Security Optimization of Resource-Constrained Internet of Healthcare Things (IoHT) Devices Using Asymmetric Cryptography for Blockchain Network

Varsha Jayaprakash[1], Amit Kumar Tyagi[2,3|0000-0003-2657-8700|*]

[1]School of Electronics Engineering, Vellore Institute of Technology, Chennai
[2]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai
[3]Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, Tamilnadu, India
varsha.jayaprakash2019@vitstudent.ac.in, amitkrtyagi025@gmail.com
*Corresponding author: amitkrtyagi025@gmail.com

ABSTRACT: The term "Internet of Things" is becoming increasingly popular and promising, ushering in a new era of smarter connectivity across billions of gadgets. In the foreseeable future, IoT's potential is boundless. The healthcare industry, often known as IoHT, is the most demanding application of IoT. Any healthcare-based IoT system starts with sensors, RFID, and smart tags, all of which are limited in terms of resources. When these devices are integrated, there is a significant need for safe information transformation since they carry sensitive patient information that might be extremely dangerous if it falls into the hands of an unauthorized person. The internet of things based on blockchain is a new technology that combines the benefits of both blockchain and cryptography to protect data at the physical layer. It is lightweight compared to other traditional approaches and does not compromise security levels, as the name implies. This paper explains how to safeguard data using elliptic curve cryptography for blockchain network to encrypt and store the data. On the basis of energy and memory efficiency, as well as latency, the proposed method is evaluated.

KEY WORDS*: Security, IoHT, sensors, RFID, resource constraints, blockchain, elliptic curve cryptography, latency, efficiency.*

1. Introduction

The Internet of Things has become the most widely used term in the world today. It is a technical concept that entails practical devices such as sensors and actuators that are used to collect real-time data, convey that data over the internet, and store that data on cloud-based platforms with or without human participation [1-3]. In 1999, Kevin Ashton coined the term "Internet of Things" to promote the usage of radio frequency-based identification (RFID), which involves a variety of embedded devices. With the advent of home automation, industrial energy meters, wearable and self-health care devices in 2011, the tremendous expansion of IoT-based devices began [4]. The health-care industry is a significant contribution to the overall number of IoT-enabled devices in the world. The advent of IoHT allows patients to self-assess their body states while concurrently uploading these data to the hospital's server, allowing doctors to maintain track of patients' health problems and schedule exams and visits only as needed, saving both money and time [5-6]. However, the widespread adoption of this

technology has resulted in a slew of concerns and challenges relating to patient data protection. Data protection is required at three layers in any IoHT device: physical/design, communication, and computation. They are further categorized as resource rich (phones, tablets, computers) and resource constrained (sensors, RFID) devices (Fig 1) [7]. Resource constrained devices are often used to deal with real time applications that require accurate processing of data. In addition to this they are limited in terms of power consumption, available memory and computation speeds [8-9].

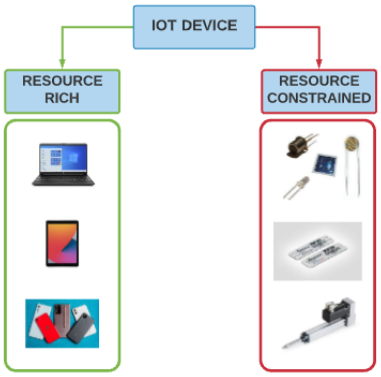

Fig 1: Categorization of IoT devices

In most of the countries, the authentic information provided by the healthcare data should be confined through "Health Information and Portability Accountability Association (HIPAA)" [9]. Efficient and safe implementation of these healthcare systems can be achieved by using optimized and robust security systems [10]. Due to the mutual distrust in the environment, gadgets will be unable to operate independently and will need to be secured and authenticated in order to function effectively. Blockchain is a distributed ledger-based authentication system can be used to keep data comprising many types of health information secure and private. Consistency of storage data is achieved using consensus algorithm. The entire framework is distributed between nodes so that even the failure of few nodes will not tamper the data or allow new attacker nodes to enter into the system [11]. Whenever peer-peer communication is observed, the public key cryptographic algorithm is used for authentication purpose between IoT devices. However, to lower the barrier to implementing and using blockchain in these cases, a lightweight blockchain consensus should be established [12]. It makes any network decentralized by improving the security. Each device in a blockchain network has a unique device ID, private key and hash function of critical data for authentication validation before the access is given to the IoT device. Asymmetric cryptography such as elliptic curve cryptography or SHA-256 is used to encrypt and decrypt the data after authentication before storing in the blocks [13].

