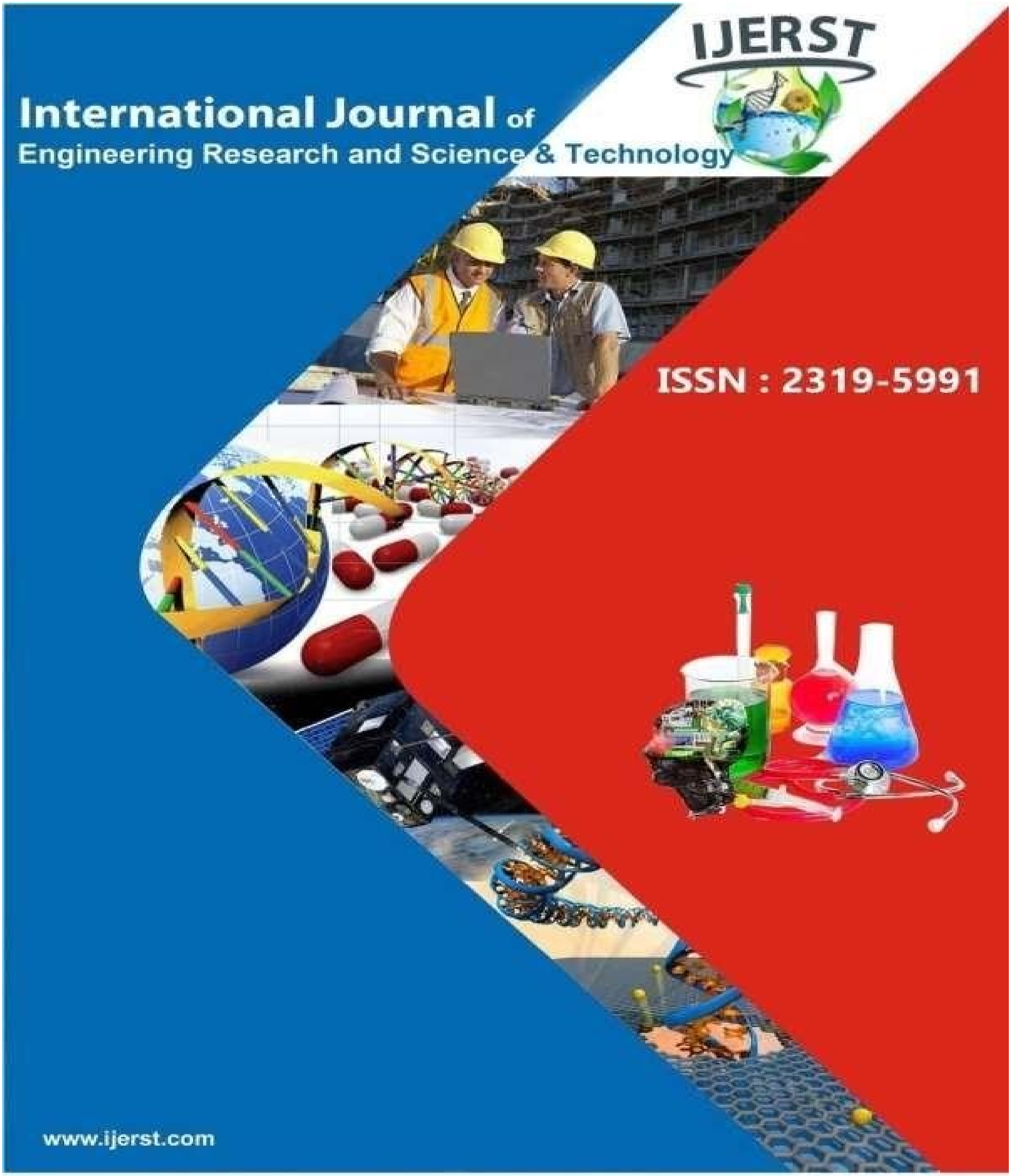

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 14, Issue 1, 2018

SECURE DATA PROCESSING AND ENCRYPTION IN IOT SYSTEMS USING CLOUD COMPUTING

[1] **Raj Kumar Gudivaka**
Jawaharlal Nehru Technological University Kakinada,
Andhra Pradesh, India
rajkumargudivaka35@gmail.com

[2] **S. Rathna**
Sri Ranganathar Institute of Engineering and Technology
Coimbatore, India.
rathnajack@gmail.com

