

Security comparison of NTRU-Encrypt and ECC in smart healthcare systems

Adil Bashir *

Department of Computer Science and Engineering

Islamic University of Science and Technology

Pulwama 192122

Jammu and Kashmir

India

Numrena Farooq [†]

Department of Computer Science and Engineering

National Institute of Technology Srinagar

Hazratbal

Srinagar 190006

Jammu and Kashmir

India

Alina Pervaiz [§]

Department of Computer Science and Engineering

Islamic University of Science and Technology

Pulwama 192122

Jammu and Kashmir

India

Ajaz Hussain Mir [‡]

Department of Electronics and Communication Engineering

National Institute of Technology Srinagar

Hazratbal

Srinagar 190006

Jammu and Kashmir

India

* E-mail: adilbashir.445@gmail.com (Corresponding Author)

[†] E-mail: mirnumrena@gmail.com

[§] E-mail: alina.pervaiz@gmail.com

[‡] E-mail: ahmir@rediffmail.com

Abstract

The Smart Healthcare System (SHS) represents a ground-breaking evolution in healthcare, integrating Internet of Things (IoT), Fog computing, and Cloud computing. This innovation deploys miniature IoT wearables for real-time patient health data collection, enabling remote monitoring, early anomaly detection, and personalized care. SHS strategically utilizes cloud computing for scalable data analytics and storage, while Fog computing enables swift data processing at intermediate nodes. The pivotal role of IoT is emphasized, with wearable devices serving as continuous data conduits for remote monitoring and data-driven healthcare. However, SHS faces security challenges, including unauthorized access, data manipulation, and cyber threats to the interconnected healthcare devices. Cryptography is essential to address these issues, however, due to inherent resource limitations of smart miniature biosensor devices, the applicability of conventional security protocols remains questionable. This research work compares NTRU Encrypt and ECC as potential candidates for SHS, demonstrating their superiority in rapid encryption, quick processing times, and efficient resource utilization.

Subject Classification: 68M25.

Keywords: ECC, NTRU, Encryption, Decryption, Fog computing, IoT, Smart healthcare system.

1. Introduction

The advancement of the healthcare sector, fuelled by innovative technologies, has led to the emergence of the Smart Healthcare System (SHS). The healthcare industry is collaborating with advanced technologies such as Radio-Frequency Identification (RFID) [1], Wireless Sensor Network (WSN) [2], Ultra High Frequency (UHF) [3], and Internet of Things (IoT) [4], Cloud Computing, Fog Computing to realize the goal of SHS. By using real-time data gathering, secure transmission, and proactive treatment options, the SHS seeks to enhance patient monitoring, maximize resource usage, and lower healthcare costs. In the field of remote healthcare, technology is expanding the accessibility of medical services beyond traditional settings, with Smart Healthcare Systems (SHS) utilizing IoT for continuous patient monitoring, early detection of anomalies, and personalized care. In terms of cost-effectiveness, widespread adoption, and social impact, IoT-based solutions are predicted to revolutionize the healthcare industry [5,6]. IoT supports e-health, m-health, and Ambient Assisted Living (AAL), enabling remote patient tracking, observing and facilitating a seamless link through cloud access [7, 8]. Designing standalone wearables is no longer enough; it is now essential to create a whole ecosystem where sensors in a body area network collaborate to sync data with cloud services via the IoT infrastructure [9,10,11]. IoT

technologies continuously capture critical patient data through wearable health monitors and advanced medical sensors. Fog computing nodes that are present closer to the network's edge, can quickly connect to these IoT devices, ensuring low-latency data processing and improved responsiveness. Authors in [12] presented Internet of Vehicles (IoVs) combined with Fog computing which improves real-time vehicle tracking, helping to reduce road accidents. By monitoring speed, location, and alcohol levels, IoVs use machine learning to identify risky vehicles. This system sends safety alerts to prevent collisions, aiming to lower accident rates. The key elements of the Smart Healthcare System include IoT devices, Fog computing nodes, Cloud servers, Electronic Health Records, and Medical Personnel which are described below.