Organization of the Work: The paper is organized as follows: Section II give a literature survey regarding related researches followed by motivation in Section III. Section IV describes the challenges in designing a secure IoT system and Section V provides solution for security of resource constrained IoHT devices. Section VI describes the blockchain mechanism employed for secure transfer of health data. Section VII explains the working principle and the algorithm of elliptic curve cryptographic algorithm used for encryption purpose before storage of data in

the blocks. Section VIII discusses the simulation results. Section XI provides an insight about the future scope of this research followed by conclusion.

2. Related Work

A lightweight blockchain architecture for healthcare database management was proposed by Leila Ismail and Huned Materwala [14]. The network participants are divided into demographic clusters by maintaining one copy of ledger. Forking is avoided by using a using a Head Blockchain Manager to handle transactions. The proposed method outperforms traditional Bitcoin network in terms of network traffic generated and computation speed. An autonomous solution to store the user credentials without the dependence of TTP was proposed by Daniel Maldonado-Ruiz [15]. The method developed was coined as "Three Blockchains Identity Management with Elliptic Curve Cryptography (3BI-ECC)". Their system ensures that there is full integrity with secure identity and communication infrastructures with the presence of specific identity blockchains in the network. The system is more transparent to the user. Utsav Banerjee, Anantha P. Chandrakasan [16] developed a variant of elliptic curve cryptography algorithm and named it a pair-based cryptography (PBC). It uses the functions of bilinear maps between elliptic curve and finite fields that enables it to be used in novel applications other than secure key exchange. Chips were fabricated involving these secure algorithms with pairing crypto core occupying 112k NAND Gate Equivalents (GE) and 16KB of SRAM proving it to be an efficient and low-power architecture. Dipankar Dasgupta, John M. Shrein and Kishor Datta Gupta [17] discussed about the strength, power consumption, security level, complexity and vulnerability of various cryptographic algorithms used in blockchain in healthcare domain such as NIST P-256 curve, DSA, ECDSA and Cryptographic hashes. They consider ECC to be susceptible to side channel attacks, fault and timing attacks. SHA-256 is considered to be unbreakable according to them. They also discussed some new research rends in blockchain and the new vulnerabilities that could occur in future.

Then, Chiu C. Tan,, Haodong Wang, Sheng Zhong and Qun Li [18] developed a lightweight identity based cryptography for body sensor networks that manages security, privacy and accessibility for health care monitoring and tested it on commercially available sensors. Simulation results showed that the proposed method performs faster computation than other sensor platforms but suffered from slow query performance compared to other ciphers. Further an efficient and secure authentication for IoT healthcare devices based on RFID tags and card readers using elliptic curve cryptography (ECC) was proposed by Davood Noori [19]. This authentication system can be used for safe communication of information regarding patients' health. The proposed algorithm proves to be efficient in terms of complexity due to lower computation cost and lesser multiplication rounds in ECC compared to other techniques. An FPGA-acceleration of ECC operation suing binary Edward curves were implemented by Carlos Andres Lara-Ninoa and Arturo Diaz-Perez [20]. The method takes advantage of the scalar point multiplication property of ECC algorithm. Results show that the proposed technique uses only 1400 slices of Virtex-5 FPGA to provide a security strength of up to 128 bits.

3. Motivation

Health care is one of the fastest sectors to adapt to the changes made in IoT based systems. ""MarketsAndMarkets" predicts that IoHT will be worth US$ 163.2B, commercial report claims a spending of $117B, and McKinsey estimates an economic impact of more than US$ 170B" [21]. development of e-health systems such as electrocardiography,

electroencephalogram, diabetes can be cost saving and help patients suffering with chronic diseases reduce the number of hospitals visits [22]. Also, the outbreak of covid-19 pandemic has created a fear in minds of people and refraining them visiting hospitals which could potentially cause them to suffer from the virus. This has enabled the IoHT sector to grow exponentially and will continue to bloom for the next few years. People are now looking for safer and less expensive ways to maintain and monitor their health. Due to the increased number of users, it has become an attractive sector for hackers. Hence, it is important to develop IoT based systems with enhanced security that enables safe transfer and computation of patients' data. Security can be achieved by various methods like cryptography, block chain technology, machine learning techniques like supervised, unsupervised and reinforced learning etc. [23]. This paper focuses on blockchain based network using elliptic curve cryptography to protect the data at the sensing/physical layer of any IoT based system.

