follows, the second section of the literature review explores recent advancements and research in the subject of data encryption in cloud computing. Public key encryption is used in section 3 of the methodology section to describe the methods and techniques used in this study to improve data security in cloud computing. The fourth section is The study's findings are presented in the discussion and analysis section, which provides a thorough analysis of the findings and their consequences. The conclusion is the final portion. The research's main conclusions are outlined in the conclusion section, which also offers a succinct evaluation of how well the hybrid RSA-NTRU architecture enhances cloud data security.

2. LITERATURE REVIEW

The ever-changing threat landscape and the vital significance of protecting data and services in the cloud have led to a great deal of study and development into cloud computing security. This review of the literature looks at important topics, issues, and advancements in the subject of cloud computing security, incorporating information from a variety of academic publications, research studies,

and real-world applications. The specific difficulties presented by the cloud environment are highlighted in the literature on cloud computing security. These include issues with data privacy, the necessity for safe access controls, data breaches, and the shared responsibility paradigm. Researchers as crucial ones that call for ongoing focus and creativity have recognized these issues. In the study [1] the goal of the project is to secure data by combining symmetric and asymmetric key encryption methods. Given the widespread use of cloud services, the paper tackles the important problem of protecting data on the cloud. The authors present a novel strategy to guarantee strong data security in the cloud that combines symmetric and asymmetric key encryption techniques. With the efficiency of symmetric key encryption and the increased security of asymmetric key encryption, this method makes use of the best features of both encryption paradigms. The goal of the hybrid approach is to address the drawbacks and security holes that come with using just one encryption technique. The goal of the authors' hybrid encryption model is to improve data security in general. A study [3] the authors discuss how important it is to secure data kept in cloud environments, where confidentiality and privacy of data are top priorities. They suggest modifying the well-known and reliable RSA public key cryptosystem in order to address this problem. The goal of this update is to enhance the efficiency and security of the RSA algorithm for cloud data storage. By presenting a method that strikes a balance between efficiency and security, the work advances the field of cloud computing security. A significant factor for cloud-based applications is computational overhead, which is why the modified RSA public key cryptosystem is made to minimize it while still offering strong data protection. The important issues of data privacy and searchability are addressed in [4], which presents a novel method for safe cloud data storage. In order to improve the security and usability of data stored in the cloud, the research focuses on developing a Dual-Server Public-Key Encryption with Keyword Search (DS-PKEKS) system. The expanding significance of secure cloud storage, where data is frequently kept remotely and accessed from several locations, is acknowledged by the writers. This paper proposes the DS-PKEKS system to guarantee data privacy and effective data retrieval. This technology lets users safely store their data in the cloud while still enabling keyword searches for specific information. It does this by combining public-key encryption with keyword search. The research offers a workable approach for safe cloud storage that does not sacrifice search capabilities, which makes a substantial contribution to the field of cloud security. Because of its ability to guarantee data security and privacy, the DS-PKEKS system is appropriate for a range of cloud-based applications where data confidentiality is crucial. The goal of the research is to offer a comprehensive model that takes into account many facets of cloud security and privacy [5]. It proposes ways to reduce possible dangers while taking into account the difficulties and weaknesses related to cloud computing. The writers stress the value of safe cloud services, especially for companies and institutions that use the cloud to handle and store sensitive data. The proposed model, which acts as a guide for safeguarding cloud services, is the paper's main contribution. The authors present a path for cloud service providers and customers to guarantee data protection, access management, and compliance with privacy rules by providing a framework that integrates security and privacy safeguards.

