SECURE AND LIGHTWEIGHT DATA SHARING MECHANISM FOR MEDICAL IoT

Tarun Sai Yakkala, Sri Krishna Kumar Modekurty, Neeraj Boggarapu, Amit Kr Mandal
Department of Computer Science and Engineering
SRM University AP, Amaravathi, India
yakkala_tarun@srmap.edu.in, modekurty_sri@srmap.edu.in, boggarapu_venkata@srmap.edu.in, amitmandal.nitdgp@gmail.com

Abstract—**The healthcare sector has engaged in substantial research in terms of technological advancement to provide patients with efficient and secure services. With the adaption of the internet of things (IoT) in the healthcare domain, remote patients are now able to share their health records with medical experts at distant locations, leading to more efficient and less expensive services. Given that data sharing over the internet entails the patients' privacy, therefore, it is necessary to ensure that data is transmitted securely so that an adversary cannot tamper with it. Again, as IoT devices are resource-constrained, therefore, it is very important to transmit the data in a lighter format. This paper presents a mechanism for the communication of data or images over the network in a secure and lighter format. The proposed mechanism is implemented on Modified Chebyshev Polynomial and suitable data and image compression techniques with minimum distortion.**

Index Terms—**Internet of Things (IoT) , IoT in healthcare , Modified Chebyshev Polynomial, Data Compression, Image Compression, Half duplex communication.**

I. Introduction

Internet of Things (IoT) is a network of physical objects that are fused with sensors, applications, and other technology to communicate and share data with different devices and systems over the web. The use of IoT in healthcare has provided significant benefits to both patients and medical practitioners, such as maintaining track of a patient's health state and, if necessary, offering telemedicine. The introduction of IoT in the field of medical sciences has become a pivotal step in the development of a productive healthcare system [17], [18].

In recent decades, technology's horizon has widened to the point where many interdisciplinary sectors have emerged, such as a merger of medical sciences and IoT. Sensitive information such as heartbeat readings, pulse readings, electrocardiogram (ECG) readings, and so on would be captured and transmitted in an IoT-based healthcare system. Devising a secure environment is critical in order to ensure that data is not compromised and that the patient's life is not imperiled [16], [17]. Therefore, in a medical-IoT network, the most critical considerations are security and privacy where users authenticate themselves by transmitting messages to sensors and Fog devices [2]. For this purpose, the users or sensors must be registered with the network before they can authenticate themselves, and authentication occurs during the login process. Since multiple communications occur among components during registration, login, and authentication, data protection must be ensured [7].

Again, with the rapid advancement of technology and increasing adaption of medical IoT devices, the volume of health data generated and transmitted is also increasing. In medical IoT, the data that is being captured can be of a variety of formats like streams, high-resolution images, graphs, charts, tables, etc [5]. With limited power, processing power, and memory it is very difficult for IoT devices to transmit a large chunk of data over a network by ensuring its security and privacy. Therefore, a suitable data compression technique is required that not only reduces the size of the data but also retains the quality of the data [5]. This will play a crucial role in the secure transmission of data over the network by consuming minimal energy.

To address these issues in this paper we proposed a Chebyshev polynomial-based secure and lightweight authentication algorithm. The devised authentication mechanism establishes a secure session key between the device and gateway. The established session key is then used to encrypt the data transmission between the device and gateway. Further, medical things can transmit textual and image data to the gateway. Therefore, to minimize the energy consumption of the IoT devices while transmitting the textual data a data compression mechanism based on a combination of LZ77 [25] and Huffman Coding is implemented to reduce the size of the transmitted textual data. Similarly, for the images, the PIL compression mechanism is implemented. The experimental results show that the protocol requires significantly less time to complete the handshake duration. Again, the incorporation of data and image compression mechanism while securely transferring the data reduces the energy consumption significantly while preserving the quality of the transmitted data.