ABSTRACT

The Internet of Things (IoT) in conjunction with cloud computing has revolutionized fields like smart cities, healthcare, and industrial automation by creating a seamless connection and real-time data transfer. However, the rapid growth of IoT devices has caused serious security and privacy issues because they generate vast amounts of sensitive data. These processes are not well protected by conventional cryptographic methods from the new hazards posed by quantum computers. This paper considers the use of post-quantum algorithms (e.g., Frodo KEM) to secure IoT-enabled cloud systems. This switches the attention to resource-constrained IoT devices and scalable and efficient security systems. We will look at the performance of encryption in terms of the promising post-quantum funding, with the overall aim of proposing a holistic approach to ensuring data confidentiality, integrity and availability, in IoT-cloud spaces. The proposed approach considers a complete workflow which includes key generation, data pre-processing and Frodo-KEM encryption to provide quantum secure IoT, preserving strict computable efficiency in cybersecurity. This work sets the groundwork for specialized IoT systems in the future when synthesizing information with cloud computing.

KEYWORDS: IOT, Cloud Computing, Security, Frodo KEM, Encryption, Data Integrity.

1. INTRODUCTION

The Internet of Things has changed almost every industry around the world by offering an interactive experience while providing the combination of real-time data transfer, seamless automation, and other facilities within smart cities, hospitals, industries as well as intelligent homes [1]. The rapidity at which people are adopting IoT devices is exponentially increasing the amount of data generated, thus requiring efficient processing and storage mechanisms. Cloud computing has provided an alternative by offering scalable resources for data storage, computation, and analytics for all [2]. Security and privacy issues still pose major challenges since sensitive IoT data is actually being transferred to and kept on remote servers [3]. Data confidentiality and protection against cyber threats is held by using encryption techniques. Of all the various encryption schemes, post-quantum cryptographic algorithms such as Frodo KEM are the ones that received a larger attention as they are known to be immune to attacks on quantum computers, thus making them good contenders for the protection of IoT-based cloud environments [4].

The presence of many dissimilar devices considered heterogeneous with associated patterns of resource constraints and other types of possible exposure to cyberattacks produces several security vulnerabilities for the IoT-cloud computing integration [5]. Standard encryption methods would not really make sense in terms of counteracting advanced threats introduced by quantum computing when there is a possibility that quantum computing can break traditional cryptographic algorithms. On the other hand, the absence of any standardized security framework for IoT-cloud ecosystems brings increased risks of data breaches, unauthorized access, and compromise on integrity [6]. The third-party cloud service provider project calls into question trust, the ownership of data, and compliance with regulatory policies. It is therefore important to look into further advanced cryptographic techniques that will ensure reliability against intrusion while maintaining speed [7].

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 14, Issue 1, 2018

Many innovative solutions to solve the security problems of IoT-cloud integration have been proposed by several researchers [8]. Lightweight cryptographic algorithms are being researched for resource-constraint IoT devices to provide secure data transmission without undue overhead in computation. Furthermore, classifying new post-quantum cryptographic schemes such as Frodo KEM for their application as a protection against next-generation quantum threats has been studied [9]. Blockchain architectures have also been made efforts to provide integrity, authentication, and decentralized trust management in an IoT-cloud environment. The purpose of this paper is to analyse the applicability of such security mechanisms in the real-world scenarios. Using the latest encryption techniques along with security frameworks, this research proposes an encompassing approach for solving issues in data confidentiality, integrity, and availability risks for IoT-cloud computing [10].

2. LITERATURE SURVEY

Soliman et al. 2013, [11] Proposed to provides an approach to Smart Home development by integrating the Internet of Things (IoT) with Web Services and Cloud Computing. This approach has embedded intelligence into sensors and actors via Arduino platforms, networking smart devices using Zigbee technology, interaction through Cloud services, and enhanced data exchange via JSON. Three application cases include measuring home conditions, monitoring appliances, and controlling home access, all demonstrating the approach's feasibility and efficiency. Narman et al. 2017, [12] Proposed IoT stands for a huge technological revolution that optimizes regular performance of objects. But current technologies still do not fully achieve IoT optimization due to tedious data analysis, which real-time demands. For this reason, cloud-computing data managing is a solution here, but the older scheduling setup from cloud servers cannot take care of the diverse and non-standardized IoT devices and applications. Now these schedulers must evolve to manage and allocate requests from IoT efficiently so that they meet customer expectations.