4. Concerns and Challenges in Implementation of Cryptographic Techniques to Resource Constrained IoHT Devices

From physical sensors to computer servers, any IoT network incorporates a wide variety of platforms. This creates a slew of new difficulties for consumers, including privacy, security, compatibility, scalability, and interoperability [23]. IoT devices are a particularly appealing target for hackers because they interact directly with the actual environment to collect sensitive data [24]. The most common attacks experienced in this stage includes eavesdropping, replay attacks, node capture attacks, side channel attacks etc. These devices can potentially be physically damaged in addition to being tapped to gather the sensitive data provided. As a result, cyber security is required, which is regarded as a key problem in the implementation of authentication, data security, availability, privacy, and accessibility [25]. The approach used to protect sensitive data is entirely dependent on the surroundings. The proposed approach must be appropriate and highly secure for an IoT device's applied layer, but it must be developed in such a way that it does not interfere with the device's normal operations. Because these devices are resource constrained, traditional PC cryptography approaches do not fit into this group.

Fig 2: Challenges in implementation of cryptography

Figure 2 explains the cryptographic technique used to preserve this information must be designed by keeping in mind the limitation of the device. The major challenges include [26]: Low computation power, Lower energy, Reduction in availability of space due to smaller size, Reduction in memory space (ROM and RAM), Lower power and Faster execution time

5. Solutions to Enhance Security in Physical Layer of IoHT Devices

The main characteristics to be taken into consideration while choosing the right cryptographic techniques are cost, performance and security level. Performance can further be divided into subsections such as energy and power consumption, latency, computation speed, memory occupation and different attack models such as linear and differential attacks, side channel attacks and gault injection attacks [27]. Most of the above-mentioned concerns are solved following LWC techniques with simple key and lesser number of rounds [1]. Cryptographic techniques are categorized as symmetric and asymmetric based on the number of keys. A symmetric cryptographic technique uses the same key for encryption as well as decryption whereas asymmetric technique has two private public key pairs [28]. In symmetric block ciphers the encryption and decryption process take place continuously. Many asymmetric algorithms such as ECC, ChaCha20 are widely used today for both lightweight as well high-end security systems [29]. This enables to share information between two parties by generating a common secret key without actually revealing each of the party's private keys [30].

6. Blockchain Based IoHT Devices

Blockchain is a public ledger used for secure and consistent transactions by anonymous users termed as miners. Only the first miner who soles the proof of work (POF) will get rewarded with bitcoins, which ultimately lead to the extension the blockchain network. The verified transactions are stored in the body of the blockchain using a structure called the Merkle tree and the blocks are linked together [31]. This decentralized characteristic of blockchain declines the need for authorities to monitor transactions and makes the system more secure, fair and unbiased [32]. As the work is now trending towards online mode of processing, Healthcare sector is also not spared from this trend. With the increasing demand for data collection, processing and storage electronically in digital format, there is equally vulnerable on the security of data being transferred across network and it opens a gate for the hackers to easily trap the information being transferred if it is not secured and encrypted. Blockchain is an advanced cryptographic technology that supports and ensures secured transmission of electronic data and it is emerging in the healthcare industry very rapidly as healthcare is becoming a vital part of our lives [33]. With healthcare automation, all the healthcare services are interconnected electronically for storing and retrieving patients' health information, monitoring and investigating healthcare details through different medium. Blockchain technology helps in revolutionizing the conventional healthcare practices to a more secured, personalized, reliable and efficient mode of practice in terms of data sharing, drug traceability, clinical trials and pharmaceutical supply chain management due to its flexible, trusted, shared and reliable architecture.

Integration of Blockchain technology with IoHT is gaining potential to address and overcome data vulnerabilities due to its (i) Scalable and decentralized architecture (ii) Uniqueness to develop applications without cloud or server dependencies (iii) Dependability

and traceability to IoHT data (iv) Ability to provide secured data transmission between IoHT devices (v) Transparency to data (vi) Reliability to services [34].

