European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 09 , 2020

PERFORMANCE ANALYSIS OF EELWE ALGORITHM USING MSEC METHOD

Radhika Rani Chintala[1], Narasinga Rao M R[2], Somu Venkateswarlu[3]
[1,2,3]Department of Computer Science and Engineering, KoneruLakshmaiah Education Foundation, Vaddeswaram, AP, India.

ABSTRACT:

Research in Human Sensor Networks (HSN) has become the primary topic, as there is significant development in Health and clinical care technologies. Lightweight encryption algorithms are utilized to guaranteeconfidentiality of the data that is communicated between sensors and servers. EELWE is a lightweight encryption algorithm that will consume less energy compared to the existing algorithms. A metric is needed toanalyze the performance of the lightweight encryption algorithms w.r.t various parameters of a cipher implementation. In this paper, a metric called MSEC (Metric for Security Vs Energy consumption) is used to measure the performance of light weight encryption algorithms. Results have proved that EELWE has exhibited better MSEC value compared to other algorithms.

Key Words: Data Confidentiality, Energy, EELWE, Performance, MSEC

1. INTRODUCTION

Monitoring humanhealth remotely has become simpler with the aide from sensors in HSN.Unlike generic WSNs, the sensors or devices in HSN are placed on or implanted inside human body, thus restricting the flexibility of regularly charging the device or replacing the energy source. The data collected by the sensors will be transferred to Health Care Monitoring system via wireless communication networks [1].This health data may be attacked by the intruder during communication. Therefore, HSN needs secure communicationwhilsttransmittingthe patient's sensitive data to servers.

It is vital to secure the data at Tier-1 device (sensor), client-side, before sending the data to backend of the cloud, which contains servers and databases [2]. If the start point was not protected, then this will leave a huge probability that anyone can obtain patients' data while transmission to a base station. So, even if there was a strong implementation of the architecture, it makes the architecture vulnerable to different attacks.

The algorithm used for security must also ensure the confidentiality, privacy, and integrity of the patient's data. After the encryption, the data will be transmitted to mobile phone, or any other mobile device (Tier-2 Device). EELWE algorithm will ensure secure data communication from sensor to mobile in HSN [3]. This covers the communication between Tier-1 and Tier-2 of the HSN as shown in Fig.1.

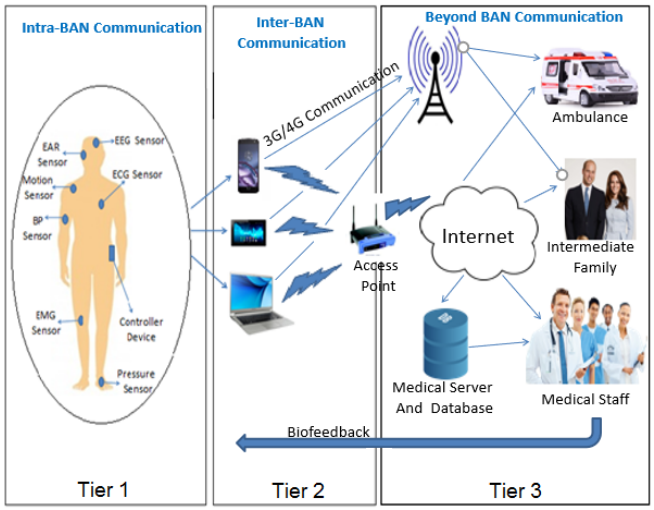

Fig.13-Tier Architecture of HSN [2]

The existing lightweight cryptographic algorithms like AES, HIGHT, IDEA, KLEIN, PRESENT, TEA, DES do not guarantee an optimal level of security in real time communication [4]. The energy consumption of EELWE is proved to be efficient compared to the above listed algorithms [3]. The focus of this paper is to analyze theperformance of an EELWE using the metric MSEC and is compared with existing algorithms.

2. LITERATURE SURVEY

Vast research was done on measuring the performance of lightweight encryption algorithms. Most of the researchers have considered the metrics such as code size, area, clock cycles for performing encryption and decryption operations for performance analysis. Some researchers focused only on security aspect in measuring the performance. They have not discussed about security metric w.r.t energy. Considering only the energy metrics or only the security aspects will notquantity the accurate performance of a lightweight encryption algorithm.

Deepti Sehrawat et al. [5] have analyzed various security attacks that can encounter on lightweight encryption algorithmsandtheir countermeasures were also discussed. Authors have clearly mentioned about various possible attacks based on the type of implementation: Software or Hardware. Most of the symmetric lightweight block ciphers are prone to brute force attacks.

Bassam Jamil Mohd et al. [6] proposed a performance metric to analyze lightweight encryption algorithm and applied it on Hight algorithm. The metric proposed is based on the area and energy parameters of an algorithm.

Chao Pei et al. [7] proposed a software performance metric which purely depends on the code size, block size and clock cycles needed for encryption and decryption operations. This metric is useful only for algorithms implemented in software and didn’t considered the security aspects.

Sohel Rana et al. [8] examined performance analysis of various lightweight encryption algorithms for different evaluation metrics like RAM size, Code size, Key size, count and RAM size.

