Improving The Quality of Service of The Wireless Sensor Network

Lovepreet Kaur[1], Er. Harpreet Kaur[2]
[1]Bahra Group of Institute, Pataila
[2]AP and H.O.D of CSE Department, Bahra Group of Institution,Bhedpura, Patiala

Abstract- *Wireless sensors are deployed in the number of applications for measuring real-time data. Wireless sensors are resource constraint devices and limited resources in terms of power and area available. Next, due to periodic measurement, a large amount of raw data is generated. Thus, processing the raw data degrades the performance of the wireless sensor. Also, wireless sensors are deployed in the open network. Thus, any user can access the network and keep an eye on the data without any verification. Due to this number of attacks, eavesdropping, tampering, and replay on the wireless sensors. To overcome these attacks, confidentiality, and authentication of the users required. Therefore, in this paper a hybrid data compression, encryption and authentication approaches are proposed for the wireless sensor network. We have done compression using the neighborhood indexing sequence algorithm and encryption using the ANU algorithm. Next, to provide authentication, lightweight encryption authentication mode such as encrypt then MAC mode has selected. The MAC is generated using a secret sharing algorithm. The experimental results are performed on MATLAB 2013a. In the last, the performance of the proposed technique is compared with the existing technique, based on the compression ratio, output file size, and ciphertext combination.*

Keywords- Wireless Sensor, Lightweight Cipher, Authenticated Encryption, ANU cipher.

I. INTRODUCTION

The Internet of Things (IoT) network is connected the various fields such as homes, e-vehicles, e-healthcare system. The wireless sensors are deployed in these applications to monitor the real-time data [1]. Further, due to continuous monitoring of the data, a large amount of raw data is generated. The wireless sensors are resource-constrained devices in which a restricted computing capacity, memory size, weak range of communication, limited amount of energy, and low bandwidth. Thus, continuous processing of the raw data degrades the performance of the wireless sensor network. In the sensor nodes, most of the energy consumed during transmission [2]. Therefore, data reduction improves the performance of the wireless sensor.

On the other side, sensitive data is monitored in wireless sensors. Thus, the data is prone to various attacks as explained below [3].

- Privacy Attack: In this attack, the attacker tries to find the information communicated between the sensor nodes. The attack based on data orientation or context orientation determines the information. The most popular privacy attacks are eavesdropping and tempering attack. In the eavesdropping attack, the attackers listen to the packet, tries to find or request to send the data. On the other side, in the tempering attack, the attacker gains the physical access of the wireless sensor nodes and try to determine cryptographic keys or modify the functionality of the nodes.
- Impersonation Attack: In this attack, the attacker tries to impersonate the nodes or make multiple fake nodes. The most popular impersonation attack is Sybil attack in which multiple identities of the sensor nodes are made. These identities either stolen or fabricated in the adversary nodes.
- Denial of Service Attack: In this attack, the attacker tries the modify the nodes such a way the nodes malfunction due to this packet loss, the total energy consumption of the nodes, or congesting the network.

To resolve these attacks, cryptography algorithms are used. In the cryptography, the symmetric algorithm used which provide confidentiality but not the authentication. On the other side, the asymmetric algorithm provides confidentiality and authentication but consumes a large number of resources and computation time. Therefore, the symmetric algorithm is worked in the different authentication modes which provide confidentiality as well as authentication. The most popular authentication modes are CCM, GCM, EAX, and CBC mode [4]. Thus, in this paper, a hybrid data compression, lightweight encryption, and authentication for the wireless sensor network are proposed.

The rest of the paper as follows. Section II defines the literature survey on compression as well as authenticated encryption schemes. Section III explains the proposed

technique and its components. Section IV shows the experimental results and performance analysis. Section V highlights the conclusion.

II. LITERATURE SURVEY

In this section, various compression and authenticated encryption schemes has used in the literature are explained.

To reduce the power consumption, the authors Srisooksai, et al. [5] reviewed the energy-efficient medium access control or routing protocol techniques. Among the different techniques, data compression is a useful technique that reduces data communication on the channel. Thus, in this paper, different compression techniques for the wireless sensor networks studied. Thereafter, each compression technique is classified in detail. Finally, they have compared the techniques, their challenges.

