International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1953126

Optimization of Security and Privacy- Preserving Data Using an IoT CLEFIA Based Security LFSR

Nahla F. Osman
Faculty of Computer Science, King Khalid University, Abha, Saudi Arabia

ABSTRACT

Over the recent years, several smart applications like RFID‟s, sensor networks, including industrial systems, critical infrastructures, private and public spaces as well as portable and wearable applications in which highly constrained devices are interconnected, typically communicating wirelessly with one another, working in concert to accomplish some task. Advanced safety and security mechanisms can be very important in all of these areas. Lightweight cryptography enables secure and efficient communication between networked smart objects. The CLEFIA algorithm is a suitable lightweight cryptographic algorithm used in medium security systems. In order to increase safety and security mechanisms, modify CLEFIA are proposed which uses the Linear Feedback Shift Register (LFSR) to overcome the security weakness of the CLEFIA algorithm against attacks. In this paper an implementation of modify CLEFIA algorithm using C++ programming language. We have also compared the results with the standard CLEFIA.

Keywords: Internet of Things (IoT), lightweight cryptography, CLEFIA algorithm and Linear Feedback Shift Register (LFSR)

I. INTRODUCTION

The Internet of Things (loT) promises to be the next big revolution of the World Wide Web. It has a very wide range of applications, ranging from smart cities, smart homes, monitoring radiation levels in nuclear plants, animal tracking, health surveillance and a lot more. When objects, people or animals are provide with unique identifiers and are able to communicate with each other without human intervention it is refer as the Internet of Things or Internet of Objects. Four major challenges in loT are power management, deployment of IPv6, standardization and security [1]. Data Security is a primary issue in any wireless cryptographic protocol, a cryptographic algorithm is an essential part in network security. One of the state-of-the-art techniques is “Lightweight Cryptography (LWC)”. Lightweight cryptography is a cryptographic algorithm or protocol tailored for implementation in constrained environments like RFID‟s, sensor networks, healthcare, the Internet of Things, cyber-physical systems, distributed control systems, indicators, measuring devices, custom controllers, smart power system etc.[6].

The organization of this document is as follows. In Section 2 (**Related Work**), I’ll give detail of any List some related work regarding the lightweight ciphers. In Section 3 (**Discussion**), present discusses the related work. Presented in Section 4(**Conclusion**).

II. RELATED WORK

This section shows some other works from related field. A number of studies by the eminent researchers are done in literature to improve the security and privacy in IoT. We are discussed more relevant and recent available solutions for security, privacy and hence improve small cryptographic algorithms for IoT.

In [8] author proposed of a Lightweight Encryption Algorithm for Secure Internet of Things named as Secure IoT (SIT). The main idea for SIT solution is a hybrid approach based on feistel and SP networks. SIT is a 64-bit block cipher by uses 64-bit key to encrypt data bit. The most fundamental component in the processes of encryption and decryption is the key. The architecture of the key expansion block is shown in **Figure 1.** below:

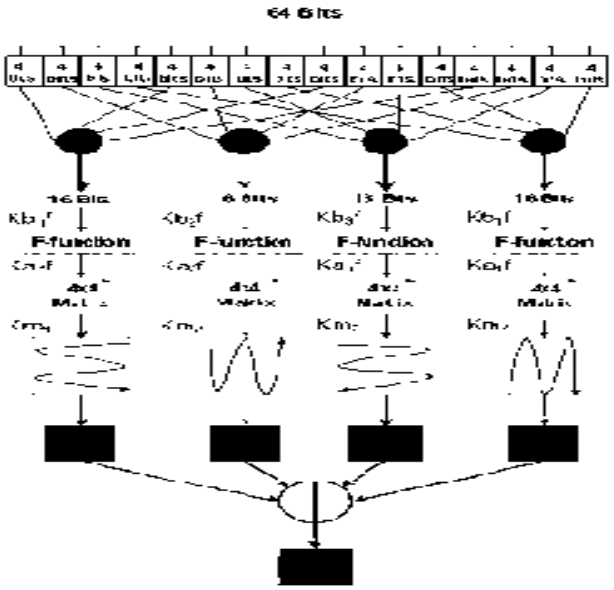

Figure 1. Key Expansion

The process of encryption is illustrated in **Figure 2.**

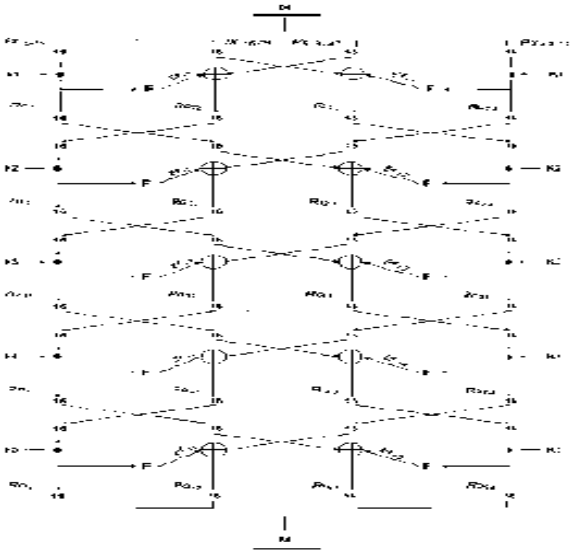

Figure 2. Encryption Process

The argument with this solution making use of the properties of both approaches to develop a lightweight algorithm that presents substantial security in IoT environment while keeping the computational complexity at moderate level. However, in this architecture 64-bit sub-key is used which is too short. Also just five encryption rounds is used which is too few to presents substantial security in IoT environment. In SPN, do not a direct implementation of confusion and diffusion.

A study in [9] proposed a novel architecture for lightweight block cipher, Piccolo. The main idea for this solution is shares the key scheduling block for two plain text blocks concurrently. The architecture of the Piccolo are shown in **Figure 3.** below. The argument with this proposed system is that by Parallelism, the speed of execution is it increased and it enhances the system throughput. However, Parallelism is a limitation for hardware implementation.

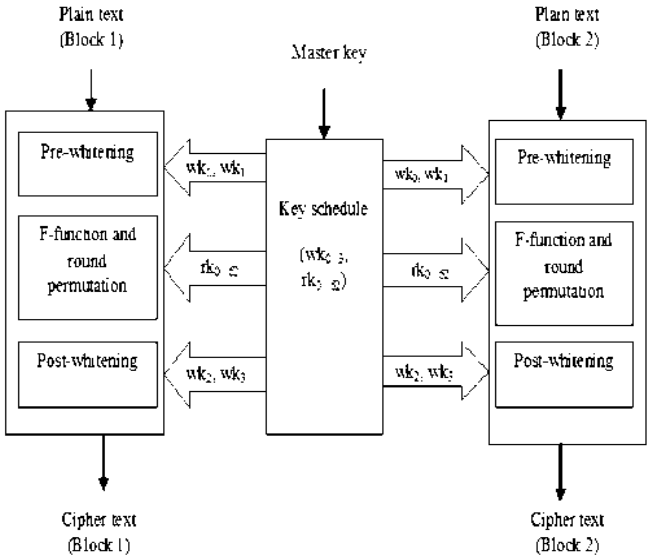

Figure 3. Novel architecture for Piccolo

In [6] a study proposed TEA solution. The basic idea for the proposed scheme is implementation of efficient pipelined TEA architecture. TEA takes 64 (block size) data bits time using a 128-bit key with 32 rounds. The **Figure 4.** shows the architecture for TEA.