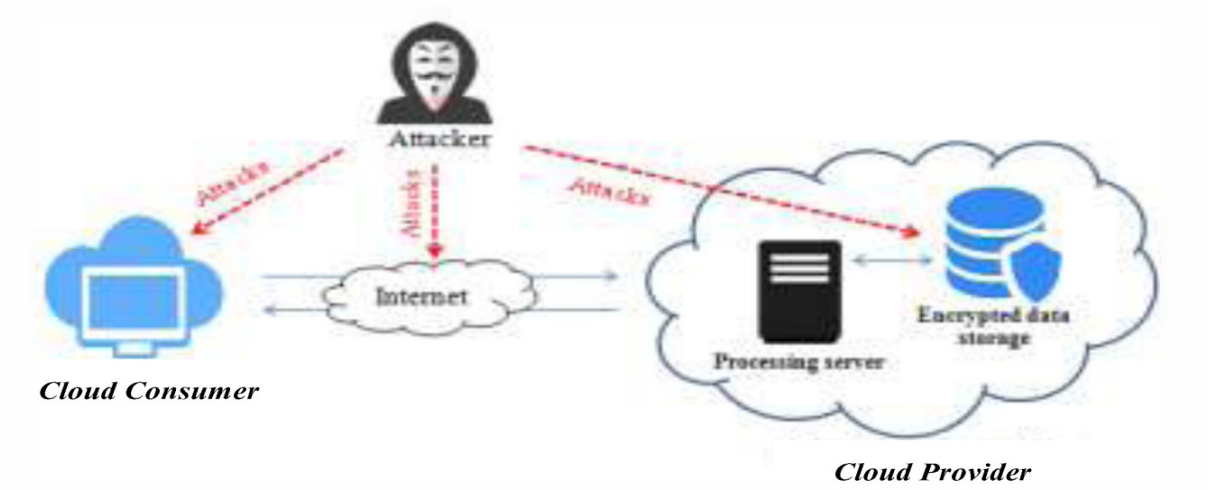

Figure 2 Scenarios of cryptographic attacks against cloud computing

The important subject of information security for big data is covered in [6], with a focus on using the NTRUEncrypt technique. With an emphasis on the NTRUEncrypt technique, the research presented in this paper attempts to offer a practical strategy for massive data security. In the context of big data, the authors examine the application of NTRUEncrypt, a public-key cryptosystem renowned for its robust security features. The paper's contribution is showing how big datasets may be encrypted and protected using the NTRUEncrypt technique. In doing so, it tackles the special difficulties that come with handling the volume and complexity of big data, which presents a new and effective technique in [7] to improve information security in Hadoop, a popular platform for distributed big data processing and storing. Information security is crucial when it comes to big data, and Hadoop is a popular framework for handling massive datasets. In order to address the need for strong security measures within Hadoop, this paper suggests a novel approach. The creation and application of this novel security technique are the main contributions made by the writers in this work. The goal of the project is to safeguard data from unauthorized access and data breaches by strengthening Hadoop's security features. Organizations and data professionals who depend on Hadoop for big data processing and management should find value in the research findings. In a time when data breaches and cyber dangers are increasing, the paper's practical significance is highlighted by its emphasis on effective security solutions for Hadoop. This work addresses a major issue in the big data industry by presenting a useful and novel way to improve information security in the Hadoop ecosystem. The suggested approach may improve an organization's overall security posture if it uses Hadoop for analytics and data management purposes. In a study conducted by [8] This paper's author's contribution is the creation and application of a better strategy for Hadoop information security. By taking this strategy, Hadoop becomes a more secure environment for large data operations by reducing the likelihood of data breaches, unauthorized access, and other security problems. The research holds great importance since it has practical consequences for professionals and organizations that handle massive databases. The work advances the larger objective of protecting sensitive and important data in the big data era by addressing the security concerns of Hadoop. In line with the increasing demand for strong security measures in the big data space, this paper presents an improved method for bolstering information security in Hadoop. The suggested method may strengthen an organization's overall security posture if it uses Hadoop for analytics and data processing. Table 1 shows the comparison of some related works for the purpose of papers, aims and contributions.

Table 1 shows the comparison of some related works for the purpose of papers, aims and contributions.

Paper	Security Models	Aim of Paper	Contribution	Methods	Purpose of Model
[1]	Cloud Security Framework	Confirm data security using asymmetric and symmetric key encryption	Enhanced security framework	Asymmetric and symmetric key encryption	Data security confirmation
[2]	Public Key Secure Scheme	Cloud and IoT security	An efficient secure scheme	Public key cryptosystem	Security in cloud and IoT
[3]	Modified RSA Public Key Cryptosystem	Secure data storage	Efficient and secure data storage	Modified RSA public key cryptosystem	Data storage security
[4]	Dual-Server Public-Key Encryption	Keyword search for secure cloud storage	Secure cloud storage with keyword search	Public-key encryption with keyword search	Secure cloud storage and retrieval
[5]	Cloud Security and Privacy Model	Secure cloud services	A security and privacy model	Model development	Providing secure cloud services
[6]	NTRUEncrypt Method	Information security for big data	Information security using NTRUEncrypt	NTRUEncrypt method	Securing big data
[7]	Efficient Method for Information Security in Hadoop	Information security in Hadoop	A new efficient method	Method development	Enhancing Hadoop security
[8]	Enhancing Approach for Information Security in Hadoop	Information security in Hadoop	Enhanced security approach	Approach development	Improving Hadoop security
[9]	Data Confidentiality in Hadoop	Data confidentiality enhancement	Enhanced data confidentiality approach	Approach development	Enhancing data confidentiality
[10]	Hybrid Pailler and RSA	Information security in big data	Security enhancement using hybrid Pailler and RSA	Hybrid encryption method	Enhancing Big Data Security
[11]	Public Key Cryptography with Matrices	Security in cloud computing	Security enhancement using matrix-based public key cryptography	Matrix-based public key encryption	Enhancing cloud security
[12]	Hybrid (RSA & AES) Encryption Algorithm	Data security in the cloud	Enhanced data security using hybrid encryption	RSA and AES hybrid encryption	Enhancing cloud data security
[13]	Secure Searching over Public-Key Ciphertexts	IoT device security	Lightweight secure searching	Lightweight secure searching over public-key ciphertexts	Security for industrial IoT
[14]	Multilevel Encryption Technique	Cloud Security	Multilevel encryption technique	Multilevel encryption	Enhancing cloud security
[15]	Cloud Security	Cloud Security	Discussion of	Literature	Understanding

