2022 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS) | 979-8-3503-3242-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISPACS57703.2022.10082815

Improved QoS in Internet of Things (IoTs) through Short Messages Encryption Scheme for Wireless Sensor Communication

Syed Hussain Ali Kazmi
Center for Cyber Security, Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), 43600 UKM Bangi,
Selangor, Malaysia
P112235@siswa.ukm.edu.my

Faizan Qamar*
Center for Cyber Security, Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), 43600 UKM Bangi,
Selangor, Malaysia
faizanqamar@ukm.edu.my

Rosilah Hassan
Center for Cyber Security, Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), 43600 UKM Bangi,
Selangor, Malaysia
rosilah@ukm.edu.my

Kashif Nisar
Faculty of Computing and Informatics, University Malaysia Sabah,
Sabah, Malaysia
kashif@ums.edu.my

***Abstract*—Global interest in Internet of Things (IoTs) can be accorded to the provisioning of Wireless Sensors Communication (WSC). Sensor data cannot be standardized due to diverse nature of measurements. However, the sensor's data needs to be converted into standard size for compatibility with encryption schemes. Therefore, IoTs face various processing and communication overhead issues for acceptable Quality of Service (QoS) in WSC. We proposed a communication model of the Short Messages Encryption Scheme (SMES) Model with the least additional padding in plain text. We performed a comparative analysis of various existing encryption modes and highlighted the limitations concerning compatibility with SMES. Our communication model utilizes Time of Day (TOD) based loose synchronization intervals in combination with Cipher Feed-Back (CFB) mode of AES encryption. Our evaluation of the proposed scheme shows least processing requirements and overheads in comparison with various other encryption modes. We concluded this paper by deliberating possible future research directions in SMES for IoTs.**

Keywords—AES, Encryption, Synchronization, Overhead, Cipher.

I. Introduction

The blooming future of emerging technologies, Internet of Things (IoTs) [1] and Wireless Sensors Communication (WSC) are unifying to revolutionize our lives by integrating entire global technology elements such as: transportation infrastructures, mailboxes, light switches, humans, cars, appliances, utilities and any other entity that might take advantage of an intelligent link [2]. IoTs contain four architectural elements which include; the sensors connecting layer, the management service layer, the gateway, network layer and the application layers, it has detector, sensors, actuators, RFID tags and computer codes. Connectivity among networks and sensors is achieved through detector layer such as it is incorporated through RFID tags, computer codes based the detector and actuators. Sensors to network connectivity level contains solid state, catalytic, spinner, photoelectric, photochemistry, infrared, accelerometers, geo location and similar devices. Various technologies such as drones have opened huge flux of sensors communication [3]. WSC is a foundational phenomenon behind intense technological integration in human life. In information theoretic perspective, WSC involves vital but usually an extremely small amount of information comprising of few bits. In integrated format, these minute portions of information in WSC act as a governing element in a large complex system.

Any kind of manipulation or compromise of information in WSC may result in complete system failure. Especially, IoTs utilize various types of sensors for health monitoring in body area networks. Security compromise of personal credentials will result in irreparable damages such as fingerprint theft, retina signature stealing etc. In the security domain, encryption is considered as a foundational mechanism; however, the wireless sensor information is usually small messages with random size. Therefore, sensor information is firstly collected in additional processing hardware of IoTs for further conversion into standard-length messages for network communication. Similarly, for incorporation of encryption, the sensor's information is padded to achieve length required by standard encryption algorithms such AES (Advanced Encryption Standard) utilizes 128bit block size. However, the padding involved during the standardization of message length causes substantial overhead. Moreover, IoTs are resource-constraint devices with limited processing capacities.

With this premise, in this paper, we performed a comparative analysis for the possibility of Short Messages Encryption Scheme (SMES) in WSC with the least additional padding. Moreover, we discussed the encryption mechanisms in detail and evaluated suitable AES encryption mode for processing requirements in resource-constraint IoTs. Thereby, we suggested a secure communication model based on counter and Time of Day (TOD) for the least overhead in encryption.