- A. *Medical IoT Devices*: Enables collection of real-time patient data like vital signs and health indicators, through sensors, wearable health monitors, and smart medical equipment.
- B. *Fog Computing Nodes*: Fog computing nodes, which are dispersed closer to the network's edge, process and analyse data from IoT devices in real-time with the least amount of delay and traffic congestion.
- C. *Cloud / Central Servers*: Centralized servers, which also store and manage the data gathered from Fog Computing nodes and give access to authorized medical staff, provide a foundation for Electronic Health Records (EHR) integration.
- D. *Electronic Health Records (EHR)*: Healthcare professionals can access patient data stored in the form of EHR allowing smooth data exchange and care coordination.
- E. *Medical Personnel*: Medical personnel with access to the EHR system, including doctors, nurses, and other permitted employees, utilize it to monitor patients' health, make informed decisions, and provide tailored care.

The flow of real-time patient data from Smart Wearable devices to healthcare professionals via fog computing nodes and centralized servers is depicted in figure 1.

Figure 1, illustrates healthcare framework, Medical IoT devices, such as wearables and implantable sensors, continually gather real-time health data from patients. This data is processed efficiently by Fog Computing Nodes situated at the network edge, ensuring low latency and quick

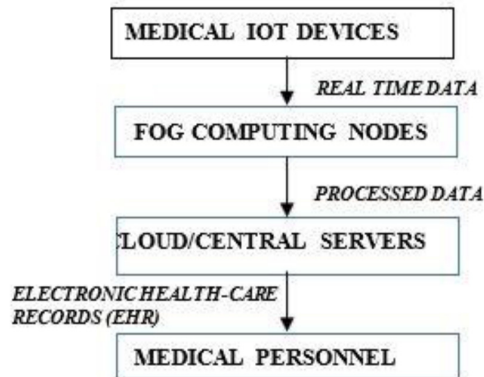


Figure 1

Block diagram of basic healthcare system

decision-making. The processed information is then transmitted to Cloud / Central Servers, where it undergoes further analysis, storage, and retrieval. This centralized approach allows for scalable data management and complex analytics. Meanwhile, the insights derived from these devices and systems empower Medical Personnel, including doctors and nurses, to make informed decisions and deliver personalized care. Together, this interconnected system forms an advanced healthcare ecosystem that enables continuous remote monitoring, timely interventions, and enhanced overall healthcare efficiency.

Even though remote monitoring and data interchange are both important components, SHS must take data security into account. As healthcare systems grow more digital, the potential of data breaches and illegal access has greatly increased. To protect against these risks, the SHS infrastructure is outfitted with cryptographic techniques like AES-32 [13], RSA [14], SIMON [15], TEA [16], NTRU Encrypt [17] and ECC [18]. In order to keep patient information private and secure from any threats, these approaches offer robust data encryption while the data is being transferred. Every cryptographic algorithm has advantages and disadvantages, but most significantly, healthcare IoT devices have limited memory, processing power, and battery life, making it crucial to ensure that cryptographic constructs used in the IoT ecosystem use the least amount of resources possible. The purpose of this research work is to assess how well NTRU Encrypt and ECC perform in Smart Healthcare System in terms of resource utilizations. By considering factors like encryption speed, processing durations, and resource consumption, we

want to identify the best cryptography solution for the healthcare ecosystem.

The purpose of this work is to examine and contrast the resource usage of the ECC and NTRU-Encrypt cryptographic algorithms for data security and encryption in the context of the Smart Healthcare System (SHS). The primary objective is to evaluate their performance in safeguarding sensitive healthcare data, ensuring privacy and integrity within the system. By thoroughly examining and comparing these algorithms, this research endeavours to contribute valuable insights into their effectiveness and suitability for securing data communication within the Smart Healthcare System. Ultimately, this research work seeks to enhance data protection and advance the security measures of modern healthcare information systems, fostering a more secure and efficient healthcare ecosystem.

II. Literature Survey

This section presents the existing research work in Smart Healthcare System and associated security concerns.