	Issues and Challenges		cloud security issues and challenges	review	Cloud Security Challenges
[16]	Cloud Computing Security Issues and Challenges	Cloud Security	Discussion of cloud security issues and challenges	Literature review	Understanding cloud security issues
[17]	Security in Cloud Computing	Cloud Security	Discussion of security opportunities and challenges in cloud computing	Literature review	Understanding cloud security opportunities and challenges
[18]	Cloud Computing Security Analysis	Cloud Security	Analysis of Cloud Computing Security	Literature review	Analyzing Cloud Security Problems

3. RESEARCH METHODOLOGY

With RSA for key exchange and NTRU for data encryption, the suggested hybrid cryptographic architecture provides a strong means of guaranteeing data security and secrecy in cloud computing settings. To build a robust and secure framework, our approach places a major emphasis on secure cryptographic operations and efficient cloud key management. This technique addresses the security issues in cloud computing by developing a safe hybrid cryptographic paradigm that makes use of RSA for key exchange and NTRU for data encryption. It guarantees the privacy of data for the duration of its life in the cloud. Key rotation, efficient key management, and access control systems are crucial elements of this secure paradigm. Businesses can use cloud computing technology with confidence while protecting their data from potential security concerns by adhering to these measures. To properly use this hybrid approach in a cloud computing context, secure deployment of cryptographic operations and cloud key management are essential. It is beyond the capabilities of a text-based platform to create a comprehensive approach with graphics for the Hybrid RSA with the NTRU concept. The process's main steps are outlined below, along with an explanation:

1. Cloud-Based Key Management:

First Step: Generating Keys

Description: The creation of cryptographic keys is the initial stage. RSA keys are generated for key exchange, while NTRU keys are generated for data encryption. RSA keys are used to exchange encryption keys in a secure manner, and NTRU keys are used to encrypt the data itself.

Method: Generate RSA key pairs (public and private keys) using a safe key generation procedure. Create NTRU keys by creating public and private key pairs that are unique to NTRU encryption utilizing an appropriate algorithm. The goal of this step is to lay the groundwork for safe cloud data storage and transfer.

Step 2: Storage of Keys

After being generated, the cryptographic keys must be safely kept inside the cloud infrastructure to avoid unwanted access.

Procedure: To safely store the generated RSA and NTRU keys, use a key management system or hardware security module (HSM).

To protect the stored keys, put access limits and encryption in place.

The goal of secure key storage is to guarantee the integrity and secrecy of the keys.

2. Activity on the Sender End:

Step 3: NTRU Data Encryption

Description: Data is initially encrypted using NTRU encryption before being sent to the cloud. NTRU is selected due to its efficiency and quickness in data encryption.

Technique: To create encrypted data, apply NTRU encryption techniques to the input.

To encrypt the data, use the NTRU public key that was previously produced.

The goal of utilizing NTRU encryption is to guarantee the confidentiality of data while it is being transmitted to the cloud.

Step 4: RSA Key Exchange

Description: RSA is used to exchange encryption keys in order to provide a secure communication channel with the cloud. RSA is a good choice for safe key exchange.

Process: Using RSA, the sender starts a key exchange with the cloud.

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

The sender and the cloud exchange secure RSA keys, enabling the safe transfer of NTRU-encrypted data. The purpose of the RSA key exchange is to guarantee the communication channel's validity and integrity.

3. Data Transfer:

Step 5: Transferring Data Securely

Description: The sender safely sends the data to the cloud over a secured communication channel after encrypting it with RSA and NTRU keys.

Procedure: Send the NTRU-encrypted data via secure connection protocols (such as SSL/TLS). Make sure that data is transmitted securely and is shielded from eavesdropping. The goal of secure data transfer is to ensure the confidentiality of data while it is being transmitted to the cloud.

4. The Recipient's Actions:

Step 6: NTRU Data Decryption

Description: The recipient (cloud) utilises NTRU decryption to unlock the encrypted data once it has been sent to it encrypted with NTRU.

Method: To decrypt the incoming data, use the matching (already produced) NTRU private key. The goal of NTRU decryption is to return the data to its original state so that it may be processed.

5. Secure Key Administration Methods:

Step 7: Turning the keys

Description: Cryptographic keys are cycled frequently to limit the exposure of long-lived keys and improve security.

Process: Update key management systems and create fresh sets of RSA and NTRU keys.

After a predetermined period of time, swap out the old keys for the new ones.

The idea of key rotation is to lower the possibility of a key being compromised over time.

Step 8: Revocation of Keys

Revocation of keys is an essential procedure for handling compromised or superfluous keys.

Procedure: When a security breach occurs or when keys are no longer required, implement a key revocation mechanism to invalidate and replace keys.

The goal of key revocation is to preserve data security and the cryptographic system's integrity.

6. Controls on Recording and Access:

9. Management of Access

Make sure that only systems or users with permission can access decrypted data by putting access control mechanisms in place.

How-to: Configure the cloud infrastructure's access policies and restrictions. Provide only authorized entities with access to decrypted data. For the purpose of protecting the integrity and confidentiality of encrypted data, access control was implemented.

Auditing and Logging in Step Ten

For the purposes of security monitoring and accountability, keep logs and audit records of every access activity pertaining to the decrypted data.