II. Related Works

Commercial utilization of wireless sensors extremely necessitates a dependable and resilient encryption mechanism. Therefore, huge research efforts are required for designing a short message encryption scheme. In [4], the authors studied utilization of RSA, ELGamal and Elliptic Curve encryption

979-8-3503-3242-1/22/$31.00 ©2022 IEEE

Authorized licensed use limited to: National Tsing Hua Univ.. Downloaded on July 29,2024 at 11:19:50 UTC from IEEE Xplore. Restrictions apply.

algorithms. However, these asymmetric schemes create higher processing and bandwidth overheads. Moreover, it is comprehensively elaborated in [5] that AES encryption solely can not meet the requirements of short message encryption. The authors in [6] suggested digital signature algorithms for short message encryption. However, these algorithms result in high processing overheads which are not feasible in low-processing IoTs. In [7], the authors suggested an image-based encryption scheme with specific image sensor applications. In [8], the authors suggested a compound chaotic map for encryption in WSC; however, the scheme contains limitations of hardware processing related to Feistel structures. The area for designing a secure short message encryption scheme in WSC contains limited research works.

III. Problem Statement

"Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication" [9]. In information security, "Confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities or processes." [10]. The incorporation of confidentiality in IoTs is primarily pursued through the encryption of data. For simple AES encryption, the data size of messages from sensors is non-standard, as 128bit; therefore, padding is added to convert the data length into standard blocks. However, padding for encryption results in significant overhead effects in throughput [11, 12]. Therefore, a SMES is required to ensure confidentiality with minimum or no encryption overhead.

IV. Short Message Encryption Scheme

A. Communication Model

To counter the problem of encryption-related overhead, initially, we suggest the communication model for message formation with the least overhead as shown in Fig. 1. The TOD loose synchronization incorporation is considered fairly possible for IoTs. We suggest a loose synchronization of 8 seconds among IoTs for TOD along with a counter with an equally spaced interval in 8 seconds. This proposed communication model involves the following steps: -

- Analog to digital conversion of sensor information as a binary stream.
- The sensor binary data stream will be converted into hex data. This process will require at most 3bit of padding.
- The data will be subject to a suitable encryption Mode to generate the encrypted data with the least overhead.
- Both transmission and receiving ends are loosely time synchronized.

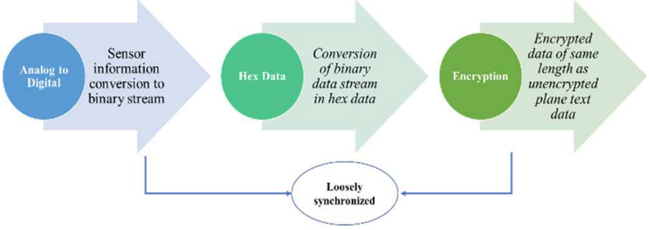
Analog to Digital
Sensor information conversion to binary stream
Hex Data
Conversion of binary data stream in hex data
Encryption
Encrypted data of same length as unencrypted plane text data
Loosely synchronized

Fig.1. Communication Model

B. Evaluation of Encryption Modes

Various AES-based cipher modes have been compared concerning message encryption. A block cipher mode of operation—or simply, mode—is an algorithm for the cryptographic transformation of data that is based on a block cipher. The following encryption modes are compared for suitability with the proposed SMES model.

1) *ECB (Electronic Code Book) mode:* This is the most straightforward way of encryption. Fig. 2 shows encryption and decryption in ECB mode [13].

a) Properties of ECB mode: Following are the properties of ECB mode.

- Identical plain text blocks result in identical cipher text.
- Blocks are encrypted independently.
- One or more-bit error in each cipher text block would make about 50% recovered plain text in error.