To make Internet of Things (IoT) devices more secure, the authors in [19] presented a method involving fog computing and Elliptic Curve Cryptography (ECC). This technique arises in response to the urgent cybersecurity issues related to fog computing and the Internet of Things. It tries to resolve the noted security issues and evaluates the advantages of ECC in a publish-subscribe communication architecture. When compared to conventional cryptographic methods, the suggested protocol offers a resource-efficient solution with scalability and lower overhead through the effective use of fog nodes. The researchers underscore the practical implementation of the protocol on real-world IoT platforms, emphasizing the importance of considering message subject access control. This research introduces an innovative approach that holds significant promise for reinforcing the security of IoT devices and offers a viable solution for addressing the security challenges posed by IoT and fog computing. This protocol's incorporation of ECC and fog computing technologies is a progressive move toward enhancing the security and dependability of IoT devices. Researchers in [20] investigate the application of Smart e-Health Gateways to integrate IoT and CPS in healthcare. These gateways offer real-time data processing and local storage, bridging sensor networks and the internet. The authors advocate for fog computing to enhance healthcare IoT systems, addressing scalability, dependability, energy efficiency, and

mobility challenges. They present the UT-GATE prototype as a promising solution for reliable, intelligent, and energy-efficient health monitoring systems. This system architecture encompasses sensor nodes, networked gateways, and back-end/user interface components to accommodate various network topologies and wireless sensor technologies. Their implementation involves fog-based data processing, LZW data compression, and sensor nodes for ECG, EEG, and EMG signals. By applying the Early Warning Scores medical case study, the authors demonstrate a practical implementation for remote health monitoring. The importance of fog computing and smart e-health gateways in enhancing healthcare IoT systems is highlighted by this study. An inventive approach to integrating CloudFog services into interoperable healthcare solutions that build upon the conventional Cloud-based architecture was the introduction of the Fog-based IoT-Healthcare (FIH) solution structure in [21]. The iFogSim simulator is used to comprehensively assess the FIH system's performance, mainly in terms of latency and power consumption [22]. Rajkomar et al.'s work [23] supports these initiatives by proposing a deep learning method that is accurate and scalable. When taken as a whole, these studies represent important developments in the field of fog-based IoT-Healthcare and highlight the increasing significance of fog and edge computing in data analytics and healthcare solutions. Further exploration of execution speed, precision, and real-world applications is essential to fully comprehend the potential and performance of these innovative solutions. Authors in [24] discuss ECC implementation, including finite fields, curve selection, and attacks, with a focus on the NIST curve P-256 using ElGamal encryption for IoT systems.

By proposing an NTRU-based authentication and key exchange protocol as a solution to replace popular public key cryptography methods like RSA, ECC prone to quantum attacks, researchers in [25] solve privacy issues in IoT settings. Because NTRU's convolution operation is faster than that of conventional systems, the suggested protocol exhibits superior efficiency. It is made to prevent a number of attacks, such as impersonation, replay, man-in-the-middle, and meet-in-the-middle assaults. The NTRU-based protocol guarantees resistance against impersonation and session key disclosure attacks in addition to enhancing security by fending off quantum computing assaults through the use of lattice-based cryptography. The high performance of the protocol, attributed to the use of NTRU, makes it suitable for practical applications in smart home, healthcare, and smart grid environments. The authors of the study mentioned in reference [26] point out that when centralized IoT installations require scalability,