The outline of this paper is as follows: in section II, a brief discussion on the previous research works in the domain of IoT and IoT in healthcare is presented, which is being followed by the proposed model for secure and lightweight data transmission in medical-IoT network in section III. The results and analysis of the proposed model are discussed in section IV. Section V concludes the manuscript.

II. RELATED WORK

In light of the recent pandemic scenario, a paradigm for telemonitoring in a cloud-based IoT environment has been proposed. The suggested model utilizes a lightweight block encryption scheme to protect patients' sensitive health data. On the basis of chaos-based encryption, a cryptosystem to safeguard patients' confidentiality has been postulated [23], [24].

A lightweight technique based on elliptic curve cryptography (ECC), XOR operations and hash function was presented to ensure patient confidentiality and access control of shared medical data [17]. Another method, based on enhanced elliptic curve encryption (ECC), was developed to facilitate end-to-end authentication for wireless body area networks (WBAN) [18].

A two factor – authentication protocol had been proposed based on the temporal credential for wireless sensor networks (WSNs). As time passed by, it was found that the authentication phase of the protocol had many security perils. Later a progressive development was made to the existing protocol by developing an untraceable temporal-credential-based two-factor authentication protocol based on ECC for wireless sensor networks. It was also proved that the advanced version of the protocol had satisfied the mutual authentication in the Burrows-Abadi-Needham (BAN) logic. Though it was an enhanced version, it also had a few drawbacks like not being able to resist the impersonation attack from a malicious user and sensor node capturing attack [7], [8], [12].

A scheme was proposed based on a level 3 feature extraction, fuzzy extraction of the user's biometrics, one-way hash functions and XOR operations. The scheme also includes three-factor, mutual authentication, a session key and key freshness. The developed authentication protocol has used the BAN logic to prove the authentication has sustained [1], [3], [4].

Two techniques have been implemented to secure the system from possible attacks by using authentication server and cryptography techniques [2]. Here the client has to traverse through three verification modules to reach the real server. The real server is embedded with the Elgamal security model, whose work is to provide End to End security with semantic principle and advanced cryptography technique. Further by integrating these two models, the result is supporting the successful security system against the malicious authentication trial and eavesdropping [10].

A data compression scheme has been proposed based on Huffman Coding. The proposed scheme comprises mechanisms for finding a definite pattern and reinstate the pattern with a variable length identifier to reduce the amount of space required for the transmission of data [5], [13]. A data compression scheme has been proposed incorporating both lossy and lossless mechanisms. The data is first compressed with a high compression ratio lossy compression technique (CR). With the help of entropy coding, the residual error between the original data and the decompressed lossy data is retained, thus allowing for lossless recovery of the original data when necessary [11].

A set of data compression techniques has been proposed that minimizes the size of the data while preserving the quality of the data. The proposed scheme has been implemented on the integration of Delta and RLE compression mechanisms [14].

A methodology was proposed for an effective controlling of energy consumption and compression rate for a cloud-based IoT network. The cited approach was based on an adaptive data compression scheme consisting of a sequential lossless entropy compression (S-LEC) scheme and the sensor Lempel-Ziv-Welch (S-LZW) scheme. Mixed-integer linear programming has been used to develop the proposed technique [6], [13].

III. PROPOSED MODEL

In the era of digitization, information would get communicated between the communicating entities over the internet. The communication medium should be secure so that the information would not get hindered. Suppose, if the transmit channel gets compromised in terms of security, then there is a chance of the information getting tampered by a malicious intruder.

The proposed model in this paper is intended for IoT in healthcare. The proposed scheme is intended towards establishing and maintaining a secure and lightweight communication channel among the communicating entities, namely: Smart healthcare devices and Edge or Fog Devices. There are three phases in the devised mechanism, namely: Registration, Authentication, and Data Compression.

