An Efficient Security Enhancement in Wireless Technologies for IoT with Hybrid Approach

Viral H. Panchal[1,*], Bhavesh K. Patel[1], and Nikita V. Panchal[2]

[1]Chhotubhai Gopalbhai Patel Institute of Technology, Uka Tarsadia University, Bardoli, Gujarat, India
[2]Vidyabharti Trust College of Business, Computer Science & Research, Bardoli, Gujarat, India
Email: viralpanchal31@gmail.com (V.H.P.); bhavesh.kpatel@utu.ac.in (B.K.P.); panchalnikita01@gmail.com (N.V.P.)
[*]Corresponding author
Manuscript received May 12, 2023; revised July 23, 2023; accepted October 12, 2023; published January 23, 2024

***Abstract*—In recent times, IoT security has gained significant attention due to continuous technological advancements. Numerous studies have been dedicated to enhancing IoT system security. This research seeks to contribute to this field by introducing an innovative approach to bolster the security of IoT Wireless Technologies. We propose the utilization of a hybrid cryptographic method to address the challenges associated with relying solely on a single cryptographic algorithm to meet all security requirements. Our research specifically focuses on overcoming the limitations of single cryptography techniques by combining various cryptographic approaches. As a result, we introduce the concept of a Hybrid Lightweight Cryptographic Approach (HLCA), which combines lightweight symmetric and asymmetric encryption algorithms. This approach aims to enhance security in wireless technologies for IoT systems.**

***Keywords*—security, Internet of Things (IoT), encryption, decryption, cryptography**

I. Introduction

IoT is an interlinked web of innumerable devices and day-to-day things that are equipped with a stupendous intelligence level for making daily living much simpler and advanced [1, 2]. It is a network employed by wireless sensor links through wireless technology and wireless network for achieving complete perception of data, intelligent processing and reliable transmission or communication. In IoT, multiple components are connected via a single network. Here ordinary units are programmed with intelligence for interacting and sensing interlinked devices via an internet [3]. Because of IoT, internet usage has enhanced to a huge level. The ground cause behind immense exploitation of the IoT paradigm is owing to swift progression in sensor technology, wireless gadgets, remote communication, and embedded frameworks. IoTs are exploited in multifarious applications including smart healthcare, smart transportation, smart homes, smart cities, smart wearables, smart farming, smart devices, etc. Through IoT technology, data can be captured, processed, and stored. Additionally, service visualization, monitoring and various device management could also be attained. However, information exchange features from device to device located universally has considerably augmented the security and complexity in IoT [4]. Moreover, sharing of colossal valuable information via an IoT platform has increased diverse security hurdles. IoT systems often are attack-prone owing to

- the dearth of intelligent or supervisory mechanisms for spotting attackers,
- easier snooping because of wireless channel usage and
- utilization of algorithms with minimal computational capability and energy consumption, compromising security aspects.

Most of the time, design of efficient protection algorithms for IoT concentrating vastly on memory usage, energy consumption, power utilization, resource consumption, system complexity mitigation and computation interval reduction has extensively led to safety compromisation in IoT, thereby opening broad pathways for vicious threats and deadly attackers. Thus, security assaults in IoT have been augmented, creating a tremendous necessity for security amelioration of wireless technologies involved and other devices in IoT for completely and effectively ensuring smooth, reliable and safer IoT network operation.

II. Literature Review

Several studies are carried out and diverse methods are proposed for maintaining IoT security in literature. In this section various security techniques employed in existing works are investigated.

Narang *et al*. [5] discussed the distinct security menaces and challenges in IoT. This work employed a combined encryption technique exploiting asymmetric and symmetric methods for securing IoT networks. It performed key creation, encryption, and decryption rapidly and offered acceptable security. Additionally, it utilized less memory owing to minimal fiscal complexity.

Izza *et al*. [6] proposed a safe authentication protocol through combining digital signature and encryption methods. The protocol resisted diverse attacks and offered reliable security.