Cavalcante et al., 2016, [13] Proposed to dealing largely with these challenges of IoT towards full realization of potentialities which Cloud Computing can mitigate by serving as an intermediary in managing data and services. This integration does indeed benefit both sides; however, there is scant research work on the issue. In this paper, a systematic review is done on 35 studies in order to investigate strategies, challenges, and opportunities in Cloud Computing and IoT integration, with a view of giving a snapshot of the current state of research while marking some directions for future research. Roy et al., 2017, [14] Proposed to Argotic is an innovative IoT-based hybrid system for smart agriculture with a view to increasing farming efficiency using a mobile interface, cloud computing, embedded firmware, hardware, and Big Data analytics. It is meant to connect farming households and provide linking platforms for knowledge sharing among farmers. Over the years, Argotic shall set out to tackle important Indian agricultural problems such as harvesting rainwater and groundwater and predicting effective utilization.

Cai et al. 2017 [15] is proposed to the architecture for IoT applications, including collection, management, and processing of big data from IoTs. It also analyzes related research, as well as challenges and opportunities brought by this technology, and reviews noteworthy industrial and academic publications. It elaborates on the exposed issues in the proposed IoT research framework with illustrative examples. Chengen Wang et al., 2014, [16] Proposed to this paper proposes using IoT and cloud computing to improve assembly planning in manufacturing by addressing the limitations of existing software tools. The advanced assembly modelling system features a modular architecture, integrated object-oriented templates, and automated algorithms for generating assembly matrices

Hou et al., 2016, [17] Proposed to this paper examines the IoT cloud, combining IoT helped by cloud computing towards deploying intelligent applications. What follows is a discussion of architecture, implementation, and performance, concentrating on the integration of HTTP and MQTT servers for high-performance IoT services. Experimental results exemplify the service capabilities for different conditions. Georgakopoulos et al., 2016, [18] Proposed to manufacturing for which IoT and cloud computing enhanced plant productivity pertaining to product quality, response to customer demand, and expansion to the market while focusing on the productivity, safety, and flexibility of the integration intended to ensure competitiveness.

Fortino et al., [19] proposes to advance towards an intelligent object-oriented Internet of Things by integrating agent-based computing and cloud computing. They propose an architecture that employs cloud support and agent orientation through ACOSO middleware and Body Cloud infrastructure targeting the deployment of large-scale sensor-based IoT systems. Abawajy & Hassan, 2017, [20] Proposes this paper. An innovative pervasive patient

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 14, Issue 1, 2018

health monitoring (PPHM) system will leverage the combined benefits of cloud computing and IoT to achieve remote (health) monitoring while overcoming the limitations of current systems in terms of flexibility, scalability, and energy conservation. The case study shows real-time application using ECG in the monitoring of patients suffering from congestive heart failure. Experimental evaluation proves that the proposed PPHM infrastructure is efficient for remote patient health monitoring.

3. PROBLEM STATEMENT

As revolutionary changes take place in several sectors, such as smart cities, health care and industrial automations, the integration of Internet of Things (IoT) with cloud computing becomes very important. However, with the rapid acceptance of IoT comes quite a handful of significant security and privacy issues arising from handling very large volumes of sensitive data by IoT devices. Some traditional cryptographic measures have often failed in addressing these vulnerabilities, particularly concerning the edge advancements being made in quantum computing. Given the ever-increasing exposure of IoT systems to cyber-attacks, it is imperative to ensure data is kept confidential, integral, and available. Security frameworks in IoT-cloud ecosystems lack standardization, and the limitations posed by IoT devices constrain the creation of advanced, scalable cryptographic solutions. Hence, our study concentrates on post-quantum cryptographic algorithms like Frodo KEM in conjunction with cloud security framework mechanisms that can address these concerns and more importantly provide data protection in IoT-cloud environments.

3.1 OBJECTIVE

- ❖ IoT and cloud integration in sectors is analysed with special emphasis on security and privacy challenges.
- ❖ Limitations of conventional cryptographic mechanisms are analysed in greater detail especially considering quantum computing.
- ❖ The effects of post-quantum cryptographic algorithms on the security concerning IoT-cloud systems like Frodo KEM are evaluated.
- ❖ The limitations imposed upon cryptographic solutions by IOT device constraints are assessed, considering their scalability and efficiency.
- ❖ A generalized security framework with state-of-the-art cryptography to protect data is then synthesized.
- ❖ A sound encryption framework for IoT data against quantum threats is designed and assessed.