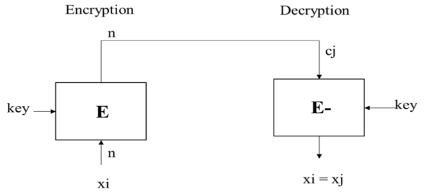

Fig. 2. ECB mode block diagram

b) *Utilization of ECB mode for SMES:* ECB mode takes plain text messages of standard block size i.e. 128 bit in case of AES or adds padding bit to get the standard block size. ECB cannot be used for encryption in SMES.

2) *CBC (Cipher Block Chaining):* CBC mode involves the use of n-bit (128 bit in AES) initialization vector, denoted as IV. Fig. 3 shows the operation of CBC mode [13].

a) Properties of CBC mode: Following are properties of CBC mode.

- When identical plain text is encrypted under the same Initialization Vector (IV) and key then the same cipher text is produced.
- The chaining process causes cipher text c_j to depend upon input x_j and all preceding plain text blocks.
- A single-bit error in cipher text block c_j affects c_j and c_{j+1} cipher text block. x_j is recovered with almost 50% error bit while x_{j+1} has a precise error at a specific bit.
- IV in CBC mode need not to be secret.

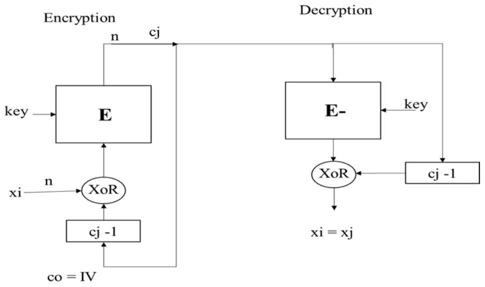

Fig. 3. CBC Mode block diagram

b) Utilization of CBC for SMES: Like ECB mode, CBC mode also takes plain text messages of standard block size

Authorized licensed use limited to: National Tsing Hua Univ.. Downloaded on July 29,2024 at 11:19:50 UTC from IEEE Xplore. Restrictions apply.

i.e. 128 bit in case of AES or adds padding bit to get the standard block size. CBC cannot be used for encryption in SMES as the message lengths can be smaller than 128 bit.

3) Output Feed-Back Mode: OFB mode operation as shown in Fig. 4 [13], utilizes an Initialization Vector (IV) and uses r<= n bit encrypted IV as feedback. "n" is block size that is 128 bit in case of AES. The OFB mode provides the computational advantage of pre-generation of key stream. It is a kind of stream cipher.

a) Properties of OFB mode: Following are properties of OFB mode.

- As in CBC and CFB changing IV would result different encryption of same plain text.
- Keystream is independent of plaint text.
- Single or more bit errors in cipher text only effect the corresponding plaint text bit.
- As in CFB, any size of plaint text 'r' can be encrypted to same length cipher text.

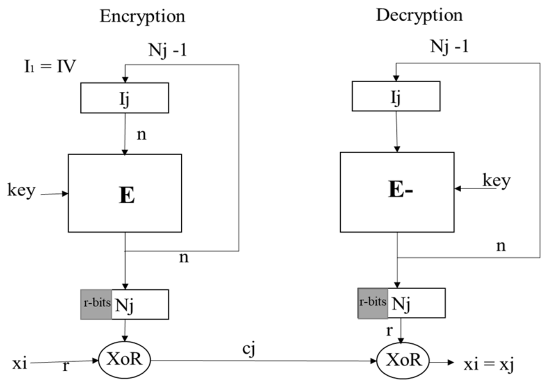

Fig. 4.OFB block diagram

b) Utilization of OFB for SMES: OFB can be used for SMES message encryption. However, the key stream would be fixed if IV is the same. By keeping IV same, key stream will also remain the same. So same plain text would have same cipher text. Unlike CFB, Feedback size also do not affect key stream. This results in the identical key stream every time and by XORing corresponding cipher texts an adversary may reduce cryptanalysis to that of a running-key cipher [14], therefore OFB would not be suitable for SMES messages encryption.