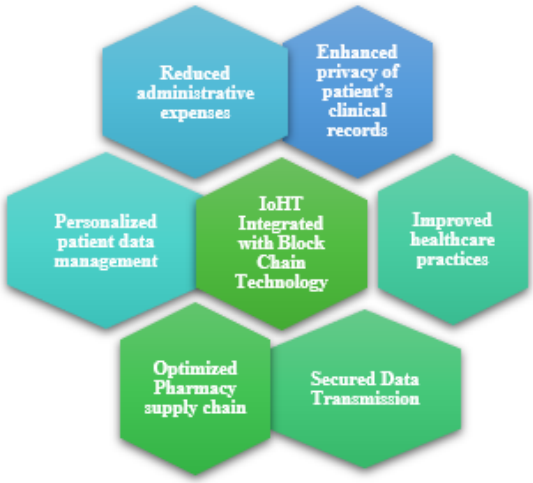

Fig 3: Advantages pf blockchain technology

Several healthcare companies use IoHT to provide services such as patient monitoring, asset management, and inventory tracking. Due to enhanced transparency and security in communication, the introduction of Blockchain characteristics in the healthcare industry provides confidence and dependability in data and services to all parties participating in this segment. There is still a lot of research being done to optimize and address the challenges of data standardization and regulation, integration with existing healthcare systems, the establishment of Blockchain-IoHT policies, improvement of latency and throughput for huge healthcare data and to prove that the healthcare practices implemented using Blockchain technology is safe and reliable before large-scale implementation.

7.Elliptic Curve Cryptography for Private Key Generation

Elliptic curve cryptography is an asymmetric public key-based encryption technique based on algebraic structure of elliptic curve over finite field that offers high level of security with lesser key size compared to other existing techniques. It was first proposed by Victor Miller **and Neal Koblitz in the year 1985 [35].** The private-public key pairs are obtained by solving the elliptic curve equation defined over a finite field given by:

$$y2 = \{x3 + ax + b\} \bmod \{p\} \qquad (1)$$

where, p is any prime number and a and b are constants such that $4a3 + 27b2 = 0$.

The user comes to a conclusion after a common elliptic curve equation to generate private-public key pairs. Each of them uses the other users public key to generate a new set of secret keys for encryption purposes. Since this uses a common key based on the users' private keys, it is difficult for any intruder to tap the message. The elliptic curve can be defined using any type of numbers namely rational, real or complex [36]. The elliptic curve lacks a straightforward encryption mechanism. Instead, ECC is used to generate a common secret key, and the data is encrypted using Elliptic Curve Diffie–Hellman (ECCDH), a hybrid cryptography system [37]. ECCDH, on the other hand, is vulnerable to man-in-the-middle

attacks [38]. After generating a secret key based on mutual acceptance, the key can be used to encrypt data using any symmetric or asymmetric technique, such as ChaCha20, AES-GCM, RSA, and so on. Confidentiality, authentication, and non-repudiation are all guaranteed via the key exchange method [39]. This paper discusses the implementation of ECC to generate private and public secret keys and develop a mechanism to encrypt the data using Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) algorithm involving the secret keys generated using ECC. The algorithm of both ECC ad RSA is discussed below.

6.1 Algorithm For ECC Based Secret Key Generation

- **EncryptionKey**(pubKey) --> (sharedECCKey, ciphertextPubKey)
- Generate **ciphertextPrivKey** = new **random** private key.
- Calculate **ciphertextPubKey** = ciphertextPrivKey * G.
- Calculate the ECDH shared secret: **sharedECCKey** = pubKey * ciphertextPrivKey.
- Return both the **sharedECCKey** + **ciphertextPubKey**. Use the **sharedECCKey** for symmetric encryption. Use the randomly generated **ciphertextPubKey** to calculate the decryption key later.
- **DecryptionKey**(privKey, ciphertextPubKey) --> sharedECCKey
- Calculate the ECDH shared secret: **sharedECCKey** = ciphertextPubKey * privKey.
- Return the **sharedECCKey** and use it for the decryption.

6.2 RSA

RSA is one of the most famous algorithms used even today in digital signatures and blockchain networks. It involves the use of both public and private keys to encrypt and decrypt the information. The difficulty in retrieving the plain text back from cipher text depends on the massive product of the two large prime numbers [40].