traditional cloud computing frameworks fall short. This is particularly evident in applications that are sensitive to delays, such as health monitoring. In order to address this problem, the paper presents the novel ideas of fog and edge computing, highlighting how they might improve latency and energy efficiency. To address this issue, the authors provide the Health Fog platform, which employs ensemble deep learning in edge devices for automated heart disease analysis. It acknowledges a present flaw in fog models concerning the trade-off between accuracy and response time. The framework makes use of the Fog Bus cloud framework to evaluate its performance. Notably, it offers adjustable modes of operation that enable the adjustment of forecast accuracy or quality of service based on different fog calculation settings and customer needs. This review underscores the growing importance of fog and edge computing in addressing the limitations of traditional cloud computing, particularly in latency-sensitive applications like health monitoring. The Health Fog framework presents a promising step forward in balancing the trade-offs between accuracy and response time in fog-based IoT environments. Authors in [27], presents a secure framework for accessing e-health data on mobile devices, particularly focusing on wearable sensor devices monitoring various health parameters. The proposed framework incorporates a multi-layered authentication process, starting with patient authentication and activating the attached sensor device. Patient biometrics, along with a username and password, are used in the SHA-512 algorithm to ensure integrity. The framework uses an Improved ECC (IECC), which adds an extra secret key for increased security, and the Substitution-Ceaser cipher to transmit sensor data securely. In comparison to current systems, the computational cost is estimated to be $4H + E_c + D_c$. The suggested IECC exhibits a statistically significant average correlation coefficient (0.045) and reduced encryption and decryption durations (1.032 μ s and 1.004 μ s, respectively) when compared to the current RSA and ECC algorithms. Formal security research and simulation have confirmed the scheme's security, offering an effective way to authenticate and Encrypt data from IoT-based medical sensors. The researchers focus on how vulnerable the current digital signature methods are to quantum assaults in their discussion of the integrity concerns associated with medical and healthcare information in a Internet of Medical Things (IoMT) [28]. The NTRU lattice is the basis for their proposed Certificate Less Signature (CLS) method, which exploits the difficulty of solving small integer issues on this lattice to make it immune to quantum threats. The literature review highlights the increasing need to protect patient data in

MCPS, particularly given the emerging risks from quantum computing. The paper introduces a quantum-resistant CLS scheme and provides both security analysis and performance evaluations. The results demonstrate a significant reduction in communication and computational costs when compared to two other quantum-resilient schemes. This research emphasizes the need for quantum attack resilience in e-health systems and offers a practical solution using the NTRU lattice to safeguard medical data integrity in MCPS, laying the foundation for future real-world implementation and assessment. The authors of [29] describe a SHS that uses blockchain technology to monitor patients remotely. To ensure rapid and secure data processing and transfer, the system's three primary levels—smart medical equipment, a fog level, and a cloud level—all work together. This platform is notable for its ability to integrate AI and smart contracts to deliver individualized treatment recommendations, predictive health insights, and immediate emergency alarms. In [30], the researchers introduce the Cross-Layer and Cryptography-based Secure Routing (CLCSR) protocol to address the security and privacy concerns in Internet of Things (IoT)-based smart healthcare systems that utilize Wireless Sensor Networks (WSNs). The protocol, which is developed in Python and Network Simulator (NS2), performs better under various sensor node configurations and attacker scenarios than other protocols, such as Hybrid Secure Routing. The CLCSR algorithm couples lighter ECC for safeguarding privacy with a cross-layer approach for safe clustering to increase average throughput, packet delivery ratio, and resource efficiency. Using lightweight NTRU encryption and Secret Sharing, the authors of [31] offer a novel approach to safe group communication in Internet of Things applications. This solution focuses on security issues in IoT networks, particularly in VANET, Precision Agriculture, and Internet of Medical Things (IoMT). The three-tiered architecture consists of a cloud server, sink nodes, and field sensor nodes. Initialization, registration, and group key generation are the three primary stages of the scheme's development. The suggested approach improves security while satisfying the crucial requirement for minimal computing overhead in IoT devices by fusing NTRU encryption with secret sharing.

Background

This section describes the cryptographic algorithms that are considered in this research work. NTRU and ECC are two cryptographic algorithms that exhibit strong security properties and computational

efficiency, making them reliable choices for secure communication and data protection in various applications:

- A. N-th degree Truncated Polynomial Ring (NTRU) [17]: The NTRU is public key cryptosystem based on lattice-based encryption. It offers a secure replacement for well-known algorithms like ECC. The speed and efficiency of NTRU are particularly beneficial, making it appropriate for devices with constrained resources like mobile platforms and IoT devices. Unlike ECC, which is based on the mathematical properties of elliptic curves, the security of NTRU is based on the difficulty of producing short vectors in particular lattices. Thanks to this unique technique, which also reduces computational cost, NTRU is able to offer strong security with relatively small key sizes, in contrast to ECC.
- B. Elliptic curve cryptography (ECC), [18]: ECC is a well-known public-key cryptographic technique. It depends on elliptic curve properties to ensure secure communication and data security across the internet. ECC is more efficient in terms of computation and bandwidth use since it provides better security with shorter key lengths than other methods. Some of its applications include secure messaging, digital signatures, and encryption for various online transactions and interactions. ECC is widely used because it may offer strong security while using few resources, which makes it a viable solution for modern cryptographic needs.