Singh *et al*. [7] discussed several lightweight encryption schemes for IoT components. The study presented a security structure for constrained resource IoT environments. A scenario-based security technique for maintaining security in resource-restricted IoT applications was provided. The scenario-based security technique provided better protection along with less resource and computational overhead performance.

Naoui *et al*. [8] presented a security solution for IoT loraWAN structure. The confidential information was encrypted using corresponding keys for ensuring confidentiality. It employed a reputation mechanism for selecting trustworthy nodes as assistants for certain heavy cryptographic operations. The protocol employed the AES128 key for safeguarding communication between

doi: 10.18178/ijfcc.2024.13.1.610

gateways and end-nodes. The messages interchanged between the nodes were secured through public keys of nodes. It ensured authenticity, safeguarded the communication and provided robustness against attacks.

Henriques and Vernekar [9] 2017 employed asymmetric and symmetric cryptography methods for protecting communication amongst diverse gadgets in IoT. The integration of asymmetric with symmetric techniques greatly minimized the encryption duration compared to exploitation of asymmetric methods alone. Moreover, exploitation of arbitrary keys particularly in case of symmetric encryption solved the session-key distribution issue. Additionally, it strengthened the encryption technique.

Chandu *et al*. [10] exploited hybrid encryption approach for safeguarding IoT information security. An advanced encryption standard (AES) method was exploited for encoding the data generated. The AES key was encoded using Rivest Shamir Adleman (RSA) method. The encrypted RSA key was shared with the legitimate person through electronic mail. This approach proved to be attack-proof and secure for many scenarios.

Elhoseny *et al.* [11] employed a cryptographic encryption with hybrid optimization methodology for securing clinical images in IoT settings. The encryption/decryption procedure's security level was enhanced through optimal key selection using particle swarm optimization and grasshopper optimization approaches. This approach consumed less time for encryption/decryption procedure and offered elevated security.

Kumar *et al*. [12] employed a combined cryptographic scheme for IoT. The authors exploited DES and RSA techniques for offering elevated information security. This hybrid approach offered greater security compared to techniques when exploited alone.

Ragab *et al.* [13] proposed a combined cryptosystem for safeguarding IoT devices. The combined cryptosystem exploited asymmetric encryption schemes like ECC and RSA and symmetric encryption techniques like XXTEA, XTEA and TEA. It employed chaotic theory for generating arbitrary keys. Results illustrated that the presented cryptosystem combining XXTEA and ECC offered higher performance and security than XXTEA and RSA.

Kumar *et al*. [14] presented a combined cryptosystem through integrating rail fences and AES for enhancing security in several applications like protecting account passwords, protecting messages comprising secret data, etc. This combined cryptosystem ensured confidentiality and outperformed the classical encryption schemes.

Yousefi and Jameii [15] provided a combined encryption approach for reducing safety menaces and boosting IoT security. This hybrid technique aimed at maintaining non-repudiation, confidentiality and integrity during information interchange in IoT. The developed technique offered rapid key creation, decryption, encryption and reasonable security.

Kalyani and Chaudhari [16] augmented security authentication in IoT through exploiting cryptographic-directed methodologies. The IoT sensitive information was secured through improved homomorphic encryption (IHE) approach. This approach initially categorized the confidential information from the IoT database. Then that confidential information was encrypted and decrypted using IHE. After key authentication while encryption the best key selection was accomplished through optimized fire-fly scheme. The presented approach displayed elevated security with decremented computational time.

Mabodi *et al.* [17] described a multi-stage trust-oriented intelligence approach for guarding IoT against threats. It adopted a cryptographic authentication mechanism involving four stages namely IoT trust node validation, route testing, gray hole intrusion investigation and vicious attack elimination procedure. This approach offered minimal false positive score, minimal false negative score, elevated security and elevated detection rate.

Safi [18] exploited NTRU asymmetric and AES symmetric encoding approaches for incrementing IoT security. It offered security because of multinomial utilization in digital signature, decryption and encryption for attaining a right message. Additionally, it used less memory owing to minimal fiscal complexity. Moreover, it augmented IoT security.