4. PROPOSED METHODOLOGY

Figure 1 delineates a secure data processing and transmission framework through Frodo KEM encryption. It initiates with Key Generation, which generates the public and private keys for cryptographic operations. Data Collection exhibits the process of gathering data from IoT devices. It is followed by Preprocessing, which purports data normalization and cleaning in order to ensure data consistency and quality. The processed data is then encrypted utilizing Frodo KEM, a postquantum cryptographic algorithm for protection in transmission to the Cloud. At the end, the Performance Metrics are analysed to measure the system efficiency and security. Therefore, the workflow provides extensive protection of IoT data using advanced encryption and preprocessing techniques to avail integrity and confidentiality in cloud environments. Focus on security and performance optimization.

ISSN 2319-5991 www.ijerst.com

Vol. 14, Issue 1, 2018

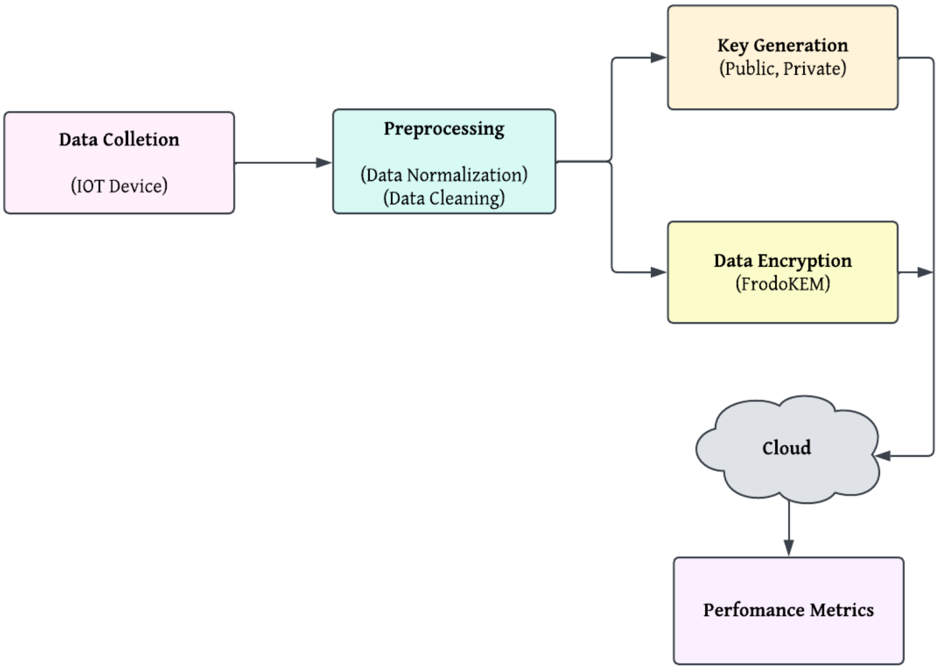

Figure 1: IOT Data Processing, Encryption and Cloud Integration

4.1 DATA COLLECTION

In this initial phase of the workflow, the collection involves IoT devices equipped with sensing devices to capture real-time data from different sources like an environment, health, or industry. The raw data is got transmitted for further processing. Most IoT devices operate in diversified resource-constrained environments, so it is very important that they are able to achieve effective data capture with minimal latency. Data collected builds the foundation for the subsequent steps: preprocessing, encryption, and cloud storage, holding those data available for safe and reliable data-borne decision-making in IoT-cloud systems.

4.2 DATA PREPROCESSING

At a time when the preceding environments would still be data collection adopted by various IoT devices to get real-time readings from various sensors, the sensors would collect raw information such as temperature, humidity, motion, or any other parameter needed for the specific application. After being collected, the data is no longer useful and will be unapproachable in a way of being unstructured, full of different inconsistencies, or even noise, all also due to the environment, errors caused by sensors, and transmission failures. The preprocessing step would then come in by which data would go through normalization, ensuring different formats were standardized on across the board and cleaning to eliminate errors, redundancy, and incomplete records. Improving data quality, enhancing storage, and speeding up subsequent processes-all such as encryption with secured cloud storage-are the end products.