NTRUEncrypt and ECC techniques find applications in ensuring secure data transmission, storage, and safeguarding sensitive patient information through authentication and encryption mechanisms. The choice between NTRUEncrypt and ECC, or their combination, depends on specific security requirements, computational resources, and the evolving threat landscape, necessitating ongoing awareness of cryptographic developments for sustained healthcare system security.

III. Implementation and Results

NTRU and ECC have been implemented using Python 3.9 and Python 2, with essential libraries such as Numpy, Sympy, and Matplotlib employed for numerical operations, symbolic mathematics, and data visualization. The development environment included VS Code as the primary integrated development environment, and Google Colab was utilized for

resource-intensive tasks, leveraging its cloud-based Jupyter notebook environment. Numpy was instrumental in handling mathematical operations involving extensive datasets, Sympy facilitated symbolic mathematics crucial in cryptographic computations, and Matplotlib was employed for creating visual representations of data and results. Security analysis considered the mathematical rigor underlying both algorithms, while performance metrics include encryption and decryption speeds, resource utilization, key generation times, and key sizes. The resistance of each algorithm to common cryptographic attacks is also discussed.

Quantitative data on key aspects such as speed, resource utilization, and key generation times were presented, enabling a comprehensive analysis of the strengths and weaknesses of each algorithm. The research aimed to draw conclusions regarding the suitability of NTRU and ECC for specific use cases based on the implemented comparisons. Overall, the detailed implementation and thorough evaluation of these cryptographic algorithms contribute valuable insights to the field of secure communications and cryptographic research.

A. Security Analysis:

Cryptographic Attack Resistance: The resilience of the NTRU and ECC cryptographic techniques to various attack types is contrasted in Table 1. ECC and NTRU are both categorized as “Resistant” to known-plaintext, chosen-ciphertext, and brute force attacks. But according to Shor’s Algorithm, NTRU is “Partially Resistant” to quantum attacks, but ECC is “Vulnerable” in the same circumstances. Furthermore, ECC is categorized as “conceivably Vulnerable” to such advanced attack methods, but NTRU is impervious to sub-exponential and lattice-based assaults. This

Table 1
Comparison of resilience to security attacks

ATTACK TYPE	NTRU	ECC
Brute Force Attack	R	R
Known-Plain Text Attack	R	R
Chosen-Cipher Attack (IND-CCA2)	R	R
Quantum Attacks (Shor’s Algorithm)	PR	V
Lattice-Based Attacks	R	PV
Sub-exponential Attacks	R	PV

*R = Resistant, V = Vulnerable, PR = Partially Resistant, PV = Potentially Vulnerable

comparison demonstrates how the security characteristics of NTRU and ECC change depending on the kind of attack.

B. Performance Analysis:

The research work considers the encryption and decryption times for measuring the feasibility of chosen algorithm for SHS. The analysis of these timings implies the amount of time for which the processing board remains active, which directly affects the battery usage and significantly impacts on lifetime of healthcare IoT devices.

- i. *Encryption Time:* The time taken by the cryptographic algorithms to Encrypt the various input data sizes is illustrated in Table 2 and is graphically represented in Figure 2.