RSA Encryption algorithm

- Input: RSA public key (n,e), Plain text
- Output: Ciphertext c
- Begin 1. Compute $c= m^e \bmod n$
- 2. Return c:
- End

RSA Decryption algorithm

- Input: Public key (n,e); Private key d; Ciphertext c
- Output: Plain text m
- Begin 1. Compute $c=c^d \bmod n$
- 2. Return m.
- End

8. Results and Discussion

The ECC algorithm is used to generate the secret key by generating random public keys and the obtained secret key for encryption and decryption is used as key for RSA algorithm of symmetric encryption. The following algorithms were implemented in Python and the results are mentioned below.

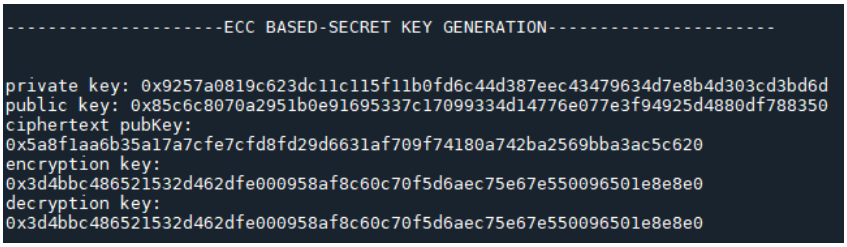

Fig 4: Secret key generation using ECC

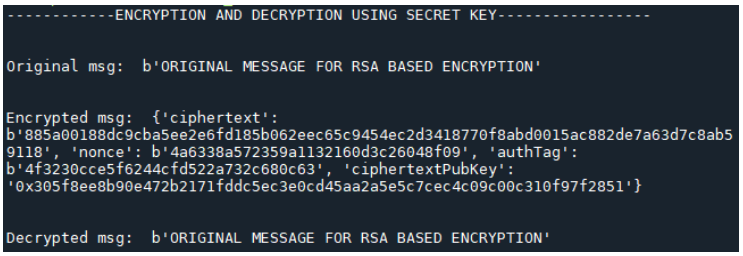

Fig 5: Encryption and decryption of data using symmetric cipher

For encryption and decryption, two distinct secret keys, namely public and private key pairs, are formed, as shown in Fig 4. As demonstrated in Fig 5, the public key pair is also utilized as a key for symmetric encryption using the RSA technique to encode and decrypt data.
The efficiency of algorithms will be investigated in the future by implementing them in a lightweight blockchain network.

9. Conclusion and Future Work

This paper examines the software implementation of the ECC algorithm for generating secret keys for data encryption in an IoHT blockchain network. The challenges of low-scale embedded device security, as well as various methods to solve them, were examined. The use of blockchain in IoHT was also discussed, and it was implemented by using ECC to generate a secret key and RSA symmetric cypher to encrypt data and update data on the blocks. These algorithms are also planned to be implemented in a lightweight blockchain network in the future, with the goal of determining their efficiency in terms of latency, memory usage, and throughput.

9.1 Future Work

IoT applications are growing rapidly day by day and as most of the industries are moving towards IoT, energy consumption is one of the main constraints of the IoT world [41-42]. The limited computational capabilities and resource constraints make it a vulnerable target for hackers [42]. IoHT is a field that is widely in use now. It deals with millions of patients' health information which needs to be secured in order to prevent misuse. In future, light weight cryptographic encryption in IoHT can improve the security level of the system and help to make the devices more efficient and secure. Lightweight block ciphers are efficient in both hardware as well as software. Asymmetric block ciphers, stream, hash and elliptical curve functions are

other available techniques which have a high potential to be employed in these devices to secure patients' information in IoHT [44, 45]. A lightweight blockchain network for secure authentication of patient's data can be developed that uses ECC algorithm to encrypt the data before it is updated on the ledger. Further the hardware performance can be studied by implementing these techniques in real time embedded systems, ARM-based microprocessors and dedicated integrated circuits which are widely used in IoHT industry to observe various parameters like circuit-footprint, throughput, latency, energy and power consumptions in order to design ultra-low power IoT devices.

Acknowledgement

We thank the Centre for Advanced Data Science and School of Computer Science and Engineering, Vellore Institute of Technology, Chennai for providing an opportunity and their kind support to proceed with the research work on time.