Process: Record who accesses data and what is done by setting up auditing and logging systems. The goal is to enable security monitoring for possible threats or unauthorized access while also promoting transparency through auditing and logging.

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

This all-inclusive approach offers end-to-end data security in cloud computing environments by fusing RSA and NTRU cryptography. To guarantee data security, integrity, and accountability throughout its lifetime in the cloud, it places a strong emphasis on key management, encryption, and access control. The figure 3 shows the procedure of the proposed model .

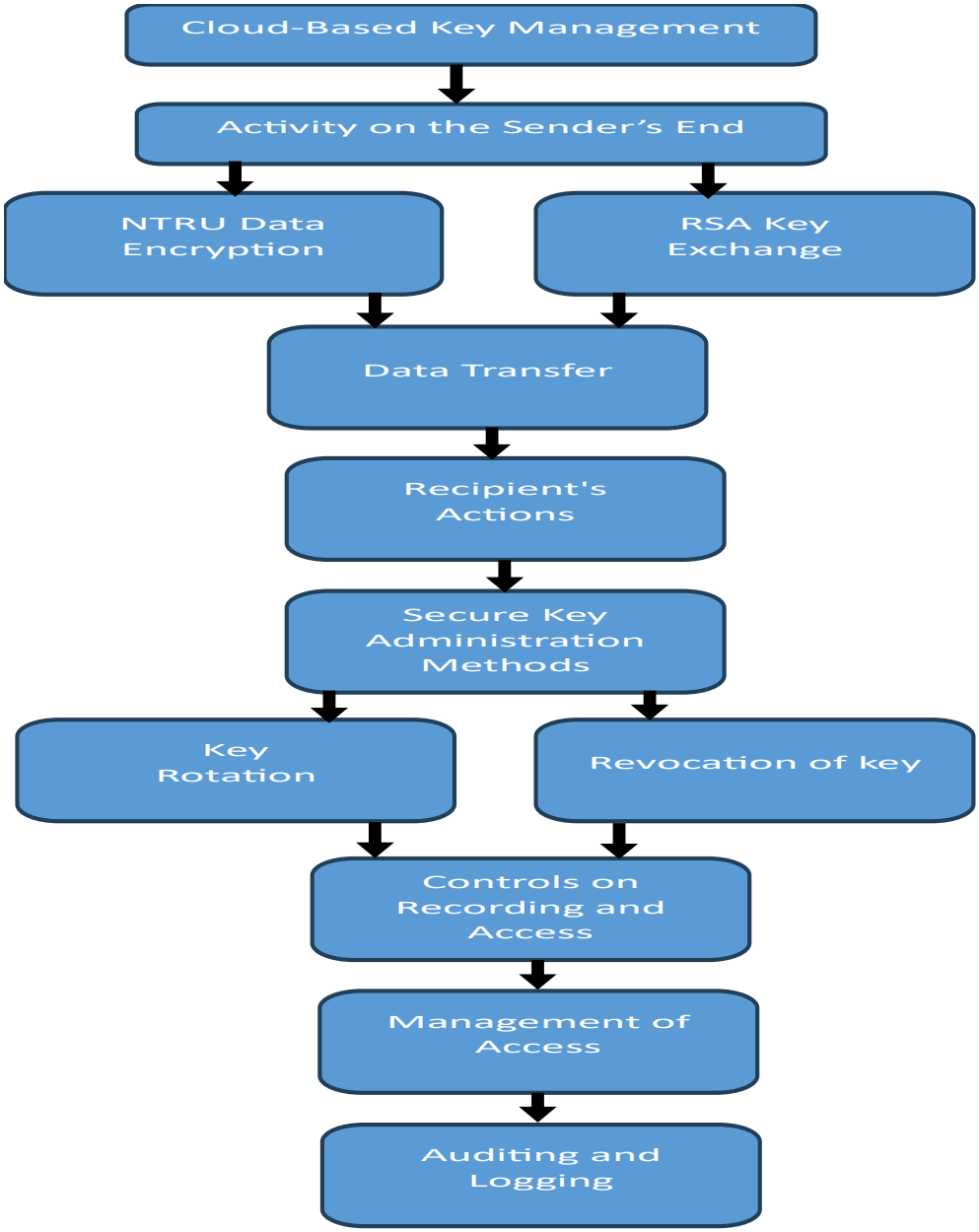

Figure 3 Procedure of the proposed model

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

4. ANALYSIS AND DISCUSSION

RSA and NTRU cryptography are used in a series of processes to provide end-to-end data security in cloud computing environments. Although software and algorithms are usually used to carry out these procedures, the authors provide a discussion and analysis along with some rudimentary mathematical representations to highlight the key cryptographic concepts.

Producing Keys:

RSA Key Pair Generation: Two huge prime numbers (p and q) are chosen in order to create an RSA key pair. It is created the public key (n, e), where e is a public exponent and n = p * q. Using modular arithmetic, the private key (d) is obtained from p, q, and e.