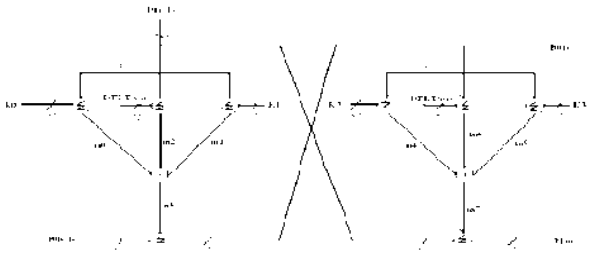

Figure 4. TEA encryption process

The single TEA round function performs the simple mixed orthogonal algebraic functions such as Right/Left shifts, Integer addition and exclusive – or operations. However, the mixing portion of TEA seems unbroken but related key attacks are possible, even though the construction of 232 texts under two related keys seems impractical is one of the weaknesses. The second failing is that the effective length of the keys is 126-bits not 128 does affect certain potential applications not the simple cipher decipher mode [6].

In [4] proposed Simeck solution is to design of Simon and Speck, and combine their components in order to get a new design of block cipher family, called Simeck. The round function and the key schedule algorithm follow the Feistel structure. Define rounds function is as the following:

$$R_{ki}(l_i;\ r_i) = (r_i \oplus f(l_i) \oplus k_i;\ l_i) \qquad (1)$$

where l_i and r_i are the two words for the internal state of Simeck, k_i is the round key, and define function f is as the following:

$$f(x) = (x \odot (x \lll 5)) \oplus (x \lll 1) \qquad (2)$$

A study in [1] proposed method of Encryption and Hash based Security in Internet of Things. The proposed algorithm takes a 64-bit binary plain text and a 128-bit master key as input. It has 32 rounds of operation. However, traditional cryptography does not fit well in IoT environment due to its constrained resources.

In [7] proposed method of an implementation of data encryption for internet of things using blowfish algorithm on FPGA. The basic idea for blowfish solution is reduced the number of rounds fiestel to 8 rounds and 4 rounds instead of 16 and The key size was changed from 448-bit to 384-bit, 320-bit, 256-bit, 192-bit, 128-bit and 64-bit.

However, traditional cryptography focus on the solutions in providing high levels of security, ignoring the requirements of constrained devices.
In [10] proposed method of Design and Implementation of Block Cipher in Hummingbird Algorithm over Spartan -2 FPGA. In this work, Block cipher encrypts 16-bit data blocks using 64-bit sub-key. The main idea of Hummingbird solution is used with a new Boolean function is derived for the S-box and Inverse S-boxes. However, in this architecture 64-bit sub-key is used which is too short. The

software performance is not good Wentao Zhang et el, [13].

In [2] proposed lightweight block cipher Simon and Speck to show optimal results in hardware and software respectively. Both ciphers offer a range of key size and width, but at least 22 numbers of rounds require performing sufficient encryption. Although the Simon is based on low multiplication complexity but the total number of required mathematical operation is quite high [11, 12].

In [3] proposed lightweight block cipher KTANTAN solution is susceptible to a class of meet-in-the-middle attacks. However, it is succeed in achieving a low area in hardware but the software performance is not good. For example, the permutation layer is extremely low-cost in hardware, but it is the true performance bottleneck for many software implementations Wentao et el, [13].

In [5] LED proposed at CHES'2011; the designers claim that LED is not only very compact in hardware but also maintains a reasonable performance profile for software implementation.

III. DISCUSSION

In related work, they discussed SIT solution. They concluded just five encryption rounds is used which is too few to presents substantial security in IoT environment. In SPN, do not a direct implementation of confusion and diffusion. In addition, Piccolo solution gives limitation for hardware implementation by Parallelism architecture. In Bluefish and Hash algorithm author, concluded traditional cryptography does not fit well in IoT environment due to its constrained resources. Also in Hummingbird and KTANTAN they concluded the software performance is not good. Based on related work, we observe many proposals algorithm present have some weaknesses. In addition, we concludes CLEFIA algorithm proposed better because potential solution for IoT environment. Especially, CLEFIA has attracted a lot of attention from cryptographic researchers due to its simplicity, impressive hardware performance and strong security.