4) Counter (CTR) Mode: Counter Mode is also known as Integer Counter Mode (ICM). It is like OFB, which turns block cipher into a stream cipher. In this mode, both sender and receiver have to access a reliable counter and this shared counter is not required to be secret. Fig. 5 shows the operation of CTR mode [15].

a) Properties of CTR Mode: Following are properties of CTR Mode.

- The initial value of the counter is to be the same and synchronized for both sender and receiver.
- It does not contain chaining dependency. A cipher text block does not depend upon the previous plain text.
- The serious disadvantage of CTR mode is that it needs a synchronized counter at the sender and receiver. In case, synchronization is lost then decryption is not possible.

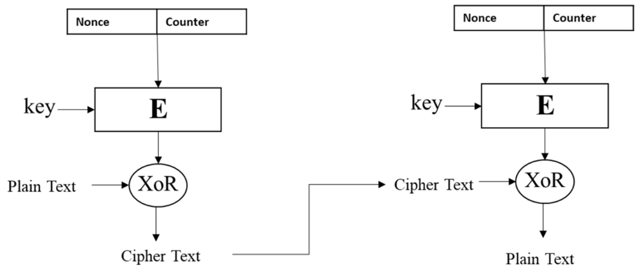

Fig. 5. CTR mode

b) Utilization of CTR (Counter) for SMES: CTR is same as OFB that converts block cipher into stream cipher. CTR mode can be used for SMES message encryption but counter would need to have loose synchronization. Synchronization precision might not be operationally feasible in IoTs. No increment in counter would result same key stream, so CTR mode is also not considered for SMES.

5) FPE (Format Preserving Encryption): FPE simplifies the encryption to sensitive information, as well as the retrofitting of encryption technology to legacy applications, where a conventional encryption mode might not be feasible. Format Preserving Encryption (FPE) are NIST (National Institute of Science and Technology) United States-published FPE algorithms as FF1, FF2 and FF3 [16]. FF2 and FF3 are considered no more secure due to their known published vulnerabilities [17]. However, FF1 is considered still secure due to its no known weakness. Therefore, FF1 has been also evaluated for implementation in Mode-5 Capable Secure Waveform. FF1 utilizes a Feistel structure for encryption and decryption. FF1 takes 10 rounds of AES for one-block encryption. The standard detailed algorithm of FF1 is given in NIST Special Publication 800-38G [18].

a) Properties of FF1: Following are properties of FF1 encryption:

- FF1 encrypts binary and non-binary data to the same length as of message.
- FF1 takes input non-secret value Tweak (T) as optional input. Changing the tweak results in different encryption of the same plain text.
- Encryption of a single message takes 10 AES rounds.

b) Utilization of FF1 for SMES: FF1 can be used for encryption in SMES. Tweak can be used as the time-synchronized parameter. Unlike CTR and OFB, any change in single or more cipher text bits will result in about 50% decrypted text in error. As FF1 single block encryption takes 10 rounds (AES encryption), it is not suitable for the encryption of SMES in IoT due to real-time processing overhead.

Authorized licensed use limited to: National Tsing Hua Univ.. Downloaded on July 29,2024 at 11:19:50 UTC from IEEE Xplore. Restrictions apply.

6) Cipher Feed-Back Mode (CFB): CFB mode operates as shown in Fig. 6 [13] and utilizes an Initialization Vector (IV) and uses r<= n bit cipher feedback that slides in IV. Here ‘n’ is the block size of cipher i.e. 128bit in AES.

a) Properties of CFB: Following are properties of CFB mode.

- Changing the IV will result in same plain text encrypted as different output.
- Chaining dependency causes c_j cipher text to depend upon x_j and the preceding plain text block.
- Unlike ECB and CBC, any size of plain text ‘r’ (r<=n)can be encrypted to the same size cipher text in a single encryption cycle.
- Any single bit error in ‘r’ bit cipher text will affect all the next received blocks.