Example in Mathematics:

Choose p = 61 and q = 53 as your two prime numbers. Subtract n from p * q to get 61 * 53 = 3233. Choose e = 17, the public exponent.

The private exponent, d, must be determined so that (e * d) % ((p-1) * (q-1)) = 1.

Generation of NTRU Key Pairs: NTRU keys need the creation of polynomial coefficients. Polynomial procedures are used to generate the public key (f), and other methods are used to generate the private key (g). Select the proper coefficients for the polynomials f and g. The public and private keys are generated using these coefficients.

NTRU Data Encryption: Polynomial operations are used in NTRU encryption. Polynomial multiplication is used to compute the ciphertext (c), and the plaintext message (m) is represented as a polynomial.

Example in Mathematics: Use a polynomial to express the message: m(x) = a_0 + a_1 * x + a_2 * x^2 +...

Calculate the ciphertext by multiplying polynomials: Where r(x) is a random polynomial, c(x) = m(x) * r(x).

Key Exchange for RSA: For secure key exchange, RSA is employed. Simplified, it entails transferring public keys between the sender and the cloud in order to use them to determine a shared secret.

Mathematical Example: The public keys of the sender and the cloud are n_s, e_s and n_c, e_c, respectively.

Example in Mathematics: Select the proper coefficients for the polynomials f and g.

NTRU Decryption of Data: NTRU decryption retrieves the original message polynomial using the private key (g).

Example in Mathematics: Subtract c(x) from g(x) to find the original message polynomial.

Rotation and Revocation of Keys: Key rotation is the process of creating fresh key pairs on a regular basis. This can be mathematically accomplished by using the previously described key generation procedures. Key revocation is an administrative process that involves invalidating keys rather than having a direct mathematical component.

Control of Access and Auditing: Although it entails creating regulations and limits that dictate who can access data, access control is not strictly mathematical. Although they require recording access events for security monitoring and accountability, auditing and logging are likewise non-mathematical. The three main mathematical components of this procedure are key exchange (RSA), encryption (NTRU), and key creation (RSA and NTRU). Mathematical ideas such as modular arithmetic, polynomial operations (NTRU), and prime factorization (RSA) are essential to the security. Ensuring the confidentiality and integrity of data in the cloud requires adherence to fundamental mathematical concepts. These procedures have been applied to encrypted data on systems that feature an i7 core processor, an 8 TB hard drive, and 32 GB of RAM. The encryption time can be defined as the amount of time it takes to encrypt the data files using the hybrid RSA and NTRU technique, and the decryption time can be defined as the amount of time it takes to turn the cypher text back into plaintext. Figure 4 displays data from a research that examined the proposed cryptosystem, RSA [9], hybrid model [10], and NTRU across various file sizes. The suggested approach demonstrated consistently effective time consumption from 100 MB to 1000 MB with a step size increase when compared to the RSA. Fig. 5 shows the outcomes of a comparison of the NTRU and the rsa, the Proposed Model, and The Hybrid Model cryptosystems for different file sizes. With the step size growing with each repeat, the recommended method required less time than the other mentioned models for data sizes ranging from 100 MB to 1000 MB. As a result, the suggested method (the proposed algorithm) completes the encoding stage more quickly than the conventional RSA and NTRU. The decoding process is seen in operation in Fig. 5. we've been getting by with encoded files of various sizes. The suggested technique outperforms the previously discussed algorithm in terms of decoding speed. It looks like the Proposed Model is a novel or customized cryptography technique. The data shows that for all cryptographic techniques, the processing time increased with the size of the data (measured in megabytes). When evaluating the effectiveness and

performance of various cryptographic techniques at various data sizes, the values in these columns can be helpful. The approach processes the data more quickly the shorter the duration. It's critical to examine these timings in order to ascertain which cryptographic technique best fits the demands of particular data sizes and performance levels.