Table 2
Comparison of Encryption times of ECC and NTRU

Data Size (bytes)	ECC Encryption Time (ms)	NTRU Encryption Time (ms)
10	1	0.5
50	2	1.5
100	3	2
200	5	4
500	12	10
1000	25	20

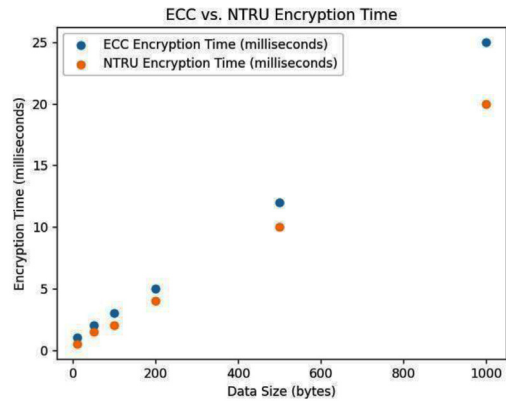


Figure 2
Encryption Times Comparison

From the observations in Figure 2 and Table 2 it is evident that the encryption time for NTRU is consistently shorter than that of ECC across all data sizes.

- ii. *Decryption Time*: The computation of decryption times for different input data sizes for ECC and NTRU is depicted in Table 3 and graphically plotted in figure 3.

Table 3
Comparison of Decryption times of ECC and NTRU

Data Size (bytes)	ECC Decryption Time (ms)	NTRU Decryption Time (ms)
10	1	0.7
50	2	1.8
100	3	2.3
200	5	4.2
500	11	11
1000	22	23

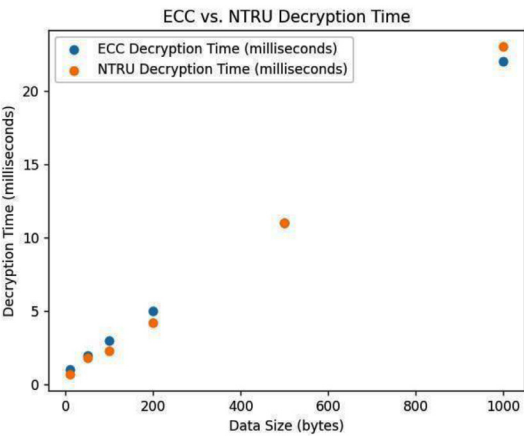


Figure 3
Decryption Times Comparison

Figure 3 and Table 3 and figure 3 demonstrate that the decryption time for NTRU is shorter compared to ECC.

- iii. *Memory Requirements*: For healthcare IoT devices such as the Apple Watch [32], the ECC and NTRU cryptographic algorithms are viable choices due to their minimal memory requirements.

The latest Apple Watch Series 8, boasting a memory capacity of approximately 32 GB, exceeds the standard needs for implementing both ECC and NTRU algorithms. Without substantial optimizations, a 256-bit ECC implementation typically necessitates around 9.8 KB of memory, while a common NTRU implementation requires approximately 5.2 KB of memory when employing a parameter set like NTRUEncrypt-256 (which utilizes 256-bit public and private keys). This generally results in lower memory usage compared to an equivalent ECC implementation. Figure 4 illustrates the comparison of memory requirements between ECC and NTRU-Encrypt.

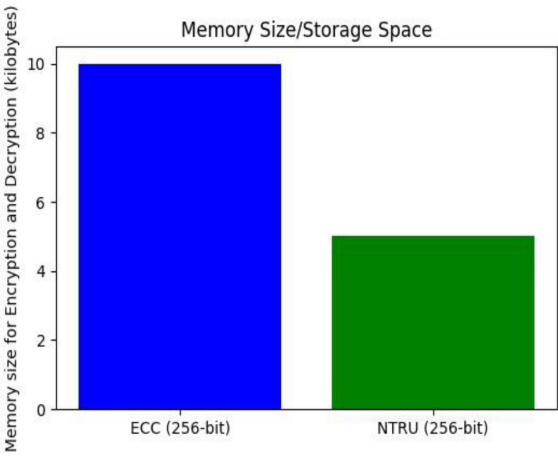


Figure 4

Memory Requirements

Based on the figure 4, we realize that NTRU takes less memory as compared to ECC which further strengthens the claim that NTRU outperforms ECC.