Tuong Ly Le, Minh-Huan Vo [6], wireless sensors are battery operated and not recharge in the usual way. Thus, energy-efficient techniques are required to improve the performance of wireless sensor networks. To achieve this goal, in this paper data compression techniques are explored and a lossless data compression technique adjusted according to the requirement in the wireless sensor. Thereafter, the proposed technique has compared with the existing two compression techniques such as bzip2 and gzip.

Shuxia Wang [7], Based on the application of wireless sensor networks, this dissertation studies the sensing data compression algorithm on sensor nodes and the compressed storage processing method of massive sensor data in wireless sensor nets.Considering the spate-temporal correlation between sensor data on a single node, an improved adaptive Huffman coding algorithm is proposed, which targets to compress the capacity of transporting information.The algorithm is applicable to wireless sensor network nodes with limited storage and computing resources.The time, space-related sensor data are compressed in the instance where the error is adjustable.And take out the corresponding experiments and analysis.Several lossless compression algorithms for sensing data characteristics were analyzed and related comparison experiments were carried.The outcomes indicate that the algorithm can significantly reduce redundant data, receive a higher compression ratio and can guarantee data reconstruction accuracy.

Azar, et al. [8], proposed the data compression technique based on the discrete wavelet transform to compress the data. The proposed technique is deployed in the wireless body sensor network in which real data of the sensors are compressed. The experimental results show that the proposed technique reduces the data by up to 90% without losing the information.

Wireless sensor network plays a central role in the IoT (Internet of Things). In the IoTs, sensitive information is communicated on the network and prone to the number of attacks Thus, authors Costa, et al. [9] studied the security concern for the wireless sensor and review the various cryptography techniques. Thereafter, the cryptography technique open research challenges have defined which can be further improved to improve the security and performance of the technique.

Madhumita Panda [10], to provide security in the wireless sensor network used the AES algorithm. AES stands for the Advanced Encryption Standard. AES algorithm has to block size 128-bit, and three key sizes 128-bit, 192-bit, and 256-bit and 10,12,14 rounds. AES is a symmetric algorithm. Thus, the same key is used for encryption and decryption purposes.

Hoang, et al. [11], used the AES algorithm in the authentication mode to provide encryption as well as authentication. They have used the CCM mode and deployed for the application wireless body area network. In their work, they have generated the 128-bit key which used in the authentication mode. The results show that the proposed technique consumes lesser power and very high resource efficiency.

Wireless sensors are deployed in the number of sensitive applications such as e-healthcare, smart grid. Thus, authors Padmini, et al. [12] studied the security algorithms for the wireless sensor network and found that the AES algorithm is preferred in the wireless sensor network for security purposes. The AES algorithm provides confidentiality, integrity, of the communicated data but not provide authentication of the user. Thus, to provide authentication AES algorithm work in the authentication mode CCM (Counter Mode with cipher block chaining mode). The algorithm software implementation has done in the JAVA.

Kardi, et al. [13], to provide the security in the wireless sensor network used the asymmetric algorithm RSA and Elliptic Curve Cryptography (ECC). In asymmetric cryptography, two keys are used; public and private keys. The secret data is encrypted using the public key and which users have the private key on the network can decrypt the secret data. The performance analysis is done on the basis of encryption time, key size, and energy consumption.

K. Shankar and Mohamed Elhoseny [14], The fast development of networking permits substantial documents, for example, multimedia images, to be effectively transmitted over the Wireless Sensor Networks (WSNs). Image encryption is generally used to guarantee security as it may secure the images in the greater part. The process of securing the images in WSN against unauthorized users is a challenging one. For guaranteeing high security among Digital Images (DIs), Light Weight Cryptographic (LWC) algorithms are utilized which split the DI into a number of blocks; this will upgrade the level of security in WSN. Here, the proposed block cipher is RECTANGLE which separates the image in a bit-slice style; and improves the DI security level by encryption and decryption depending on the determination of optimal public key and private key individually. The key optimization was finished by the metaheuristic algorithm, for example, Opposition-based Grey Wolf Optimization (OGWO) which chosen optimal key on the basis of the most extreme PSNR value. The exhibited RECTANGLE–OGWO accomplished the least time to produce key which remained as an incentive to encrypt and decrypt the image. The result showed that the RECTANGLE–OGWO algorithm enhanced the accuracy of DI security for all the images (Lena, Barbara, Baboon, Airplane and House) when contrasted with existing algorithms.