A. *Registration*

Registration is the first phase among the mentioned three phases of the model, as shown in Figure 1. In this phase, if a new smart healthcare device wants to communicate with Edge or Fog devices, it should first register its device identification and password. The device ID number(D_i) and password (Pw_i) requires every time it wants to get connected to the IoT network. The device ID number and a random large number R_i, the password and the current timestamp (t) are then subjected to a series of XOR operations.

$$PID_i = D_i \oplus R_i$$
$$PIN_i = Pw_i \oplus t$$

The XORed output PID_i and PIN_i is sent towards the other end. On receiving the output at the Edge or Fog devices end, two random large numbers S and P and a random point x are chosen.

$$T_p(x) = (2xT_{p-1}(x) - T_{p-2}(x))\%K \tag{1}$$

where $T_0(x) = 1\%K$ and $T_1(x) = x\%K$. The value of p is a large prime number, K is a large integer and $x \in [-\infty, \infty]$

Next, the calculation of $T_s(x)$ is performed which is based on the modified Chebyshev polynomial, as stated in equation 1. A combination and a series of XOR and hash operations

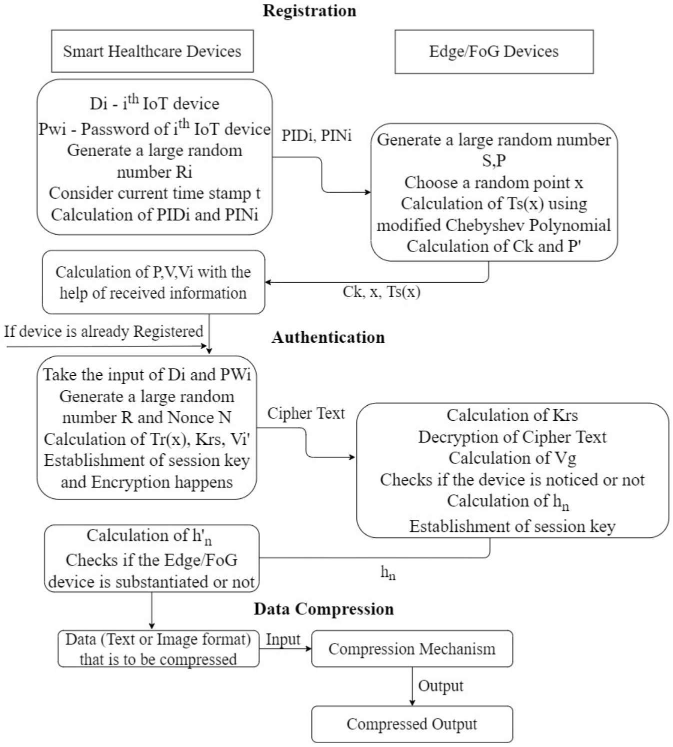
Registration
Smart Healthcare Devices
Edge/FoG Devices
Di - ith IoT device
Pwi - Password of ith IoT device
Generate a large random number Ri
Consider current time stamp t
Calculation of PIDi and PINi
PIDi, PINi
Generate a large random number S,P
Choose a random point x
Calculation of Ts(x) using modified Chebyshev Polynomial
Calculation of Ck and P'
Calculation of P,V,Vi with the help of received information
Ck, x, Ts(x)
If device is already Registered
Authentication
Take the input of Di and PWi
Generate a large random number R and Nonce N
Calculation of Tr(x), Krs, Vi'
Establishment of session key and Encryption happens
Cipher Text
Calculation of Krs
Decryption of Cipher Text
Calculation of Vg
Checks if the device is noticed or not
Calculation of h$_n$
Establishment of session key
Calculation of h'$_n$
Checks if the Edge/FoG device is substantiated or not
h$_n$
Data Compression
Data (Text or Image format) that is to be compressed
Input
Compression Mechanism
Output
Compressed Output

Fig. 1. Proposed Model

are performed among P and the transmitted outputs and the final result is assigned to a variable called a C_k.