IV. CONCLUSION

In this paper, we discussed more relevant and recent available solutions for security, privacy and we have presented some small cryptographic algorithms for IoT. Modified CLEFIA algorithm is proposed which uses the Linear Feedback Shift Register (LFSR) to overcome the security weakness of the original CLEFIA algorithm against attacks. We demonstrate proposed cryptosystem contributes to the network security on Internet of Things and very fast and useful scheme. We believe that CLEFIA algorithm should be considered to be implemented in the IoT.

V. REFERENCES

[1]. B.Vinayaga Sundaram, Ramnath.M, Prasanth.M and Varsha Sundaram.J, "Encryption and Hash based Security in Internet of Things" 3rd International Conference on Signal Processing Communication and Networking (ICSCN), IEEE, 2015, pp.1-6.

[2]. B. Ray, S. Douglas, S. Jason, T. Stefan, W. Bryan, and W. Louis,"The SIMON and SPECK Families of Lightweight Block Ciphers", Cryptology ePrint Archive, Report/404, 2014, pp.1-42.

[3]. Bogdanov, A. and Rechberger, C., "A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN" In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, Springer, 2011, pp. 229–240.

[4]. Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong, "The Simeck Family of Lightweight Block Ciphers" ,IACR, 2015, pp. 1-23.

[5]. Jian Guo, Thomas Peyrin, Axel Poschmann and Matt Robshaw, "The LED Block Cipher" In: Preneel, B., Takagi, T. (eds.): CHES 2011, LNCS 6917, vol. 6917, Springer, 2011, pp. 326–341.

[6]. Kiran Kumar.V.G, Sudesh Jeevan Mascarenhas, Sanath Kumar and Viven Rakesh J Pais, "Design And Implementation Of Tiny Encryption Algorithm", Int. Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 5, Issue 6, (Part -2), 2015, pp.94 97.

[7]. Kurniawan Nur Prasetyo ST., Yudha Purwanto, ST., MT. and Denny Darlis, S.Si., MT., "AN IMPLEMENTATION OF DATA ENCRYPTION FOR INTERNET OF THINGS USING BLOWFISH ALGORITHM ON FPGA", 2nd (ICoICT), IEEE, 2014 pp. 75-79.

[8]. Muhammad Usman, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan and Usman Ali Shahy, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017 , pp.402-411.

[9]. Rahiyanath T. Y., "A NOVEL ARCHITECTURE FOR LIGHTWEIGHT BLOCK CIPHER, PICCOLO", IJRET: International Journal of Research in Engineering and Technology, Volume: 04, Issue: 09, 2015, pp.97-103.

[10]. Shumit Saha, Md. Rashedul Islam, Habibur Rahman, Mehadi Hassan and A.B.M. Aowlad Hossain, "Design and Implementation of Block Cipher in Hummingbird Algorithm over FPGA", 5th ICCCNT, Hefei, China, IEEE – 33044, 2014, pp. 1-5.

[11]. S. Khan, M. S. Ibrahim, K. A. Khan, and M. Ebrahim, "Security Analysis of Secure Force Algorithm for Wireless Sensor Networks", arXiv preprint arXiv: 1509.00981, 2015, pp.1-7.

[12]. T. Mourouzis, G. Song, N. Courtois, and M. Christofii, "Advanced Differential Cryptanalysis of Reduced-Round SIMON64/128 Using Large Round Statistical Distinguishers", Cryptology ePrint Archive, Report/481, 2015 , pp. 1-9.

[13]. Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang and Ingrid Verbauwhede, "RECTANGLE: A Bit-slice Lightweight Block Cipher Suitable for Multiple Platforms", Vol. 58: 122103(15), 2015, pp. 1-22.

Cite this article as :

Nahla F. Osman, "Optimization of Security and Privacy- Preserving Data Using an IoT CLEFIA Based Security LFSR", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 375-379, May-June 2019.
Available at doi : https://doi.org/10.32628/CSEIT1953126
Journal URL : http://ijsrcseit.com/CSEIT1953126