From, the literature survey found that in the literature, various data compression techniques such as Huffman encoding, LZW encoding, and DWT encoding schemes are used. These techniques have limitation such as
The Huffman encoding frequency and probabilities change if the ensemble change. This LZW algorithm is affected bythe growing dictionary issue.

On the other side, for the security purposes, various symmetric algorithms such as AES, RC4, RC5, Blowfish [5-6], asymmetric algorithms RSA and Elliptic Curve Cryptography [9], and encryption authentication schemes such as AES-CCM [7-8] are used. These approaches consume large resources. Therefore, NIST recommended preferringa lightweight algorithm for the resource constraint devices. In the literature, the RECTANGLE algorithm is used for data encryption but due to a large number of rounds, and bit-level permutation takes large computation time. Therefore, we selected the neighborhood indexing sequence algorithm,ANU cipher, and secret sharing algorithm which consumes lesser computation time for data encryption and authentication.

III. PROPOSED WORK

In this section, proposed lightweight compression, as well as authenticated encryption scheme for the wireless sensor is explained. The block diagram for the proposed technique is shown in Fig. 1.

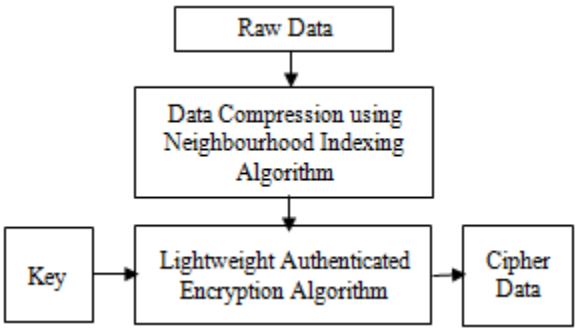

Fig. 1 Block Diagram of the Proposed Technique

3.1 Data Compression using Neighbourhood Indexing Algorithm [15]

The proposed NIS algorithm is a single character encoding scheme that works on the principle of "traversing data based on 0's and 1's". It assigns shorter length codewords to each character in the input sequence by the exploitation of valuable information among adjacent bits of the input character. Among the two shorter codewords generated by 0's and 1's traversal, the optimal codeword will be chosen on the basis of the minimum number of bits required to store the codeword of a respective character. The pseudocode for the data compression is shown in Table1. Next, to understand the NIA algorithm, it is explained with an example in Fig. 2.

Table 1 Pseudocode for the Data Compression

1. The algorithm reads the character and converts into corresponding ASCII value. Thereafter, the ASCII decimal value transform into binary equivalent using successive division method.

2. Next, the procedure "traversing data based on 0' s and 1' s" will be carried out. The bit traversal starts with the initial first bit in the binary equivalent of the input character and identifies whether the number is 0 or 1.

3. Next, 0's-based traversal is initiated and stores the control bit as 00 (when the identified first bit is 0) or 10 (when the identified first bit is 1). With the first bit as reference, the algorithm starts traversing from the second bit to identify 0's and store its positions when a 0 value is found. Once a value of 0 is found, its position (x) is stored in the codeword (00- x) and the procedure is initiated till the last seventh bit is reached.

4. When the traversal process reaches the final number, the corresponding codeword will be laid in.

5. Later on the completion of 0's based traversal, 1's based traversal will take place. The process involved in 0' s based traversal and 1's based traversal are similar, except that the 0's based traversal searches for 0's in the binary digits, whereas the 1's based traversal find 1' s in the binary digits.

6. Once the two codewords are generated, the proposed algorithm compares it and selects the codeword with the minimum number of bits as an optimal codeword. The number of bits in optimal codeword may contain a maximum of 4 bits and a minimum of 1 bit. Finally, all the resultant optimal codewords of encoded characters are concatenated with the control bits and generate the compressed file.

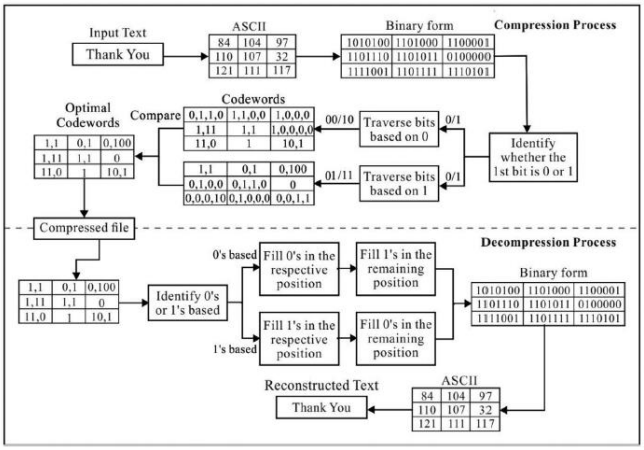

Fig. 2 NIS Diagram for better understand.