$$P' = P \oplus PID_i$$
$$C_k = H(PIN_i \parallel PID_i) \oplus P'$$

The values of $C_k, x, T_s(x)$ are transmitted back to the smart healthcare device end. Once the values are transmitted, a combination and a series of XOR and hash operations are performed among C_k, device ID number, password, P, $T_s(x)$ and the final result is assigned to a variable called the V_i.

$$P = C_k \oplus H(PIN_i \parallel PID_i) \oplus PID_i$$
$$V = P \oplus T_s(x)$$
$$V_i = V \oplus H(D_i \parallel Pw_i)$$

The total computation cost is $8T_{XOR} + 3T_H + 1T_{CP}$, where T_{XOR} stands for XOR operation , T_H stands for Hash operation and T_{CP} stands for modified Chebyshev polynomial operation.

At the end of registration, the $P, x, T_s(x)$, and V_i values are stored.

B. Authentication

The second and the most vital phase of the proposed model is Authentication, as depicted in Fig. 1. This phase aims at establishing a secure connection among the communication entities. In this phase, an input of device ID number(D_i) and password (Pw_i) are considered at the smart healthcare device end. Two large random numbers are considered by the name R and nonce N. Next, the values of $T_r(x)$ and K_{rs} are computed using the modified Chebyshev polynomial, as stated in equation 1. An XOR operation is performed between the V_i and hash output of the device ID number and password and the value is assigned to V_i'.

$$V_i' = V_i \oplus H(D_i \parallel Pw_i)$$

Next, the session key is established. Later, a process of encryption happens and the cipher text is transmitted to the other end.

$$SessionKey = H(N \parallel K_{rs})$$
$$Encryption(e) = E(K_{rs}, \{V_i \parallel N\})$$

On the Edge or Fog device end, the value of K_{rs} is computed using the modified Chebyshev polynomial, as stated in equation 1, followed by the process of decryption.

$$Decryption = D(K_{rs}, e)$$

Next, an XOR operation is performed between P and $T_s(x)$. Next, it is ensured that the smart healthcare device is notified by the Edge or Fog device followed by the establishment of a session key at the Edge or Fog device end.

$$V_g = P \oplus T_s(x)$$
$$SessionKey = H(N \parallel K_{rs})$$

The hash value of N is computed and transmitted to the smart healthcare end to make sure that the Edge or Fog device is also verified by the smart healthcare device, by comparing the transmitted hash value with the computed hash value of N at the smart healthcare device. The total computational cost is $2T_{XOR} + 3T_H + 3T_{CP}$.

C. Data Compression

As depicted in Fig. 1, the Data Compression is the final phase of the devised methodology. This phase ensures that the data either in text format or image format is compressed to ease the computation and reduce the overhead on the resource-constrained devices. In this model, a combination of LZ77 and Huffman Coding is used. LZ77 compresses the text into a sequence of literal letters. The intermediate sequence is then compressed even more by Huffman coding as it would have compressed the same letters in the original data based on the Huffman codes. As a result, this two-step approach produces compressed data in the binary format. This binary format is encoded using utf-8. PIL (Python Imaging Library) was used for image compression.

After successful completion of all the three phases, the compressed data undergoes encryption and the encrypted data (cipher text) would be transmitted from the smart healthcare devices to the Edge or Fog devices and get decrypted and decompressed to retain the original data.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

In a medical IoT network, the process of handshake plays an important role between the interacting entities, namely: Smart Healthcare devices and Edge or Fog devices. The handshake duration is computed until the establishment of the session key. A total of 30 samples are collected, which are divided into three equal sets. A gap of 10 minutes is considered after collecting all the samples of a particular set and the results are depicted in the form of a graph in Figure 2. Standard deviation was ascertained on the collected data samples for more accurate results. The standard deviation of the collected samples is 0.009555169842. The time is represented in terms of seconds(sec).