References

[1] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in *IEEE Access*, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] Singh, S., Sharma, P.K., Moon, S.Y. *et al.* Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *J Ambient Intell Human Comput* (2017).

[4] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, Jun. 2020.

[5] Kute S.S., Tyagi A.K., Aswathy S.U. (2022) Industry 4.0 Challenges in e-Healthcare Applications and Emerging Technologies. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_1

[6] Kute S.S., Tyagi A.K., Aswathy S.U. (2022) Security, Privacy and Trust Issues in Internet of Things and Machine Learning Based e-Healthcare. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_15

[7] K. McKay, L. Bassham, M. S. Turan, and N. Mouha, Report on Lightweight Cryptography (Nistir8114). Gaithersburg, MD, USA: NIST, 2017.

[8] O. Toshihiko, ''Lightweight cryptography applicable to various IoT devices,'' NEC Tech. J., vol. 12, no. 1, pp. 67–71, 2017.

[9] Ullah A, Sehr I, Akbar M, Ning H (2018) FoG assisted secure De-duplicated data dissemination in smart healthcare IoT. In: 2018 IEEE international conference on smart internet of things (SmartIoT). IEEE, pp 166–171.

[10] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review," *Symmetry*, vol. 12, no. 7, p. 1191, Jul. 2020.

[11] D. Li, W. Peng, W. Deng and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 2018, pp. 1-6, doi: 10.1109/ICCCN.2018.8487449.

[12] Berdik, David, Otoum, Safa, Schmidt, Nikolas, et al. (2021). A Survey on Blockchain for Information Systems Management and Security. Information Processing & Management, 58(1).

[13] Alexopoulos N, Daubert J, Mühlhäuser M, et al. Beyond the Hype: On Using Blockchains in Trust Management for Authentication [J]. 2017:546-553.
[14] L. Ismail, H. Materwala and S. Zeadally, "Lightweight Blockchain for Healthcare," in *IEEE Access*, vol. 7, pp. 149935-149951, 2019, doi: 10.1109/ACCESS.2019.2947613.
[15] D. Maldonado-Ruiz, J. Torres and N. El Madhoun, "3BI-ECC: a Decentralized Identity Framework Based on Blockchain Technology and Elliptic Curve Cryptography," *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 2020, pp. 45-46, doi: 10.1109/BRAINS49436.2020.9223300.
[16] [16] U. Banerjee and A. P. Chandrakasan, "A Low-Power Elliptic Curve Pairing Crypto-Processor for Secure Embedded Blockchain and Functional Encryption," *2021 IEEE Custom Integrated Circuits Conference (CICC)*, 2021, pp. 1-2, doi: 10.1109/CICC51472.2021.9431552.
[17] Dasgupta, D., Shrein, J.M. & Gupta, K.D. A survey of blockchain from security perspective. *J BANK FINANC TECHNOL* **3,** 1–17 (2019). https://doi.org/10.1007/s42786-018-00002-6
[18] C. C. Tan, H. Wang, S. Zhong and Q. Li, "IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks," in *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 6, pp. 926-932, Nov. 2009, doi: 10.1109/TITB.2009.2033055.
[19] Noori, D., Shakeri, H. & Niazi Torshiz, M. Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment. *EURASIP J. on Info. Security* **2020,** 13 (2020). https://doi.org/10.1186/s13635-020-00114-x
[20] Lara-Nino, Carlos Andres, Arturo Diaz-Perez, and Miguel Morales-Sandoval. "Lightweight elliptic curve cryptography accelerator for internet of things applications." *Ad Hoc Networks* 103 (2020): 102159.
[21] J. J. P. C. Rodrigues *et al*., "Enabling Technologies for the Internet of Health Things," in *IEEE Access*, vol. 6, pp. 13129-13141, 2018, doi: 10.1109/ACCESS.2017.2789329.
[22] A.M. Khairuddin, K.N.F.K. Azir and P.E. Kan, “Limitations and future of electrocardiography devices: A review and the perspective from the Internet of Things”. International Conference on Research and Innovation in Information Systems, pp. 1-7, 2017.
[23] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?" in *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41-49, Sept. 2018, doi: 10.1109/MSP.2018.2825478.
[24] A. Banafa, ‘‘Three major challenges facing IoT,’’ IEEE IoT Newslett., Mar. 2017. [Online]. Available: https://iot.ieee.org/newsletter/march2017/three-major-challenges-facing-iot.html
[25] W. Feng, Y. Qin, S. Zhao, and D. Feng, ‘‘AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS,’’ Comput. Netw., vol. 134, pp. 167–182, Apr. 2018.
[26] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, ‘‘A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues,’’ J. Netw. Comput. Appl., vol. 58, pp. 73–93, Dec. 2015.
[27] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, ‘‘Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions,’’ J. Ambient Intell. Hum. Comput., vol. 4, pp. 1–18, May 2017
[28] W. Stallings. (2017). Book: Cryptography and Network Security: Principles and Practice. [Online].
[29] I. Bhardwaj, A. Kumar, and M. Bansal, ‘‘A review on lightweight cryptography algorithms for data security and authentication in IoTs,’’ in Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC), Sep. 2017, pp. 504–509.
[30] Uppu, R., Wolterink, T. A., Goorden, S. A., Chen, B., Škorić, B., Mosk, A. P., & Pinkse, P. W. (2019). Asymmetric cryptography with physical unclonable keys. *Quantum Science and Technology*, *4*(4), 045011.