IV. Conclusion

Based on the outcomes of this research, we draw the conclusion that both ECC and NTRU cryptographic algorithms are viable choices for healthcare IoT devices. Nevertheless, NTRU exhibits distinct advantages in terms of computational efficiency and memory utilization during both encryption and decryption processes. Specifically, NTRU encryption demonstrates a significant 14.29% faster performance compared to ECC encryption. Moreover, in the context of decryption, NTRU maintains its

computational superiority, showcasing a commendable 4.49% faster performance than ECC decryption for the specified data sizes in this particular scenario. These findings underscore NTRU's potential as a robust cryptographic algorithm, offering improved performance for encryption and decryption tasks. Beyond its computational benefits, NTRU's resistance to quantum attacks adds an additional layer of security, making it highly effective for safeguarding sensitive data, especially in smart healthcare systems. Its compatibility with IoT and fog computing further enhances security in connected healthcare networks. By capitalizing on NTRU's strengths, healthcare organizations can establish a resilient infrastructure, mitigating vulnerabilities, instilling trust in data interchange, and optimizing the use of limited available resources.

Acknowledgement

This research work was funded by JKST&IC and is currently being implemented at Islamic university of Science and Technology, Kashmir.

References

- [1] C. T. Turcu, "RFID-based solutions for smarter healthcare," arXiv preprint arXiv:1705.09855 (2017).
- [2] A. Onasanya, S. Lakkis, and M. Elshakankiri, "Implementing IoT/WSN based smart Saskatchewan healthcare system," *Wireless Networks*, vol. 25, pp. 3999–4020 (2019).
- [3] S. de Miguel-Bilbao, J. A. Hernandez, O. J. Suarez, P. Marina, V. M. Febles, L. E. Rabassa, S. Suarez, J. Karpowicz, P. Zradzinski, K. Gryz, and E. Aguirre, "Near field exposure conditions by UHF-RFID systems in smart healthcare environments," in Proc. 2021 IEEE Int. Joint EMC/SI/PI and EMC Europe Symp., pp. 13–18 (2021).
- [4] L. Catarinucci, D. De Donno, L. Mainetti, L. Patrono, M. Stefanizzi, M. L. Lops, and L. Tarricone, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526 (Dec. 2015).
- [5] A. Dohr, R. Modre-Opsrian, M. Drobits, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in Proc. Int. Conf. Information Technology: New Generations, pp. 804–809 (2010).

- [6] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516 (2012).
- [7] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516 (2012).
- [8] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Gener. Comput. Syst.* (2017).
- [9] European Research Cluster on the Internet of Things, "IoT semantic interoperability: Research challenges, best practices, solutions and next steps," IERC AC4 Manifesto - "Present and Future," (2014).
- [10] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1578–1586 (2014).
- [11] L. Jiang, L. D. Xu, H. Cai, Z. Jiang, F. Bu, and B. Xu, "An IoT-oriented data storage framework in cloud computing platform," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1443–1451 (2014).
- [12] R. Parveen, R. Singh, and S. Kumar, "IoV based intelligent vehicle tracker using fog computing with supervised machine learning techniques," *J. Discrete Math. Sci. Crypt.*, vol. 24, no. 5, pp. 1393–1413 (2021).
- [13] T. N. Dang and H. M. Vo, "Advanced AES algorithm using dynamic key in the Internet of Things system," in *Proc. 2019 IEEE 4th Int. Conf. Comput. Commun. Syst.*, Singapore, pp. 682–686 (2019).
- [14] P. Bhati, S. Tripathi, S. Kumari, S. Sachan, and R. Sharma, "A research on DNA and RSA cryptography for hybrid encryption and decryption for cloud processing via IoT devices," in *Proc. 2023 2nd Int. Conf. Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*, Vellore, India, pp. 1–5 (2023).
- [15] N. Allassaf, A. Gutub, S. A. Parah, and M. Al Ghamdi, "Enhancing speed of SIMON: A lightweight-cryptographic algorithm for IoT applications," *Multimedia Tools Appl.*, vol. 78, pp. 32633–32657 (2019).
- [16] M. Abdulraheem, J. B. Awotunde, R. G. Jimoh, and I. D. Oladipo, "An efficient lightweight cryptographic algorithm for IoT security,"