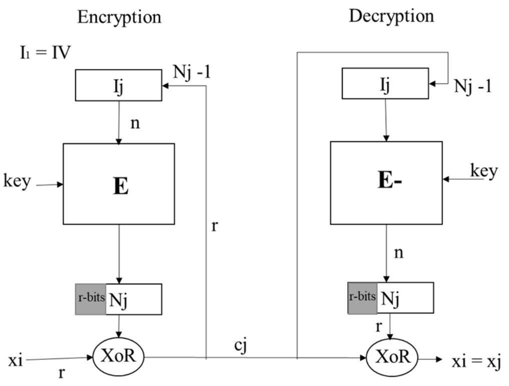

Fig. 6. CFB Block diagram

b) Utilization of CFB for SMES: CFB can be used to encrypt data in SMES but in case of fixed IV, same plain text will result in the same cipher text. Further, if whole message is sent in feedback then the loss of a single message by a receiver would make system unsynchronized. In short-length messages there is the possibility that every next plain text message is having only little change. First, the available option is to keep changing the IV. In loosely synchronized systems, linking IV with time would result in a change of IV at specific intervals. But, during an interval, the same plain text would have same corresponding cipher text. This results in an identical key stream every time and by XORing corresponding cipher texts an adversary may reduce cryptanalysis to that of a running-key cipher. For SMES, by reducing feedback size and keeping a counter at start, it is possible to have different cipher text of the same plain text. However, by reducing the feedback, the number of iterations will increase. After a complete single message transmission IV is reset to the original state.

C. Encryption Mode for Proposed Communicaiton Model

We proposed a modified CFB mode for SMES. The proposed mode will contain the IV with time-synchronized dynamic changes after every specific interval. NIST recommends, *“**For the CBC and CFB modes, the IVs must be unpredictable**. In particular, for any given plaintext, it must not be possible to predict the IV that will be associated to the plaintext”* [19]. However, IV need not to be secret but NIST recommendations are as caution. There are also some known IV attacks for CFB in DES block cipher [28]. Fig. 7 depicts the functional diagram of proposed SMES.

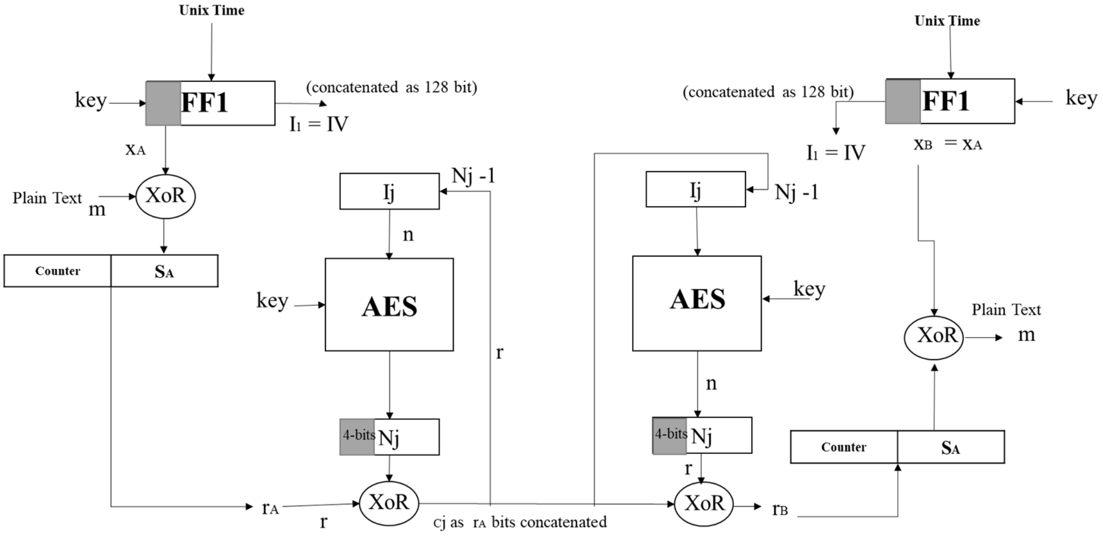

Fig. 7. SMES Block diagram

Following NIST recommendation, IV is kept completely pseudo-random in proposed encryption scheme.