Mbarek *et al*. [19] proposed a neoteric authentication protocol for offering an efficient and safe transaction in IoT networks. A mutual and self-adaptive key updation based authentication approach was presented. The factors namely energy consumption, authentication delay and authentication breakdown rate were also evaluated. Through exploiting dynamic key upgrading methods, the presented solution enhanced the key upgrading system by enabling distinct ways of authenticating keys, thereby significantly diminishing the sequence of different jamming attacks. The approach rendered elevated security and outperformed the similar existing authentication protocol in authentication breakdown rate and energy usage.

AlMajed and AlMogren [20] adopted elliptic curve cryptography (ECC) approach for protecting IoT. It considered analysis and evaluation of security requisites for particular encryption attributes. This scheme safeguarded the encoding operation against different encryption attacks and malleability intrusions.

III. Problem Statement

IoT being a swiftly evolving paradigm has drawn colossal attention among researchers and industrial experts. IoT has revolutionized the interacting ways of organizations and individuals with the natural world. For practical IoT realization, development of multifarious neoteric versions of technologies and platforms including process and device tracking, identification, sensing, actuation, computational sensing, communication, distributed and coordinated control, user modelling and acceptable knowledge processing techniques are richly needed along with consideration of device lifetime, energy, power use and cost constraints. Nevertheless, amongst all these requisites, the leading, most desired and challenging requisite is deemed to be security. It could be extensively affirmed that the vicious attack chances would be hugely actuated and expanded to the natural world from the internet. Therefore, IoT security is of utmost importance and mandatory.

In most IoT applications, wireless technologies like wireless fidelity, radio-frequency identification (RFID), ZigBee, Bluetooth, Backfi, RuBee, Wavenis etc. are

exploited for communication functions. However, securing IoT links completely is impossible without safeguarding IoT's wireless infrastructures or components that exploit these technologies. Often wireless IoT structures which exploit these wireless technologies are hugely resource-restrained and thus are liable to diverse harmful intrusions. Generally, the wireless structure of IoT is an extremely vulnerable section of IoT. Thus, there are the probabilities of attackers exploiting this section as a prime gateway or entrance door for establishing their attacking network.

Many existing and baseline research studies on IoT security have not devoted much attention towards securing their associated wireless technologies, thereby leading to poor security, variety of hazardous attacks and privacy breaching of users. The security compromisation has opened new pathways for attackers, vicious users and cyber-attacks making existing authentication and safety algorithms redundant in guarding the modern IoT systems. This has in turn necessitated the proposal and implementation of ameliorated security algorithms through combining attractive security attributes. This research intends to consider security enhancements in wireless technologies linked with IoT structures through developing hybrid security approaches for protecting IoT links from diverse vicious attacks. Moreover, a performance assessment for comparing the security enhancement impact of hybrid approach on power utilization, energy efficiency, memory and resource usage over competing security algorithms will be conducted.

IV. Research Gaps

Security plays a leading part in any system's reliable and uninterrupted operation. IoT being a massive and interconnected mesh of countless devices with certain intelligence levels has gained prevalent significance. However, the interconnectivity of networks in IoT has vastly introduced security susceptibilities and trust issues.

Existing security methods often face hurdles in managing IoT security along with considering computational and resource minimization aspects. Many of them end up with security compromisation while attempting to diminish the security algorithm's computational complexity.

Compromisation of authentication in most instances leads to compromisation of other security services like availability, integrity, and confidentiality. Also, utilization of single and classical cryptographic methods with inferior encryption/decryption operations in many IoT networks has largely led to weaker security creating high possibilities for multiple and unpredictable malicious attacks. Additionally, these methods have not concentrated on securing diverse communicating infrastructures involved with IoT networks.

This research concentrates on addressing the afore-discussed barriers through achieving security enhancement in wireless technologies by developing hybrid security algorithms for protecting IoT systems.

V. Research Objectives

The preliminary aim of the proposed research is to enhance the security in wireless technologies for IoT systems. The proposed research objectives are listed in the points below:

- To design an efficient security system for IoT based wireless technologies.
- To address the security challenges such as authenticity, confidentiality, integrity, privacy of the IoT data which are the major concerns in a dynamic IoT network.
- To achieve high efficiency, scalability, and bandwidth utilization by addressing node mobility issues.
- To reduce energy consumption and improve fault tolerance of the proposed security enhancement approach.
- To propose a context-aware approach which can effectively deal with the dynamic environment of the IoT networks.