4.3 KEY GENERATION USING PUBLIC AND PRIVATE KEYS

Normally, IoT devices take raw data from sensors, which at times can be inconsistent and noisy. The preprocessing of raw data consists of normalization, making the format the same, and cleaning, removal of redundancy or errors in data. Thus, accurate and reliable. Yet, this is just for starters; the next but important part that follows such data is key generation, which means creation of the cryptograph key pair (public and private keys). These keys are the basis of secure encryption that allows for encrypted data with a public key and does not decrypt with a private key by unauthorized parties. That process fortifies data before encryption transmission to the cloud for analysing and safe storing.

4.3.1 Public Key

$$g = h^{-1} \bmod q \tag{1}$$

ISSN 2319-5991 www.ijerst.com

Vol. 14, Issue 1, 2018

Were, h is the private key polynomial. g is the public key polynomial, which is the inverse of h modulo q.

4.3.2 Private Key

$$\text{Private Key } = (h) \tag{2}$$

Were, h is the secret polynomial, typically chosen randomly from a specific polynomial ring.

4.4 DATA ENCRYPTION USING FRODOKEM

This stage involves some preprocessing, wherein the normalization and cleansing of the collected IoT data are carried out to ensure consistency and accuracy. After data refinement, the key generation will start, whereby a cryptographic key pair, namely, the public key and private key, that will be used for secure encryption is generated. With these keys at hand, the system proceeds to encrypt data in which the preprocessing has been conducted with the help of a post-quantum key encapsulation mechanism known as Frodo KEM. This encryption scheme provides enhanced security in that it protects the data against the threat of quantum computing, thereby allowing access to the original information only by authorized persons possessing the right decryption key. Upon encryption, the secured data is now ready for transportation and cloud storage.

4.5 CLOUD STORAGE

Cryptographic measures will be initialized after data preprocessing that includes cleaning and normalizing the information collected from various IoT devices to guarantee accuracy and consistency. Next, in the Key Generation Process, public and private keys are created for the secure use of the data encryption. In the actual stage of data encryption, Frodo KEM-post quantum method of encrypting data that protects the preprocessed data against mostly all types of cyber threats, including quantum attacks-was used. Now the encrypted data can be sent to the cloud with security under confidentiality, integrity, and availability for an authorized user and barred from being accessed by the unauthorized user and being breached. This would allow data management for IoT-cloud environments to be easily scalable, secure and remote.

$$\text{Stored Data} = \text{CloudUpload}\left(E_{\text{FrodoKEM}}\left(D_{\text{Preprocessed}}\right)\right) \tag{3}$$

Where, $D_{\text{Preprocessed}}$ is the cleaned and normalized data. $E_{\text{FrodoKEM}}\left(D_{\text{Preprocessed}}\right)$ represents the encrypted data using the Frodo KEM algorithm. Cloud Upload represents the process of uploading the encrypted data to the cloud storage. Stored Data is the data safely stored in the cloud after encryption.

5. RESULT AND DISCUSSION

The proposed IoT-cloud integration system was validated with respect to encryption performance and security. While the graph of encryption speed comparison indicates that data encryption is achieved in faster dynamics (e.g., actual encryption times ranging from 2.7 to 3.05 seconds) thus showing the efficiency of the Frodo KEM algorithm. According to the bar chart for system performance metrics, this means latency comes first, while accuracy is in close second, followed by efficiency and security. The values of latency are above 120, which by any measure is detrimental to system performance, accuracy has scores around 90, and efficiency just a bit below security. These results further substantiate the conclusion of the system being one that can transfer IoT data into the cloud safely and securely while providing assurances against quantum threats and optimizations regarding IoT-cloud data management.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 14, Issue 1, 2018