- in Proc. Int. Conf. Information and Communication Technology and Applications, pp. 444–456 (2020).
- [17] O. M. Guillen, T. Pöppelmann, J. M. B. Mera, E. F. Bongenaar, G. Sigl, and J. Sepulveda, "Towards post-quantum security for IoT endpoints with NTRU," in Proc. Design, Automation & Test in Europe Conf. & Exhibition (DATE), pp. 698–703 (2017).
 - [18] H. B. Mahajan and A. A. Junnarkar, "Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing," *Multimedia Tools Appl.* (2023).
 - [19] A. A. Diro, N. Chilamkurti, and N. Kumar, "Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing," *Mobile Netw. Appl.*, vol. 22, pp. 848–858 (2017).
 - [20] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jjiang, and P. Liljeberg, "Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Gener. Comput. Syst.*, vol. 78, pp. 641–658 (2018).
 - [21] R. Mahmud, F. L. Koch, and R. Buyya, "Cloud-fog interoperability in IoT-enabled healthcare solutions," in Proc. 19th Int. Conf. Distributed Computing and Networking, ACM, p. 32 (2018).
 - [22] R. M. Abdelmoneem, A. Benslimane, E. Shaaban, S. Abdelhamid, and S. Ghoneim, "A cloud-fog based architecture for IoT applications dedicated to healthcare," in Proc. 2019 IEEE Int. Conf. Communications (ICC), 2019, pp. 1–6 (2019).
 - [23] A. Rajkomar, E. Oren, K. Chen, A. M. Dai, N. Hajaj, M. Hardt, P. J. Liu, X. Sun, P. Sundberg, H. Yee, and others, "Scalable and accurate deep learning with electronic health records," *NPJ Digit. Med.*, vol. 1, no. 1, p. 18 (2018).
 - [24] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *J. Interdiscip. Math.*, vol. 23, no. 2, pp. 463–470 (2020). doi: 10.1080/09720502.2020.1731959
 - [25] S. Jeong, K. Park, Y. Park, and Y. Park, "An efficient NTRU-based authentication protocol in IoT environment," in K. Arai, S. Kapoor, and R. Bhatia (eds.), *Intelligent Computing. SAI 2018, Adv. Intell. Syst. Comput.*, vol. 857, Springer, Cham, pp. 1153–1165 (2019). doi: 10.1007/978-3-030-01177-2_91.

- [26] S. Tuli, N. Basumatary, S. S. Gill, M. Kahani, R. C. Arya, G. S. Wander, and R. Buyya, "HealthFog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments," *Future Gener. Comput. Syst.*, vol. 104, pp. 187–200 (2020).
- [27] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," *IEEE Access*, vol. 8, pp. 52018–52027 (2020).
- [28] Z. Xu, D. He, P. Vijayakumar, K. K. R. Choo, and L. Li, "Efficient NTRU lattice-based certificateless signature scheme for medical cyber-physical systems," *J. Med. Syst.*, vol. 44, pp. 1–8 (2020).
- [29] L. Fetjah, K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "Towards a smart healthcare system: An architecture based on IoT, blockchain, and fog computing," *Int. J. Healthcare Inf. Syst. Informatics (IJHISI)*, vol. 16, no. 4, pp. 1–18 (2021).
- [30] A. Kore and S. Patil, "Cross layered cryptography based secure routing for IoT-enabled smart healthcare system," *Wireless Netw.*, pp. 1–15 (2022).
- [31] S. Saha, A. Hota, B. Choudhury, A. Nag, and S. Nandi, "NTRU and secret sharing based secure group communication for IoT applications," *IEEE Access*, vol. 11, pp. 117341–117350 (2023). doi: 10.1109/ACCESS.2023.3325305
- [32] Apple Inc., "Apple Watch Series 6 – Technical Specifications," [Online]. Available: https://support.apple.com/kb/SP878?locale=en_US. [Accessed: Jun. 30, 2024].

Received July, 2024