VI. Proposed Research Methodology

This research aims to enhance the security in wireless technologies for IoT systems using a hybrid cryptographic approach. Due to the resource constraint nature of IoT devices, it is difficult to design a secure cryptographic approach which is suitable in all IoT environments. In this context, this research proposes a hybrid lightweight cryptographic algorithm (HLCA) which is the combination of lightweight symmetry, and asymmetric encryption algorithms for improving security in wireless technologies. It can be inferred from existing works that lightweight symmetric and asymmetric algorithms improve the integrity, privacy, reliability, and confidentiality of IoT data with small key size (Singh & Sharma, [7] 2017). They require very less computation power and memory space.

However, in cryptographic techniques, it is difficult to achieve all security requirements using a single cryptographic algorithm. For example, symmetric encryption approaches provide simple and secure data transmission with high security. However, their efficiency while sharing secret keys is not effective. Whereas asymmetric encryption overcomes this problem, they are slow and require more resources for computation. On the other hand, hashing techniques provide a unique yet robust signature-based security to maintain data integrity. However, they are not effective when used as a single approach. To overcome the limitations associated with single cryptography techniques, this research intends to combine different cryptographic approaches and hence proposes a hybridized approach. The proposed hybrid (HLCA) approach combines a symmetric block cipher known as QARMA encryption, an asymmetric Elliptic Curve Digital Signature Algorithm (ECDSA), and a BLAKE2 based hashing technique.

Using these techniques together, the proposed approach aims to preserve the data privacy, security, and anonymity of user's data.

A. Proposed HLCA for Security Enhancement

Wireless technologies such as radio-frequency identification (RFID), ZigBee, and Bluetooth are sensitive to security attacks because of their diverse nature of the data transmission network. Also, these technologies have limited energy and processing ability for sensor nodes which makes it quite difficult to adopt an effective security approach for these technologies.

The proposed HLCA is a hybridized approach which combines three different encryption techniques which aims to

overcome the challenges faced by conventional approaches. QARMA encryption is a symmetric lightweight block cipher algorithm used mainly for memory encryption and for software security. ECDSA is an asymmetric encryption approach which is based on the digital signature algorithm DSA. The ECDSA uses an ECC (elliptic curve cryptography) based mathematical approach for key generation which is appropriate for security encryption. The BLAKE2 hashing is a cryptographic hash function which is selected because of its superior attributes such as high speed, security, and simplicity. The implementation of the proposed approach will consist of the following stages:

Step1- Key generation: Initially, the sensitive IoT data will be encrypted securely using a QARMA-128 block cipher technique. The encryption will be done by encoding the data using public keys. This technique can generate encrypted keys and can provide the highest security in the IoT environment.

Step 2: Key authentication: In this stage, the generated keys will be authenticated by generating an authentication certificate. This certificate will be used for authentication of the data transmission process. In this step, the certificate is provided for the generated key for establishing the trust relationship between the sender and the receiver. The certificate will be generated using the ECDSA approach which ensures the encryption of the certificate data. The generation of the authentication certificate will enhance the effectiveness of the cryptographic process and also enhance the stability of the system to withstand attacks and secure the data transmission process in wireless devices.

Step 3: Data Encryption, Transmission and Decryption: In this step, the proposed HLCA algorithm will ensure that the data is not altered by any unauthorized user. The data obtained from wireless technologies are subjected for double encryption using the QARMA-128 block cipher and the ECDSA. Here double encryption means that initially the data will be encrypted using a symmetric key encryption QARMA-128 and then the symmetric key itself will be encrypted using a public key. The ECDSA will ensure that only authenticated keys are used for encryption I.e., keys which are provided with an authentication certificate. Furthermore, Since the data will be encrypted using both public keys and asymmetric keys, it is essential to prevent the access of any unauthorized entities to the public keys. In this case, the proposed lightweight hashing technique BLAKE2 will be used for hashing the key data which will allow only authorized users to access the key information and thereby protects the security of the data.