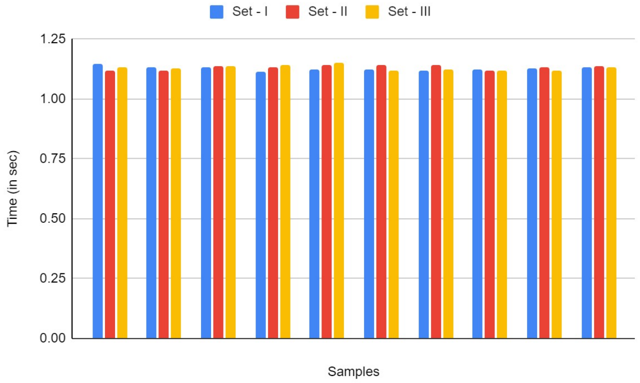

Fig. 2. Handshake Duration

The data is encrypted and decrypted using cryptographic techniques in a cryptosystem. To establish a secure communication connection, cryptographic algorithms are applied. The presented paradigm uses the Advanced Encryption Standard (AES) algorithm. The advantage of AES is its key length variations, which make it a fast and elegant algorithm. The encryption will become exponentially harder to breach as the key length increases. Three different cryptographic algorithms and the corresponding encryption time in seconds(sec) are graphed in Figure 3.

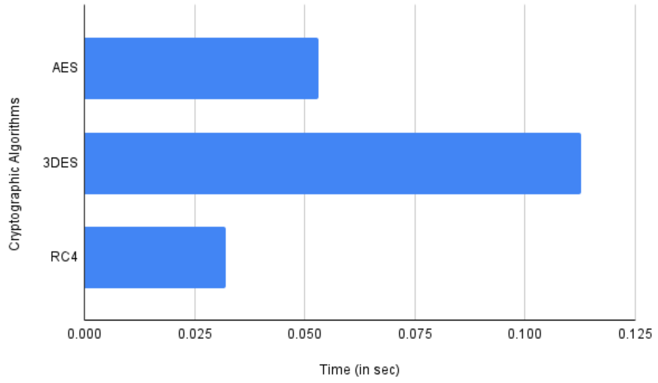

Fig. 3. Cryptographic Algorithms

In the medical field, data can exist in many forms and sizes. As data is exchanged via a network in IoT, there will be a range of extensions for various data formats. During the implementation of the proposed model, text and image data are taken into account. Text files of sizes 404 KB,52 KB and 24 KB are considered for the proposed mechanism. The considered text has undergone a variety of text compression techniques like Huffman Coding, LZW (Lempel–Ziv–Welch), and a combination of Huffman coding and LZ77. The observed results are tabulated in Table I. As per the observed results, the combination of Huffman Coding and LZ77 has shown better results among all the three text compression mechanisms by compressing the text to 127 KB, 14 KB and 12 KB respectively. Due to certain limitations of Huffman Coding, the text was encoded in such a way that instead of compressing, the size of the text got expanded. Similarly, LZW has performed the same way but it's much better than the Huffman Coding.

TABLE I
TEXT COMPRESSION MECHANISMS

Compression Mechanism	Dataset Name	Original Size	Observed Results	Time Complexity
Pure Huffman Coding	Arrhythmia[20]	404KB	1.19MB	O(nlogn)
	Cancer[21]	52KB	272KB	
	Diabetes[22]	24KB	79KB	
Pure LZW	Arrhythmia[20]	404KB	330KB	O(n)
	Cancer[21]	52KB	52KB	
	Diabetes[22]	24KB	34KB	
LZ77 + Huffman Coding	Arrhythmia[20]	404KB	127KB	O(n)
	Cancer[21]	52KB	14KB	
	Diabetes[22]	24KB	12KB	

An image of size 26 KB is considered for the proposed system. Two image compression mechanisms were considered, namely: PIL compression and OpenCV compression. After performing various image quality checks [15], the performance of both the image compression mechanisms was pretty much similar with a little difference leaving the PIL compression mechanism to be more optimal when compared to OpenCV compression. The results are depicted in Table II and Table III, and represented as a graphed in Figure 4.