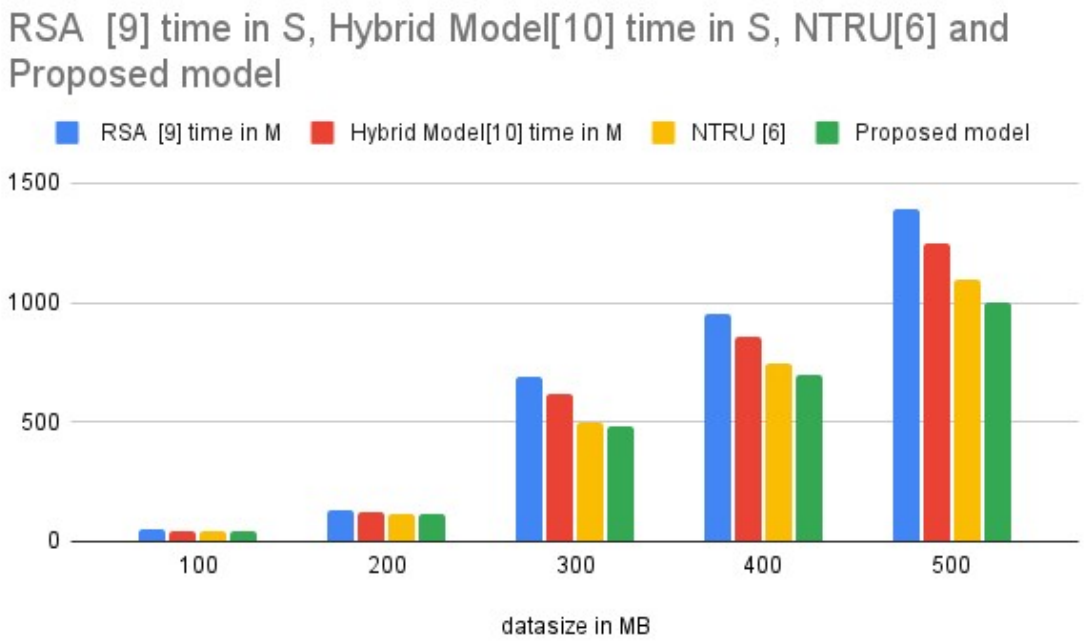

Figure 4. RSA, hybrid model, NTRU, and proposed model encryption times.

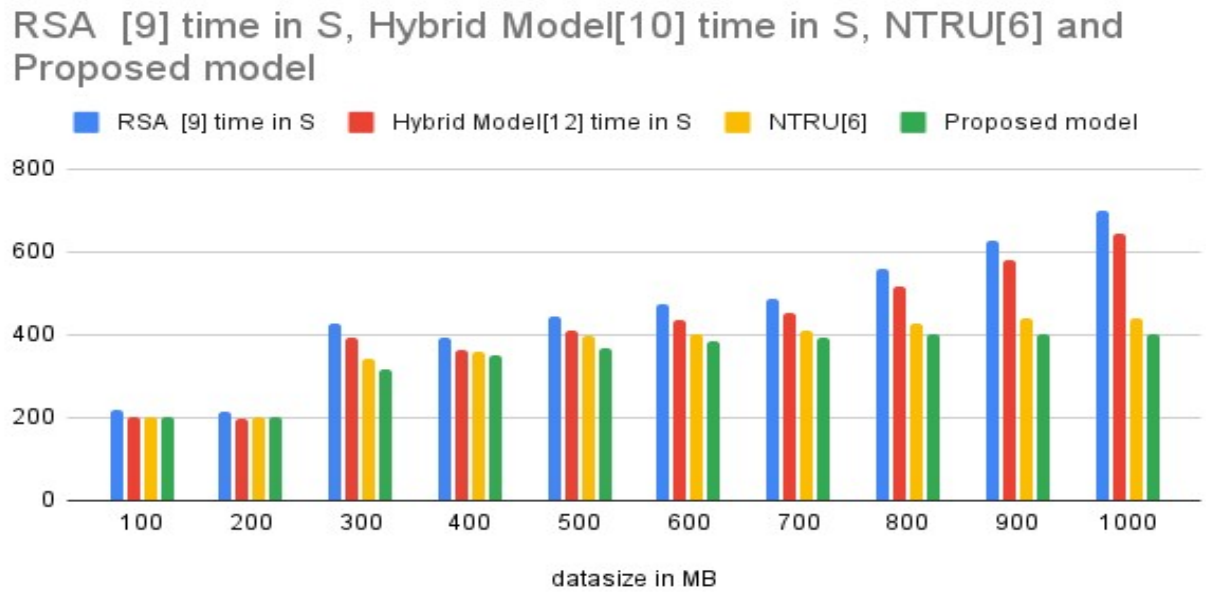

Figure 5. RSA, hybrid MODEL, NTRU, AND PROPOSED model decryption times.

5. CONCLUSION

A reliable and efficient way to guarantee data security and confidentiality in cloud computing environments is provided by the suggested hybrid cryptographic architecture, which combines RSA for key exchange and NTRU for data encryption. This technique tackles important cloud security issues by giving priority to secure cryptographic operations and effective cloud key management. With regard to key generation, storage, exchange, transport, and decryption, it offers a secure paradigm that ensures data privacy throughout its lifecycle. To keep the security posture intact, it is essential to implement access control, key rotation, and key management systems. Companies can safely use cloud-computing technologies while protecting their data from possible security risks. While protecting their data from potential security concerns, businesses can confidently use cloud-computing technology. To success applying this hybrid strategy in a cloud-computing context, secure deployment of cryptographic operations and cloud key management are essential. Secure data storage and confidentiality are largely dependent on mathematical foundations like prime factorization, polynomial operations, and modular arithmetic. The performance research shows that, for a range of file sizes, the suggested solution regularly beats out-of-the-box techniques like RSA and NTRU in terms of data encryption and decrypt time. This shows that the suggested hybrid paradigm, which can easily adjust to different data volumes and performance needs, is a viable and effective way to safeguard data in cloud computing settings.

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.6120).

REFERENCES:

[1] Jayapandian, N., Rahman, A. M. Z., Radhikadevi, S., & Koushikaa, M. (2016, February). Enhanced Cloud Security Framework To Confirm Data Security On Asymmetric And Symmetric Key Encryption. In *2016 World Conference On Futuristic Trends In Research And Innovation For Social Welfare (Startup Conclave)* (Pp. 1-4). Ieee.