[31] Amit Kumar Tyagi, Aswathy S U, G Aghila, N Sreenath "AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology" IJIN, Volume 2, Pages 175-183, October 2021.

[32] M. N. M. Bhutta *et al*., "A Survey on Blockchain Technology: Evolution, Architecture and Security," in *IEEE Access*, vol. 9, pp. 61048-61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[33] M. R. Naqvi, M. Aslam, M. W. Iqbal, S. Khuram Shahzad, M. Malik and M. U. Tahir, "Study of Block Chain and its Impact on Internet of Health Things (IoHT):Challenges and Opportunities," *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020, pp. 1-6, doi: 10.1109/HORA49412.2020.9152846.

[34] Sharma, A., Kaur, S., & Singh, M. (2021). *A comprehensive review on blockchain and Internet of Things in healthcare. Transactions on Emerging Telecommunications Technologies.* doi:10.1002/ett.4333

[35] Singh, L. D., & Singh, K. M. (2015). *Implementation of Text Encryption using Elliptic Curve Cryptography. Procedia Computer Science, 54, 73–82.*

[36] Gueron, S., Krasnov, V. Fast prime field elliptic-curve cryptography with 256-bit primes. *J Cryptogr Eng* **5,** 141–151 (2015). https://doi.org/10.1007/s13389-014-0090-x

[37] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Inform. Theory, IT-22 :644-654, Nov 1976.

[38] A. M. Johnston, P. S. Gemmell, "Authenticated key exchange Provably Secure Against the Man-in-Middle Attack", Journal of Cryptology, Springer, 2002, Vol. 15 Number 2 pages 139-148.

[39] N. Mehibel and M. Hamadouche, "A new approach of elliptic curve Diffie-Hellman key exchange," *2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B)*, 2017, pp. 1-6, doi: 10.1109/ICEE-B.2017.8192159.

[40] Chandel S., Cao W., Sun Z., Yang J., Zhang B., Ni TY. (2020) A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption. In: Arai K., Bhatia R. (eds) Advances in Information and Communication. FICC 2019. Lecture Notes in Networks and Systems, vol 70. Springer, Cham. https://doi.org/10.1007/978-3-030-12385-7_67.

[41] Dhanda, S.S., Singh, B. & Jindal, P. Lightweight Cryptography: A Solution to Secure IoT. *Wireless Pers Commun* **112,** 1947–1980 (2020).

[42] Singh, S., Sharma, P.K., Moon, S.Y. *et al.* Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *J Ambient Intell Human Comput* (2017).

[43] Tibrewal I., Srivastava M., Tyagi A.K. (2022) Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore.

[44] Tyagi, Amit Kumar; Nair, Meghna Manoj; Niladhuri, Sreenath; Abraham, Ajith, "Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead", Journal of Information Assurance & Security. 2020, Vol. 15 Issue 1, p1-16. 16p.

[45] Madhav A.V.S., Tyagi A.K. (2022) The World with Future Technologies (Post-COVID-19): Open Issues, Challenges, and the Road Ahead. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_22