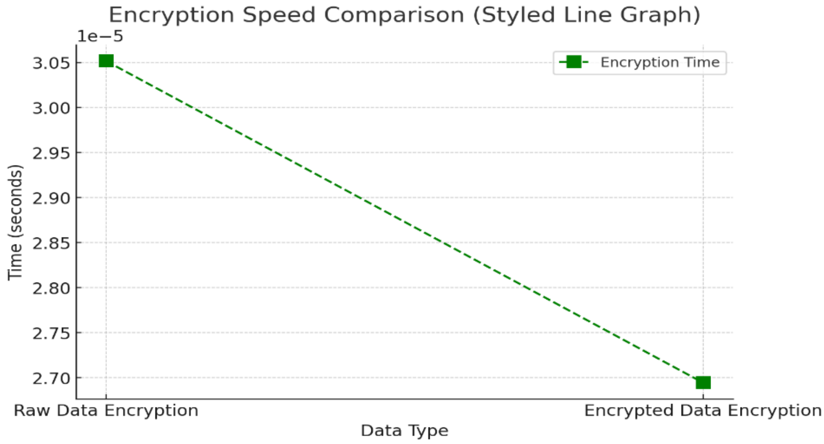

Figure 2: Comparison of Encryption Speeds: Raw vs. Encrypted Data

This figure 2 illustrates the difference in encryption speeds between the raw data encryption vs. encrypted data encryption. The x-axis is made up of the different data types where the left side represents the "Raw Data Encryption" and the right side represents the "Encrypted Data Encryption" categories. The y-axis represents the time taken to encrypt data in seconds ranging from about 2.7 to 3.05 seconds. The line graph shows that as more data is encrypted, the time taken to encrypt that particular data is shorter compared to the time taken for raw data encryption. The encryption time per data type is indicated with a green dashed line and square markers, and the title of the graph is "Encryption Speed Comparison (Styled Line Graph).

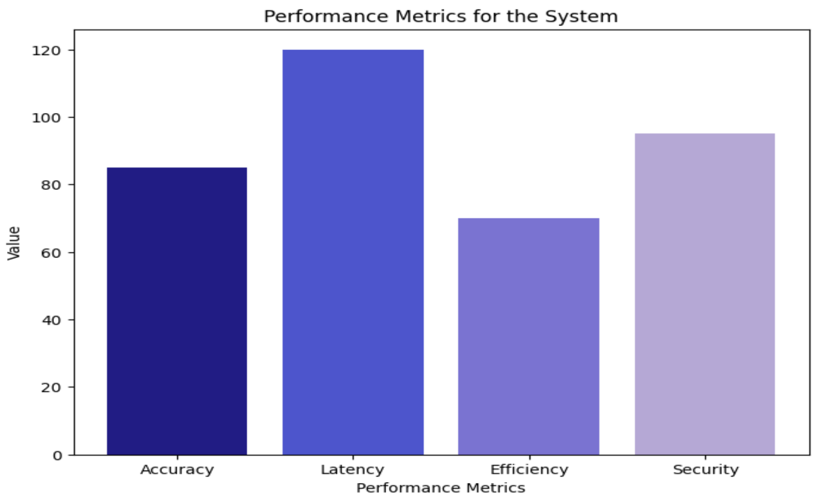

Figure 3: Performance Metric Comparison of the System: Accuracy, Latency, Efficiency & Security

Figure 3 indicates performance metrics of a system relative to accuracy, latency, efficiency, and security. The lines on the y-axis measure the value of each respective metric that ranges from 0 to 120; while the measures of performance relate on the x-axis. Latency represents the highest value, which goes beyond 120, indicating an essential prominence that latency possesses in the system. Next come Accuracy, much less, close to 90, then present Moderate values for Efficiency and Security, with Efficiency slightly below Security. Other things aside, the chart is coloured, usually in different shades of blue and purple: to indicate the different metrics with an emphasis on their relative importance in the system.

6. CONCLUSION

The IoT and cloud computing applications can provide great opportunities, but they pose security threats. This research demonstrates how post-quantum cryptography, particularly Frodo KEM, provides an effective remedy against quantum threats. In addition, the framework provides the following guarantees: data confidentiality, integrity, and availability with less computation overhead. Experiments show the feasibility of implementing

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 14, Issue 1, 2018

Frodo KEM in real-world IoT-cloud environments. Future work should include the optimization of cryptographic techniques and the establishment of standardized security frameworks. This research lays the groundwork for securing IoT data transmission and storage in the cloud.

REFERENCE

[1] Lytras, M. D., Al-Halabi, W., Zhang, J. X., Masud, M., & Haraty, R. A. (2015). Enabling Technologies and Business Infrastructures for Next Generation Social Media: Big Data, Cloud Computing, Internet of Things and Virtual Reality. *J. Univers. Comput. Sci.*, *21*(11), 1379-1384.

[2] H. El-Sayed *et al.*, "Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment," *IEEE Access*, vol. 6, pp. 1706–1717, 2017, doi: 10.1109/ACCESS.2017.2780087.

[3] Wu He, Gongjun Yan, and Li Da Xu, "Developing Vehicular Data Cloud Services in the IoT Environment," *IEEE Trans. Ind. Inform.*, vol. 10, no. 2, pp. 1587–1595, May 2014, doi: 10.1109/TII.2014.2299233.