TABLE II
IMAGE COMPRESSION

S.No	Compression Mechanism	Results Observed
1.	PIL Compression	13 KB
2.	OpenCV Compression	14 KB

TABLE III
IMAGE QUALITY METRICS OF TRANSMITTED MEDICAL IMAGE

Compression Mechanism	Image Quality Metrics			
	PSNR	MSE	RMSE	SSIM
PIL	36.46071705	20.43225826	4.520205555	0.9494908679
OpenCV	36.4106395	20.65387187	4.544653108	0.949293001

It is important to formulate a model or protocol for IoT devices that considers the devices' resource constraints. Thus, it is important to ensure that devised protocols consume less amount of energy [19]. The energy consumption is computed based on equation 2. The computed values of energy consumption are represented in joules per bit(J/bit) and represented in Table IV.

$$E_{Tx}(k,d) = Eelec * k + \epsilon amp * k * d^2, d > 1 \tag{2}$$

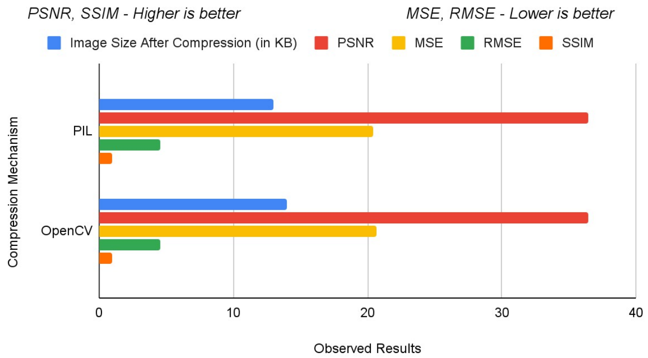

Fig. 4. Image Compression and Quality Metrics

where $E_{Tx}(k,d)$ stands for transmitting data energy consumption, k stands for volume of data in terms of bit, $Eelec$ stands for data transmission's energy consumption in terms of nanojoules per bit (nJ/bit), $\epsilon\ amp$ stands for energy consumption constant and d stands for distance.

TABLE IV
ENERGY CONSUMPTION DURING FILE TRANSMISSION

File Name	Before Compression	After Compression
Arrhythmia[20]	0.1658093568 J\bit	0.0520767456 J\bit
Cancer[21]	0.0213417684 J\bit	0.0056641056 J\bit
Diabetes[22]	0.0098500608 J\bit	0.0046749312 J\bit
Remdesivir Image	0.0103594776 J\bit	0.005166312 J\bit

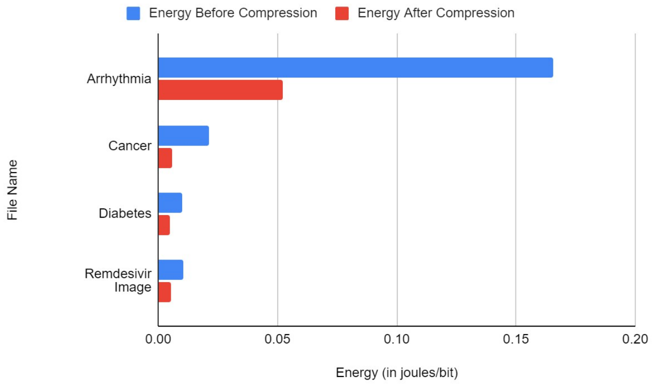

Fig. 5. Energy Consumption

Another prominent evaluation criterion taken into account when assessing the efficiency of the proposed model is the file transmission time. The file transmission time values are obtained while transmitting the files and graphed in Figure 6. It is evident that the lower the file size, the faster the transmission. The time is represented in terms of milliseconds (millisec).

During the execution of the suggested model, the CPU and Memory utilization's were logged and graphed under the name Figure 7. The CPU and memory utilization's peaks are just around 6% and 3%, respectively, as shown in Figure 7. Therefore, from the experimental results it is evident that the proposed methodology capable of establishing a lightweight communication among the IoT devices.