3.2 Lightweight Authenticated Encryption Algorithm

In this section lightweight authentication encryption scheme, encrypt then MAC mode is selected for providing encryption as well as authentication as shown in Fig. 3. This mode provides the first authentication then decrypts the data on the receiver side.

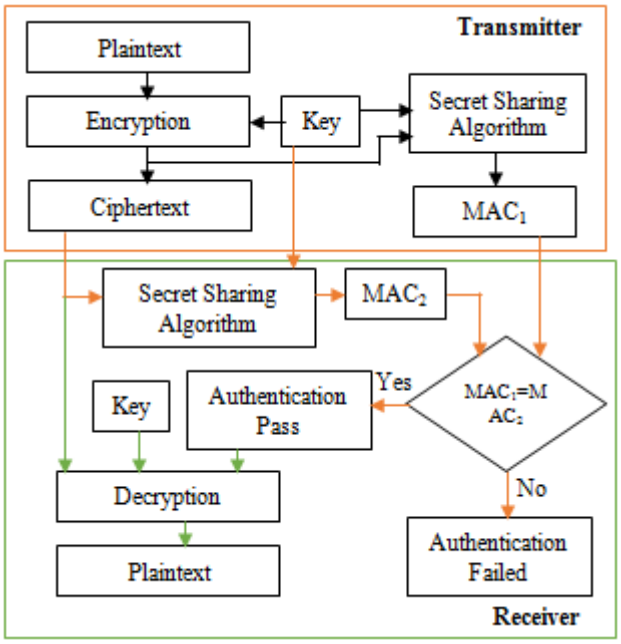

Fig. 3 Block Diagram of Transmitter and Receiver of Encrypt then MAC Mode

The data is encrypted using a lightweight ANU algorithm due to consuming less area, provide better security, and simpler key scheduling. Next, the MAC is generated using a secret sharing algorithm. The detail description of the ANU cipher and RC4 algorithm is given below.

3.2.1 ANU Algorithm

ANU algorithm was originated in 2016 by Bansod, et al. [16]. The algorithm has block size-64bit, key size-80/128 bit, and no. of rounds 25. ANU algorithm is based on the Feistel Network as shown in Fig. 4. The block is divided into two parts (P_i^L) and (P_i^R) and each part 32-bit long. Next, on the left part function is applied. The function has two operations F_1 and F_2. On the left part, F_1 and F_2 function is applied in which 3-bit left circular shift and 8-bit right circular shift performed, respectively. Next, on the shifted bits, s-box is applied which substitute the original bits with another value as shown in Table 2.

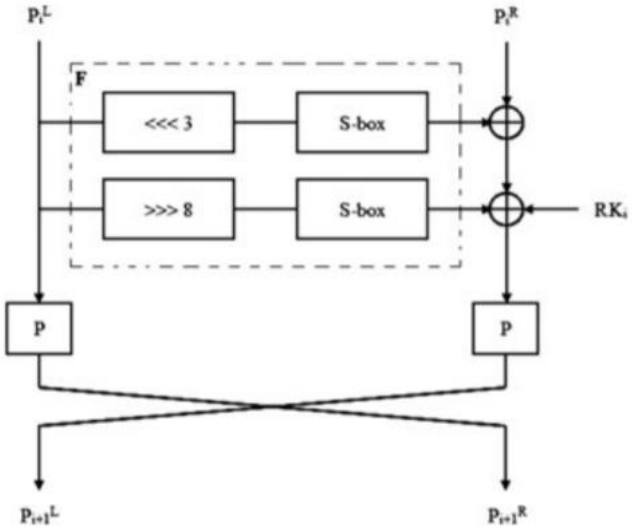

Fig. 4 Block Diagram of ANU Cipher

Further, XOR with the right part and key is performed. In last, bit level permutation is performed on the left and right part and their position is changed respectively as shown in Table 3. This process is performed 25 times.