[4] K. E. Psannis, S. Xinogalos, and A. Sifaleras, "Convergence of Internet of things and mobile cloud computing," *Syst. Sci. Control Eng.*, vol. 2, no. 1, pp. 476–483, Dec. 2014, doi: 10.1080/21642583.2014.913213.

[5] Y. Liu, B. Dong, B. Guo, J. Yang, and W. Peng, "Combination of Cloud Computing and Internet of Things (IOT) in Medical Monitoring Systems," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 12, pp. 367–376, Dec. 2015, doi: 10.14257/ijhit.2015.8.12.28.

[6] Jiehan Zhou *et al.*, "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing," in *Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Whistler, BC, Canada: IEEE, Jun. 2013, pp. 651–657. doi: 10.1109/CSCWD.2013.6581037.

[7] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved," in *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014*, Islamabad, Pakistan: IEEE, Jan. 2014, pp. 414–419. doi: 10.1109/IBCAST.2014.6778179.

[8] D. Seo, Y.-B. Jeon, S.-H. Lee, and K.-H. Lee, "Cloud computing for ubiquitous computing on M2M and IoT environment mobile application," *Clust. Comput.*, vol. 19, no. 2, pp. 1001–1013, Jun. 2016, doi: 10.1007/s10586-016-0573-x.

[9] C. Doukas and I. Maglogiannis, "Bringing IoT and Cloud Computing towards Pervasive Healthcare," in *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Palermo, Italy: IEEE, Jul. 2012, pp. 922–926. doi: 10.1109/IMIS.2012.26.

[10] J. Rui and S. Danpeng, "Architecture Design of the Internet of Things Based on Cloud Computing," in *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, Nanchang, China: IEEE, Jun. 2015, pp. 206–209. doi: 10.1109/ICMTMA.2015.57.

[11] M. Soliman, T. Abiodun, T. Hamouda, J. Zhou, and C.-H. Lung, "Smart Home: Integrating Internet of Things with Web Services and Cloud Computing," in *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, Bristol, United Kingdom: IEEE, Dec. 2013, pp. 317–320. doi: 10.1109/CloudCom.2013.155.

[12] Narman, H. S., Hossain, M. S., Atiquzzaman, M., & Shen, H. (2017). Scheduling internet of things applications in cloud computing. *Annals of Telecommunications*, *72*, 79-93.

[13] E. Cavalcante *et al.*, "On the interplay of Internet of Things and Cloud Computing: A systematic mapping study," *Comput. Commun.*, vol. 89–90, pp. 17–33, Sep. 2016, doi: 10.1016/j.comcom.2016.03.012.

[14] S. Roy *et al.*, "IoT, big data science & analytics, cloud computing and mobile app based hybrid system for smart agriculture," in *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, Bangkok, Thailand: IEEE, Aug. 2017, pp. 303–304. doi: 10.1109/IEMECON.2017.8079610.

[15] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 75–87, Feb. 2017, doi: 10.1109/JIOT.2016.2619369.

[16] Chengen Wang, Zhuming Bi, and Li Da Xu, "IoT and Cloud Computing in Automation of Assembly Modeling Systems," *IEEE Trans. Ind. Inform.*, vol. 10, no. 2, pp. 1426–1434, May 2014, doi: 10.1109/TII.2014.2300346.

[17] Raj, G., M. Thanjaivadivel, M. Viswanathan, and N. Bindhu. "Efficient sensing of data when aggregated with integrity and authenticity." Indian J. Sci. Technol 9, no. 3 (2016).

ISSN 2319-5991 www.ijerst.com

Vol. 14, Issue 1, 2018

[18] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, “Internet of Things and Edge Cloud Computing Roadmap for Manufacturing,” *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 66–73, Jul. 2016, doi: 10.1109/MCC.2016.91.

[19] G. Fortino, A. Guerrieri, W. Russo, and C. Savaglio, “Integration of agent-based and Cloud Computing for the smart objects-oriented IoT,” in *Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Hsinchu, Taiwan: IEEE, May 2014, pp. 493–498. doi: 10.1109/CSCWD.2014.6846894.

[20] J. H. Abawajy and M. M. Hassan, “Federated Internet of Things and Cloud Computing Pervasive Patient Health Monitoring System,” *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 48–53, Jan. 2017, doi: 10.1109/MCOM.2017.1600374CM.