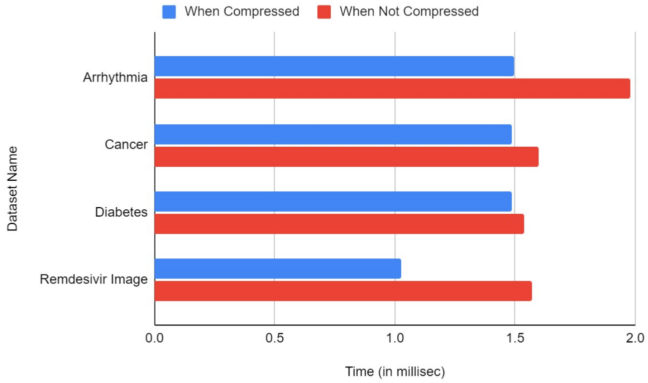

Fig. 6. File Transmission

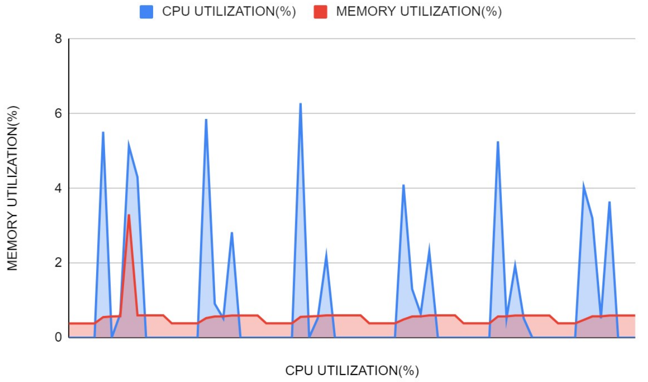

Fig. 7. CPU Utilization VS Memory Utilization

V. CONCLUSION

In today's world, most of the data would get transmitted digitally over a network in a variety of ways like electronic mail, social media messages, etc. In the Internet of Things, it's critical to establish secure communication among communicating entities and to visualize the data optimally to reduce data transmission overhead on resource-constrained devices. In this paper, an attempt has been made to give the reader an insight into a methodology for data communication among the resource-constrained IoT devices which is secure and lightweight. To achieve the goal of secure communication among the communicating devices two phases, namely: registration and authentication were performed in the devised mechanism. The implementation of both the phases was primarily based on the semi-grouping nature of the modified Chebyshev Polynomial. A diversified data compression mechanism had been performed to find an optimal mechanism to ease the computation on the IoT devices. From the results that were obtained, it is evident that the proposed mechanism is suitable for IoT devices for instituting secure and lightweight communication in a medical-IoT environment.

References

[1] B. H. Taher, S. Jiang, A. A. Yassin and H. Lu, ”Low-Overhead Remote User Authentication Protocol for IoT Based on a Fuzzy Extractor and Feature Extraction,” in IEEE Access, vol. 7, pp. 148950-148966, 2019.

[2] El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. Sensors 2019, 19, 1141.

[3] Hao, F. (2014), On robust key agreement based on public key authentication. Security Comm. Networks, 7: 77-87.

[4] Kang D, Jung J, Kim H, Lee Y, Won D. Efficient and secure biometric-based user authenticated key agreement scheme with anonymity. Secur Commun Netw. 2018;2018:1-14.

[5] Chatterjee, R. J. Shah and K. S. Hasan, ”Efficient Data Compression for IoT Devices using Huffman Coding Based Techniques,” 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 5137-5141.

[6] H. M. Al-Kadhim and H. S. Al-Raweshidy, ”Energy Efficient Data Compression in Cloud Based IoT,” in IEEE Sensors Journal, vol. 21, no. 10, pp. 12212-12219, 15 May15, 2021.

[7] Nandy T, Idris MYIB, Md Noor R, et al. Review on security of internet of things authentication mechanism. IEEE Access. 2019;7:151054-151089.