- TOD is maintained through 32bit UNIX time also known as Epoch time.

- The time has reached up to 1556668800 (“1011101000011001100101110100011’) seconds on 0000hrs 1 May, 2019 since Jan 1, 1970.

- FF1 encryption with 256bit key to generate a completely random number.
- The 128bit block IV is generated through repeating and concatenating of FF1 encrypted 31bit of UNIX time.
- IV is calculated in terms of future, present and past value as +IV, IV, -IV for compatibility with time interval instances.

Authorized licensed use limited to: National Tsing Hua Univ.. Downloaded on July 29,2024 at 11:19:50 UTC from IEEE Xplore. Restrictions apply.

- The plain text message is XOR with left most bit of IV.
- The counter is to keep cipher text different for the corresponding same plain text. We used 12it counter in our analysis, however, counter size can be changed as per update requirements from sensors. The counter is concatenated with the XOR value of plain text.
- In the proposed implementation of 4bit feedback, in CFB mode. The resulting 4bit cipher is concatenated as cipher text of the same length as combined counter and plain text.
- The IV generation is performed in every interval with preprocessing; therefore, the processing time for IV **generation** would not affect in real-time processing. Moreover, time-dependent IV are secure and resistant to the majority of cyber attacks [20].

D. Pseudocode for proposed Model

Following is the pseudocode for above-proposed message authentication protocol of SMES.

(a) Step for every 8 second interval

i. User "A" calculates a secret (w_A). $E\text{`}_k$ is encryption function (instead of One-way function) which is FF1 in proposed protocol. 'K' is 256 bit pre-shared key.

ii. (32 bit) UNIX time is used for 8 second TOD interval. w_A is 128bit random by 32bit concatenation to form 128bit as 'T_A'. 'IV_A' is utilized as IV for CFB.

$$IV_A = E\text{`}_k\,(T_A)$$

iii. "A" extracts the most significant bits (MSB) 'x_A' bit from IV_A of same length as message data from sensor.

(b) Protocol Message: 'm' is the data bit in the message. 'n' is 12bit counter value that is incremented for every next plain text message. E_{kCFB} is an encryption function i.e. CFB mode of AES. ('||' denotes concatenation).

$$S_{A\,=}\, m \text{ XoR } x_A$$

$$A \longrightarrow B \quad : \quad Ek_{CFB}\,(n \,||\, S_A)$$

(c) Protocol Actions: To receive message, "B" does following actions

i. B's equipment computes $IV_B = E\text{`}_k\,(T_B)$

ii. User "B" extracts the first bit from IV_B as per size of m.

iii. "B" decrypts the received message and extracts 'n" and checks if n > n`, here 'n`' is counter value for previous message.

iv. If 'n' is new then it will be stored for comparison with next message but Reply will not be generated.

v. The message is extracted as $x_A = x_{B.}$

vi. If $x_A \neq x_{B,}$ then decryption process in performed with +IV or -IV.

vii. Any error in encrypted data would result in 50% of plain text in random. Therefore, due to synchronization, the number value in message should satisfy the following condition:-

n+ > n > -n.

viii. If n is drastically changed and does not follow above condition of n in +IV, IV and -IV then the message is discarded.

E. Performance Evaluation

The performance of the proposed model is evaluated by comparison with CFB, OFB and FF1. Number of AES iterations with respect to block size is considered to comparison criteria. Here, FF1 utilization for IV calculation under preprocessing. However, the comparison of the proposed scheme counts for 10 AES cycles of FF1 in as shown in Fig. 8 and Fig. .9. The analysis shows that OFB and CBC are better that FF1 in terms of processing performance and overhead. Following are the advantages of using loosely synchronized CFB mode as SMES.