[2] Thirumalai, C., Mohan, S., & Srivastava, G. (2020). An Efficient Public Key Secure Scheme For Cloud And Iot Security. *Computer Communications*, *150*, 634-643.

[3] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An Industrial Iot-Based Blockchain-Enabled Secure Searchable Encryption Approach For Healthcare Systems Using Neural Network. Sensors, 22(2), 572.

[4] Almaiah, M. A., & Al-Khasawneh, A. (2020). Investigating The Main Determinants Of Mobile Cloud Computing Adoption In University Campus. Education And Information Technologies, 25(4), 3087-3107.

[5] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber Security Threats In Cloud: Literature Review. In 2021 International Conference On Information Technology (Icit) (Pp. 779-786). Ieee.

[6] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A Novel Hybrid Trustworthy Decentralized Authentication And Data Preservation Model For Digital Healthcare Iot Based Cps. Sensors, 22(4), 1448.

[7] Adil, M., Khan, R., Ali, J., Roh, B. H., Ta, Q. T. H., & Almaiah, M. A. (2020). An Energy Proficient Load Balancing Routing Scheme For Wireless Sensor Networks To Maximize Their Lifespan In An Operational Environment. Ieee Access, 8, 163209-163224.

[8] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An Anonymous Channel Categorization Scheme Of Edge Nodes To Detect Jamming Attacks In Wireless Sensor Networks. Sensors, 20(8), 2311.

[9] Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A Conceptual Model For Investigating The Effect Of Privacy Concerns On E-Commerce Adoption: A Study On United Arab Emirates Consumers. Electronics, 11(22), 3648.

[10] Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Abou Elazm, A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure Health Monitoring Communication Systems Based On Iot And Cloud Computing For Medical Emergency Applications. Computational Intelligence And Neuroscience, 2021.

[11] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A Lightweight Hybrid Deep Learning Privacy Preserving

Model For Fc-Based Industrial Internet Of Medical Things. Sensors, 22(6), 2112.

[12] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving Energy Efficiency With Content-Based Adaptive And Dynamic Scheduling In Wireless Sensor Networks. Ieee Access, 8, 176495-176520.

[13] Alabadleh, A., Aljaafreh, S., Aljaafreh, A., & Alawasa, K. (2018). A Rss-Based Localization Method Using Hmm-Based Error Correction. Journal Of Location Based Services, 12(3–4), 273–285.

[14] Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification Of Cyber Security Threats On Mobile Devices And Applications. In Artificial Intelligence And Blockchain For Future Cybersecurity Applications (Pp. 107-123). Cham: Springer International Publishing.

[15] Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). Mac-Aodv Based Mutual Authentication Scheme For Constraint Oriented Networks. Ieee Access, 8, 44459-44469.

[16] Almomani, O., Almaiah, M. A., Alsaaidah, A., Smadi, S., Mohammad, A. H., & Althunibat, A. (2021, July). Machine Learning Classifiers For Network Intrusion Detection System: Comparative Study. In 2021 International Conference On Information Technology (Icit) (Pp. 440-445). Ieee.

[17] Adil, M., Khan, R., Almaiah, M. A., Binsawad, M., Ali, J., Al Saaidah, A., & Ta, Q. T. H. (2020). An Efficient Load Balancing Scheme Of Energy Gauge Nodes To Maximize The Lifespan Of Constraint Oriented Networks. Ieee Access, 8, 148510-148527.

[18] Alsyouf, A., Lutfi, A., Al-Bsheish, M., Jarrar, M. T., Al-Mugheed, K., Almaiah, M. A., ... & Ashour, A. (2022). Exposure Detection Applications Acceptance: The Case Of Covid-19. International Journal Of Environmental Research And Public Health, 19(12), 7307.

[19] Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity Concerns In Smart-Phones And Applications: A Survey. In 2021 International Conference On Information Technology (Icit) (Pp. 725-731). Ieee.

[20] Almaiah, M. A. (2021). A New Scheme For Detecting Malicious Attacks In Wireless Sensor Networks Based On Blockchain Technology. In Artificial Intelligence And Blockchain For Future Cybersecurity Applications (Pp. 217-234). Cham: Springer International Publishing.

[21] Alese, B. K., Philemon E. D., Falaki, S. O., Comparative Analysis Of Public-Key Encryption Schemes, International Journal Of Engineering And Technology Volume2 No. 9, 2012.

[22] Rajadurga, K., And S. Ram Kumar. "Gf (2m) Based Low Complexity Multiplier For Elliptic Curve Cryptography Systems." *Networking And Communication Engineering* 6, No. 4 (2014): 150-155.

[23] Alamer, M., & Almaiah, M. A. (2021, July). Cybersecurity In Smart City: A Systematic Mapping Study. In 2021 International Conference On Information Technology (Icit) (Pp. 719-724). Ieee.

[24] Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, A. K. A., ... & Aldhyani, T. H. (2022). Performance Investigation Of Principal Component Analysis For Intrusion Detection System Using Different Support Vector Machine Kernels. Electronics, 11(21), 3571.