[8] Qi Jiang, Jianfeng Ma, Fushan Wei, Youliang Tian, Jian Shen, Yuanyuan Yang, An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks, Journal of Network and Computer Applications, Volume 76, 2016, Pages 37-48, ISSN 1084-8045.

[9] Saraiva DAF, Leithardt VRQ, de Paula D, Sales Mendes A, González GV, Crocker P. PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices. Sensors (Basel). 2019;19(19):4312. Published 2019 Oct 5.

[10] Sharma, Santosh Kumar and Pataballa, Vishnu Murthy and Boddepalli, Subha Sri, Multilayer Authentication-Crypto for Internet of Things Security using End-to-End Cryptography (2018). International Journal of Advanced Studies of Scientific Research, Vol. 3, No. 11, 2018.

[11] C. J. Deepu, C. -H. Heng and Y. Lian, ”A Hybrid Data Compression Scheme for Power Reduction in Wireless Sensors for IoT,” in IEEE Transactions on Biomedical Circuits and Systems, vol. 11, no. 2, pp. 245-254, April 2017.

[12] Yang S-Y, Xu C-B. Cryptanalysis of an untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. In: Proceedings of the 3rd International Conference on Wireless Communication and Sensor Networks (WCSN 2016). Atlantis Press; 2017:661-665.

[13] S. Hamdan, A. Awaian and S. Almajali, ”Compression Techniques Used in Iot: A Comparitive Study,” 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS), 2019, pp. 1-5.

[14] Hanumanthaiah, A. Gopinath, C. Arun, B. Hariharan and R. Murugan, ”Comparison of Lossless Data Compression Techniques in Low-Cost Low-Power (LCLP) IoT Systems,” 2019 9th International Symposium on Embedded Computing and System Design (ISED), 2019, pp. 1-5.

[15] Samajdar T., Quraishi M.I. (2015) Analysis and Evaluation of Image Quality Metrics. In: Mandal J., Satapathy S., Kumar Sanyal M., Sarkar P., Mukhopadhyay A. (eds) Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, vol 340. Springer, New Delhi

[16] R. R. K. Chaudhary and K. Chatterjee, ”An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System,” 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), 2020, pp. 991-995.

[17] Zhuo Zhao, Chingfang Hsu, Lein Harn, Qing Yang, Lulu Ke, ”Lightweight Privacy-Preserving Data Sharing Scheme for Internet of Medical Things”, Wireless Communications and Mobile Computing, vol. 2021, Article ID 8402138, 13 pages, 2021.

[18] Sowjanya, K., Dasgupta, M. Ray, S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. Int. J. Inf. Secur. 19, 129–146 (2020).

[19] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, ”Energy-efficient communication protocol for wireless microsensor networks,” Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000, pp. 10 pp. vol.2-, doi: 10.1109/HICSS.2000.926982.

[20] ”Arrhythmia - Dataset - DataHub - Frictionless Data.” https://datahub.io/machine-learning/arrhythmia. Accessed 4 Mar. 2022

[21] ”Real Breast Cancer Data — Kaggle.” 5 Aug. 2021, https://www.kaggle.com/amandam1/breastcancerdataset. Accessed 4 Mar. 2022.

[22] ”diabetes.csv — Kaggle.” 13 Nov. 2017, https://www.kaggle.com/saurabh00007/diabetescsv. Accessed 4 Mar. 2022.

[23] Hamza, R., Yan, Z., Muhammad, K., Bellavista, P., Titouna, F. (2020, July). A privacy-preserving cryptosystem for IoT E-healthcare. Information Sciences, 527, 493-510.

[24] Akhbarifar, S., Javadi, H.H.S., Rahmani, A.M. et al. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. Pers Ubiquit Comput (2020).

[25] Jacob Ziv, The universal LZ77 compression algorithm is essentially optimal for individual finite-length N-blocks. IEEE Transaction Inf. Theory, 55, 5 (May 2009), 1941–1944.