(a) CFB is preferable compared to OFB as specific bit flip will not result in change of corresponding plain text.

(b) CFB mode can use 4-bit feedback block size for encryption in SMES.

(c) The proposed mechanism would provide a time synchronization-based encryption with dynamic IV as according to NIST "The IV need not be secret, but it must be unpredictable".

(d) Counter-based change in plain text would change the cipher text of all the preceding plain text, even if IV is same for 8 seconds.

(e) Single bit flip in cipher text will result about 50 % of the preceding bit in error. This feature would detect integrity violations of messages.

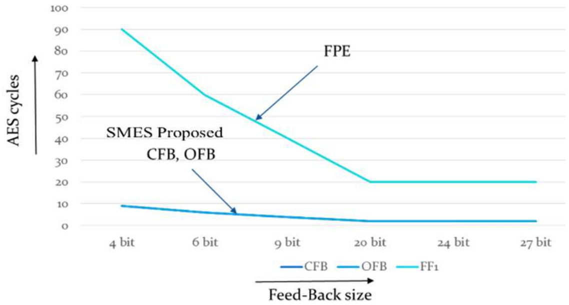

Fig.8. Block Size vs. AES cycles comparison of 40bit plain text

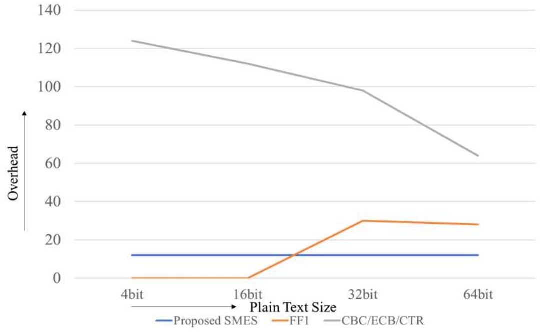

Fig.9. Comparison of AES modes with Overhead vs plain text plain text size

Authorized licensed use limited to: National Tsing Hua Univ.. Downloaded on July 29,2024 at 11:19:50 UTC from IEEE Xplore. Restrictions apply.

V. Future Research Directions

The proposed communication model provides secure SMES based on TOD. The encryption with the almost same length as of original message fairly reduces various processing and communication overheads. The proposed mechanism provides a joint utilization of FF1 and CFB, however, research is required in the following domains for further realization of the proposed communication model.

A. Protocol Optimization:- The proposed scheme can be further optimized by utilizing high-precision clocks such as atomic clock. Reduction in the time interval of synchronization would allow a reduction in the size of the counter bit to reduce the overhead. Time-synchronized systems can produce a strong stream for cipher.

B. Hardware Analysis

The hardware dependability fairly governs the design of every encryption model. The proposed scheme follows the principle of least processing requirement of IoTs. However, hardware-based analysis and evaluation of proposed model would further reveal the unforeseen benefits of reduced in overheads.

C. Integration with External Networks

IoTs are an integral part of the emerging heterogeneous networking paradigm [21]. Therefore, it is a necessary requirement to consider the integration and compatibility issues of the proposed communication model with existing networking protocols.

VI. Conclusion

Integration of WSC with IoTs is a governing factor behind the wide utilization of emerging technologies in human society, such as health, automobile etc. However, the security of sensors data is a paramount requirement. Therefore, encryption is used to ensure sensors data confidentiality. Existing encryption schemes result several overheads in terms of processing and bandwidth due to data padding. We proposed a time synchronization-based SMES with least padding requirements. Our analysis and evaluation show that the proposed scheme is efficient in terms of processing requirements. Moreover, we highlighted various future research directions for the realization of the proposed scheme in heterogenous IoTs communication.

Acknowledgment

The authors would like to acknowledge Universiti Kebangsaan Malaysia Geran Galakan Penyelidik Muda (GGPM) GGPM-2021-040.