[25] Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S. (2020). A New Hybrid Text Encryption Approach Over Mobile Ad Hoc Network. Int. J. Electr. Comput. Eng.(Ijece), 10(6), 6461-6471.

[26] Alrawad, M., Lutfi, A., Alyatama, S., Elshaer, I. A., & Almaiah, M. A. (2022). Perception Of Occupational And Environmental Risks And Hazards Among Mineworkers: A Psychometric Paradigm Approach. International Journal Of Environmental Research And Public Health, 19(6), 3371.

[27] Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., ... & Aldhyani, T. H. (2022). Investigating The Effect Of Perceived Security, Perceived Trust, And Information Quality On Mobile Payment Usage Through Near-Field Communication (Nfc) In Saudi Arabia. Electronics, 11(23), 3926.

[28] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity Threats, Countermeasures And Mitigation Techniques On The Iot: Future Research Directions. Electronics, 11(20), 3330.

[29] Albalawi, A. M., & Almaiah, M. A. (2022). Assessing And Reviewing Of Cyber-Security Threats, Attacks, Mitigation Techniques In Iot

Environment. J. Theor. Appl. Inf. Technol, 100, 2988-3011.

[30] Qasem, M. H., Obeid, N., Hudaib, A., Almaiah, M. A., Al-Zahrani, A., & Al-Khasawneh, A. (2021). Multi-Agent System Combined With Distributed Data Mining For Mutual Collaboration Classification. Ieee Access, 9, 70531-70547.

[31] Almudaires, F., & Almaiah, M. (2021, July). Data An Overview Of Cybersecurity Threats On Credit Card Companies And Credit Card Risk Mitigation. In 2021 International Conference On Information Technology (Icit) (Pp. 732-738). Ieee.

[32] Almedires, M., & Almaiah, M. (2021, July). Cybersecurity In Industrial Control System (Ics). In 2021 International Conference On Information Technology (Icit) (Pp. 640-647). Ieee.

[33] Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., ... & Alghanam, O. A. (2023). Investigating The Role Of Perceived Risk, Perceived Security And Perceived Trust On Smart M-Banking Application Using Sem. Sustainability, 15(13), 9908.

[34] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A New Blockchain-Based Authentication Framework For Secure Iot Networks. Electronics, 12(17), 3618.

[35] Kumar, Y. K., & Shafi, R. M. (2020). An Efficient And Secure Data Storage In Cloud Computing Using Modified Rsa Public Key Cryptosystem. *International Journal Of Electrical And Computer Engineering*, *10*(1), 530.

[36] Chen, R., Mu, Y., Yang, G., Guo, F., & Wang, X. (2015). Dual-Server Public-Key Encryption With Keyword Search For Secure Cloud Storage. *Ieee Transactions On Information Forensics And Security*, *11*(4), 789-798.

[37] 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.

[38] Yousif, M. K., Dallalbashi, Z. E., & Kareem, S. W. (2023). Information Security For Big Data Using The Ntruencrypt Method. *Measurement: Sensors*, *27*, 100738.

[39] 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.

[40] Yousif, R. Z., Kareem, S. W., & Abdalwahid, S. M. (2020). Enhancing Approach For Information Security In Hadoop. *Polytechnic Journal*, *10*(1), 81-87.

[41] Mohamed, M. A., Shawai, Y. G., Almaiah, M. A., Derahman, M. N., Lutfi, A., & Bakar, K. A. A. (2024). Challenges In Data Representation For Efficient Execution Of Encryption Operation. Bulletin Of Electrical Engineering And Informatics, 13(2), 1207-1216.

[42] Scientific, L. L. (2024). Enhancing Cloud Security Based On The Kyber Key Encapsulation Mechanism. Journal Of Theoretical And Applied Information Technology, 102(4).

[43] Alkhdour, T., Almaiah, M. A., Ali, A., Lutfi, A., Alrawad, M., & Tin, T. T. (2024). Revolutionizing Healthcare: Unleashing Blockchain Brilliance Through Fuzzy Logic Authentication. *Journal Of Theoretical And Applied Information Technology*, *102*(4).

[44] Almaiah, M. A., Ali, A., Shishakly, R., Alkhdour, T., Lutfi, A., & Alrawad, M. (2024). A Novel Federated-Learning Based Adversarial Framework For Audio-Visual Speech Enhancement. *Journal Of Theoretical And Applied Information Technology*, *102*(4).

[45] Almaiah, M. A., Ali, A., Shishakly, R., Alkhdour, T., Lutfi, A., & Alrawad, M. (2024). Building Trust In Iot: Leveraging Consortium Blockchain For Secure Communications. *Journal Of Theoretical And Applied Information Technology*, *102*(3).

[46] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly Detection Ids For Detecting Dos Attacks In Iot Networks Based On Machine Learning Algorithms. *Sensors*, *24*(2), 713.

[47] Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaayah, M. A. (2024). Cybersecurity Awareness Among Secondary School Students Post Covid-19 Pandemic. *Journal Of Advanced Research In Applied Sciences And Engineering Technology*, *37*(1), 115-127.