Table 2 S-Box for the ANU Cipher

X	0	1	2	3
S-Box(X)	2	9	7	E
X	4	5	6	7
S-Box(X)	1	C	A	0
X	8	9	A	B
S-Box(X)	4	3	8	D
X	C	D	E	F
S-Box(X)	F	6	5	B

Table 3Permutation- Layer for the ANU Cipher

I	0	1	2	3	4	5	6	7
BP(i)	20	16	28	24	17	21	25	29
I	8	9	10	11	12	13	14	15
BP(i)	22	18	30	26	19	23	27	31
I	16	17	18	19	20	21	22	23
BP(i)	11	15	3	7	14	10	6	2
i	24	25	26	27	28	29	30	31
BP(i)	9	13	1	5	12	8	4	0

The pseudocode for the key scheduling is shown in the Table 4.

Table 4 Key Scheduling for the ANU Cipher

Key Scheduling
For 80-bit Key
Left Circular shift(Key, 13)
S-Box Layer(Key_{0-3})
XOR Operation ($Key_{63-59}, Round\_Counter$)
For 128-bit Key
Left Circular shift(Key, 13)
S-Box Layer(Key_{0-7})
XOR Operation ($Key_{63-59}, Round\_Counter$)

3.2.2 Secret Sharing Algorithm

The secret sharing algorithm was designed by Adi Shamir [17]. In which different shares are generated of the original part (n), and threshold (t) is taken in which n number of shares are added and compared with the threshold and based on that generate unique part. On the receiver side, same procedure is applied to generate the unique part. This algorithm is used to generate the MAC in the proposed technique. In which ciphertext, different parts are generated and based on the threshold unique cipher is generated which used as a MAC.

Table 5 Secret Sharing Algorithm

Original Stream	10101100
Share1	11101100
Share2	10111100
Share3	10101110
Threshold=3	
Addition Performed on the Share	31313310
Unique Share	10101100

In the receiver side, same procedure is applied on the ciphertext and unique cipher is generated and compared with the transmitted MAC. If the MAC is equal then authentication pass and decryption module work. Otherwise, authentication is failed. To understand the secret sharing algorithm explained with example in Table 5.

IV. EXPERIMENTAL RESULTS

In this section, the proposed technique is designed and simulated in MATLAB 2013a. In our work, standard dataset images are taken for data compression as well as data encryption. Next, the performance analysis of the proposed technique is done using various parameters.

- Compressed Ratio

This parameter is used to determine how many bits are reduced after applying the data compression technique [18] as shown in Table 6.

Table 6 Compression Ratio for the Different File Size

File	Compression Ratio
Random File1	0.99
Random File2	1
Random File 3	0.98
Random File 4	0.97

- PSNR (Peak Signal to Noise Ratio)

PSNR parameter is the ratio between the original data and encrypted data. It is measured in the decibels (dB). The higher the value of PSNR means the original data matched with the encrypted data. Therefore, in the encryption, minimum PSNR is required between original and encrypted Data. The PSNR for the different datasets is shown in Table 7.

Table 7 Peak Signal to Noise Ratio

Data	PSNR (in dB)
Random File1	8
Random File2	11.09
Random File 3	7
Random File 4	10

- Correlation

This parameter is used to determine how much correlation between original and encrypted data. In the ideal case, 0 correlation is required. The correlation to the different images shown in Table 8.

Table 8 Correlation for the Encryption

Data	Correlation
Random File1	0.01
Random File2	0.20
Random File 3	0.30
Random File 4	0.10

- Computation Time

The time spent in the data compression, encryption, and generation of MAC is determined using computation time. The computation time for the proposed technique shown in Table 9.

Table 9 Computation Time for the Proposed Technique

Technique	Computation Time (in Seconds)
Data Compression using NIS and Encryption-Authentication using ANU and Secret Sharing Algorithm	5

- Cipher Text Combination

In the lightweight cryptography, reducing the block size degrades the security and prone to the birthday attack. Thus, to increase the block size, the encrypted then MAC mode is hybrid as shown in Table 10.