References

[1] M. M. Rahman, M. Manavalan, and T. K. Neogy, "Artificial Intelligence in 5G Technology: Overview of System Models," *Asia Pacific Journal of Energy and Environment,* vol. 8, no. 1, pp. 17-26, 2021.

[2] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of Things and its applications: A comprehensive survey," *Symmetry,* vol. 12, no. 10, p. 1674, 2020.

[3] S. H. A. Kazmi, A. Masood, and K. Nisar, "Design and Analysis of Multi Efficiency Motors Based High Endurance Multi Rotor with Central Thrust," in *2021 IEEE 15th International Conference on Application of Information and Communication Technologies (AICT)*, 2021: IEEE, pp. 1-4.

[4] M. Agoyi and D. Seral, "SMS security: an asymmetric encryption approach," in *2010 6th International Conference on Wireless and Mobile Communications*, 2010: IEEE, pp. 448-452.

[5] R. Rayarikar, S. Upadhyay, and P. Pimpale, "SMS encryption using AES algorithm on android," *International Journal of Computer Applications,* vol. 50, no. 19, pp. 12-17, 2012.

[6] N. Saxena and N. S. Chaudhari, "Secure encryption with digital signature approach for Short Message Service," in *2012 World Congress on Information and Communication Technologies*, 2012: IEEE, pp. 803-806.

[7] W. Wang *et al.*, "An encryption algorithm based on combined chaos in body area networks," *Computers & Electrical Engineering,* vol. 65, pp. 282-291, 2018.

[8] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, and J. Liu, "A novel block encryption algorithm based on chaotic S-box for wireless sensor network," *IEEE Access,* vol. 7, pp. 53079-53090, 2019.

[9] J. Kim, H. Wu, and R. C. W. Phan, "Cryptography and future security," *Discrete Applied Mathematics,* vol. 241, p. 1, 2018.

[10] S. Samonas and D. Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security," *Journal of Information System Security,* vol. 10, no. 3, 2014.

[11] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, 2003, pp. 151-159.

[12] O. Abolade, A. Okandeji, A. Oke, M. Osifeko, and A. Oyedeji, "Overhead effects of data encryption on TCP throughput across IPSEC secured network," *Scientific African,* vol. 13, p. e00855, 2021.

[13] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[14] S. Gangwar and P. K. Yadav, "Information Security: New Cryptographic Approach," *International Journal of Computational Intelligence Research,* vol. 13, no. 4, pp. 537-545, 2017.

[15] "operation modes of block cipher." https://xianmu.github.io/posts/2017-08-13-operation-modes-of-block-cipher.html (accessed.

[16] J. Vance and M. Bellare, "An extension of the FF2 FPE Scheme," *Submission to NIST,* 2014.

[17] R. Agbeyibor, J. Butts, M. Grimaila, and R. Mills, "Evaluation of format-preserving encryption algorithms for critical infrastructure protection," in *International Conference on Critical Infrastructure Protection*, 2014: Springer, pp. 245-261.

[18] W. Stallings, "Format-preserving encryption: Overview and NIST specification," *Cryptologia,* vol. 41, no. 2, pp. 137-152, 2017.

[19] M. J. Dworkin, "Sp 800-38a 2001 edition. recommendation for block cipher modes of operation: Methods and techniques," ed: National Institute of Standards & Technology, 2001.

[20] H. T. Assafli, I. A. Hashim, and A. A. Naser, "The Evaluation of Time-Dependent Initialization Vector Advanced Encryption Standard Algorithm for Image Encryption," *Engineering and Technology Journal,* vol. 40, p. 08, 2022.

[21] F. Qamar, M. U. A. Siddiqui, M. N. Hindia, R. Hassan, and Q. N. Nguyen, "Issues, challenges, and research trends in spectrum management: A comprehensive overview and new vision for designing 6G networks," *Electronics,* vol. 9, no. 9, p. 1416, 2020.

Authorized licensed use limited to: National Tsing Hua Univ.. Downloaded on July 29,2024 at 11:19:50 UTC from IEEE Xplore. Restrictions apply.