VII. Conclusion

This paper addresses the shortcomings of current security methods applied to wireless technologies within IoT environments. Additionally, we examine various existing hybrid encryption/decryption techniques utilized in securing IoT devices. Our contribution involves the introduction of a hybrid lightweight cryptographic approach (HLCA) aimed at bolstering security in wireless technologies for IoT systems. The HLCA approach integrates lightweight symmetric and asymmetric encryption algorithms, effectively fulfilling all research objectives while showcasing exceptional performance in terms of data privacy, integrity, scalability, security, latency, and throughput.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Mr. Viral H. Panchal, the first author, conducted an analysis of existing security research, summarizing its limitations and writing the paper. Mr. Bhavesh K. Patel, the second author, focused on highlighting the advantages of the existing work and identifying open research issues. Ms. Nikita V. Panchal, the third author, performed a thorough check of the paper; all authors had approved the final version.

References

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[2] P. V. Dudhe, N. V. Kadam, R. M. Hushangabade, and M. S. Deshmukh, "Internet of things (IoT): An overview and its applications," in *Proc. 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing*, pp. 2650–2653, 2017.

[3] M. A. Sadeeq, S. R. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of things security: A survey," in *Proc.* 2018 *International Conference on Advanced Science and Engineering (ICOASE)*, pp. 162–166, 2018.

[4] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, pp. 8–27, 2018.

[5] S. Narang, T. Nalwa, T. Choudhury, and N. Kashyap, "An efficient method for security measurement in internet of things," in *Proc. 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, pp. 319–323, 2018.

[6] S. Izza, M. Benssalah, and K. Drouiche, "An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment," *Journal of Information Security and Applications*, vol. 58, p. 102705, 2021.

[7] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2017.

[8] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Enhancing the security of the IoT LoraWAN architecture," in *Proc. 2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, pp. 1–7, 2016.

[9] M. S. Henriques and N. K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in IoT," in *Proc.* 2017 *International Conference on IoT and Application (ICIOT)*, pp. 1–4, 2017.

[10] Y. Chandu *et al*., "Design and implementation of hybrid encryption for security of IOT data," in *Proc. 2017 International Conference on Smart Technologies for smart NATION (SmartTechCon)*, pp. 1228–1231, 2017.

[11] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, and A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in internet of things," *Neural Computing and Applications*, vol. 32, no. 15, 2020.

[12] A. Kumar, V. Jain, and A. Yadav, "A new approach for security in cloud data storage for IoT applications using hybrid cryptography technique," in *Proc.* 2020 *International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, pp. 514–517, 2020.

[13] A. Ragab, G. Selim, A. Wahdan, and A. Madani, "Robust hybrid lightweight cryptosystem for protecting IoT smart devices," in *Proc. International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pp. 5–19, 2020.

[14] M. T. Kumar *et al.*, "A hybrid approach for enhancing security in internet of things (IoT)," in *Proc. 2019 International Conference on Intelligent Sustainable Systems*, pp. 110–114, 2019.

[15] A. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," in *Proc. 2017 International Conference on IoT and Application (ICIOT)*, pp. 1–5, 2017.

[16] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in Internet of Things using the optimum authentication key," *International Journal of Computers and Applications*, vol. 42, no. 3, pp. 306–314, 2020.
[17] K. Mabodi *et al*., "Multi-level trust- based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," *The Journal of Supercomputing*, pp. 1–26, 2020.
[18] A. Safi, (2017). Improving the security of internet of things using encryption algorithms. *International Journal of Computer and Information Engineering*, vol. 11, no. 5, pp. 558–561, 2017.
[19] B. Mbarek, M. Ge, and T. Pitner, "An efficient mutual authentication scheme for internet of things," *Internet of Things*, vol. 9, 2020.
[20] H. AlMajed and A. AlMogren, "A secure and efficient ECC-based scheme for edge computing and internet of things," *Sensors*, vol. 20, no. 21, 2020.

\