Table 10 Comparative Analysis of Cipher Text Combination

Techniques	Brute Force Combination
Data Encryption using AES and Authentication using CCM Mode	2^{128}
Data Encryption using ANU and Authentication using Secret Sharing Algorithm	2^{192}

V. CONCLUSION

In this paper, the quality of the wireless sensor network is improved using compression and lightweight encryption authentication scheme. The result show that proposed technique achieves better compression, consume lesser resources and increases the block size of cipher, provide authentication and takes lesser computation. In the future, hardware implementation of the proposed technique will be done.

REFERENCES

[1] Wohwe Sambo, D., Yenke, B. O., Förster, A., &Dayang, P. (2019). Optimized clustering algorithms for large wireless sensor networks: A review. *Sensors*, *19*(2), 322.

[2] Sheltami, T., Musaddiq, M., &Shakshuki, E. (2016). Data compression techniques in wireless sensor networks. *Future Generation Computer Systems*, *64*, 151-162.

[3] Tayebi, A., Berber, S., & Swain, A. (2013, December). Wireless Sensor Network attacks: An overview and critical analysis. In *2013 Seventh international conference on sensing technology (ICST)* (pp. 97-102). IEEE.

[4] Švenda, P. (2016). Basic comparison of Modes for Authenticated-Encryption (IAPM, XCBC, OCB, CCM, EAX, CWC, GCM, PCFB, CS).

[5] Srisooksai, T., Keamarungsi, K., Lamsrichan, P., & Araki, K. (2012). Practical data compression in wireless sensor networks: A survey. *Journal of network and computer applications*, *35*(1), 37-59.

[6] Le, T. L., & Vo, M. H. (2018, November). Lossless Data Compression Algorithm to Save Energy in Wireless Sensor Network. In *2018 4th International Conference on Green Technology and Sustainable Development (GTSD)* (pp. 597-600). IEEE.

[7] Wang, S. (2019). Multimedia data compression storage of sensor network based on improved Huffman coding algorithm in cloud. *Multimedia Tools and Applications*, 1-14.

[8] Azar, J., Darazi, R., Habib, C., Makhoul, A., &Demerjian, J. (2018, June). Using DWT lifting scheme for lossless data compression in wireless body sensor networks. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 1465-1470). IEEE.

[9] Costa, D. G., Figuerêdo, S., & Oliveira, G. (2017). Cryptography in wireless multimedia sensor networks: A survey and research directions. *Cryptography*, *1*(1), 4.

[10] Panda, M. (2015, January). Data security in wireless sensor networks via AES algorithm. In *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)* (pp. 1-5). IEEE.

[11] Hoang, V. P., Dao, V. L., & Pham, C. K. (2016, September). A compact, ultra-low power AES-CCM IP core for wireless body area networks. In *2016 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)* (pp. 1-4). IEEE.

[12] Padmini, R., Pavithra, A. B., Manjunath, B. E., & Manjunath, M. (2018). Authenticated Encryption for Wireless Sensor Network. *Perspectives in Communication, Embedded-systems and Signal-processing-PiCES*, *2*(4), 95-97.

[13] Kardi, A., Zagrouba, R., &Alqahtani, M. (2018, April). Performance Evaluation of RSA and Elliptic Curve Cryptography in Wireless Sensor Networks. In *2018 21st Saudi Computer Society National Computer Conference (NCC)* (pp. 1-6). IEEE.

[14] Shankar, K., &Elhoseny, M. (2019). An Optimal Lightweight RECTANGLE Block Cipher for Secure Image Transmission in Wireless Sensor Networks. In *Secure Image Transmission in Wireless Sensor Network (WSN) Applications* (pp. 33-47). Springer, Cham.

[15] Uthayakumar, J., Vengattaraman, T., &Dhavachelvan, P. (2019). A new lossless neighborhood indexing sequence (NIS) algorithm for data compression in wireless sensor networks. *Ad Hoc Networks*, *83*, 149-157.

[16] Bansod, G., Patil, A., Sutar, S., &Pisharoty, N. (2016). ANU: an ultra lightweight cipher design for security in

IoT. *Security and Communication Networks*, *9*(18), 5238-5251.

[17] Dehkordi, M. H., &Mashhadi, S. (2008). An efficient threshold verifiable multi-secret sharing. *Computer Standards & Interfaces*, *30*(3), 187-190.

[18] Uthayakumar, J., Vengattaraman, T., &Dhavachelvan, P. (2018). A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications. *Journal of King Saud University-Computer and Information Sciences*.