Sooyeon Shin et al. [9] discussed about several benchmarking projects like ECRYPT II, eBACS, etc., that have been promoted to calculateperformance of the cryptographic primitives including lightweight block ciphers on different hardware or software platforms.ENCRYPT II measured performance considering code size, RAM use, cycle count in encryption and decryption, where eBACS measured the performance of various cryptographic primitiveson personal computers and servers taking the speed metric into consideration.

Deepti Sehrawat et al. [10] discussed about the available tools and parameters for measuring the performance evaluation of security algorithms. Authors have considered only the metrics for software implementation. Evaluation parameters considered are Code size, RAM usage, Cycle count in encryption, Cycle count in decryption, Energy consumed, and a combined metric which is given after the normalization.

3. EELWE ALGORITHM

The EELWE (Energy Efficient Lightweight Encryption) algorithm is implemented in three versions with different block sizes[2]. EELWE32 takes a block size of 32-bit, EELWE48 takes a block size of 48-bit and EELWE64 takes a block size of 64-bit. Though block size is being varied, a fixed 80-bit key is appliedto all the variants. An 80-bit is expanded using key scheduling process where each round takes two sub keys for a total of 254 rounds. EELWE is implemented in hardware using the Xilinx IDE platform. Step by step process of an algorithm is shown in Fig.2.

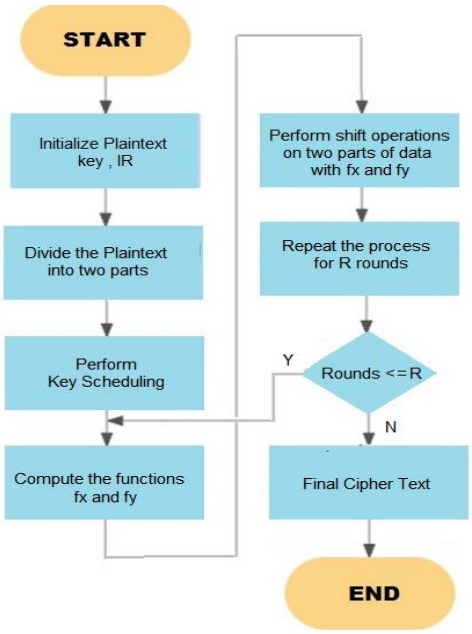

Fig.2Encryption process of EELWE [2]

The round function of EELWE32, where a 32-bit plaintext is divided into two parts P1 and P2, is discussed in the following steps:

1. P1 data is split up into 2 parts Pa(6-bits) and Pb(7-bits).
2. P2 data is split up into 2 parts Pc(8-bits) and Pd(11-bits).
3. The round function is applied on Pa and Pb using the below nonlinear functions.

$$Ta = (Pa[a1] \oplus Pa[a2]) \oplus kx$$

$$Tb = (Pb[b1] \& Pb[b2]) \oplus (Pb[b3] \& IR[i])$$

$$fx = Ta \oplus Tb$$

where ai indicates the bit positions of Pa,bi indicates the bit positions of Pb, andIR indicates irregular update rule.

4. Tc and Td is computed based on Pc and Pd using the following nonlinear functions.

$$Tc = (Pc[c1] \oplus Pc[c2]) \oplus ky$$

$$Td = (Pd[d1] \& Pd[d2]) \oplus (Pd[d3] \& Pd[d4])$$

$$fy = Tc \oplus Td$$

where ci indicates the bit positions of Pc, anddi indicates the bit positions of Pd.

5. P1 and P2 are updated by performing left shift operation with fy and fx respectively.

$$P1 = shl(P1, fy)$$
$$P2 = shl(P2, fx)$$

The above steps are repeated for 254 iterations and are performed for EELWE32, EELWE48 and EELWE64 based on the parameters shown in table1.

Table1. Parameters for different versions of EELWE

Parameters	**EELWE 32**	**EELWE48**	**EELWE64**
P1 (in bits)	13	19	27
P2 (in bits)	19	29	37
Pa (in bits)	6	8	10
Pb (in bits)	7	11	17
Pc (in bits)	8	12	14
Pd (in bits)	11	17	23
ai (bit positions of Pa)	5, 2	7, 3	9, 5
bi (bit positions of Pb)	6, 3, 1	10, 6, 4	16, 11, 7
ci (bit positions of Pc)	7, 3	11, 5	13, 7
di (bit positions of Pd)	10, 7, 5, 1	16, 12, 8, 3	22, 17, 11, 5
Round function per iteration	1 time	2 times	3 times

Energy consumption of an EELWE algorithm that is implemented in hardware is calculated using the metrics such as Time, Area and Power[11].

4. METHODOLOGY

Key length plays a significantrole in determining security level of a cipher[12]. It defines an upper bound for the effort required in exhaustive key search. If the key is recovered by an adversary, then the entire security of the communications will be compromised. The security level [13] of a cipher is specified as a known plaintext attack i.e., if an adversary has a pair of plain text along with its matching ciphertext, what is the effort to recover the key. For a γ-bit key, if the key recovery cannot be done in less effort than exhaustive key search, then γ will be the security level of a cipher. Thus, exhaustive search for γ bit keys will have to search through an average of $2^{\gamma-1}$ keys with the worst-case scenario of searching up to 2^{γ} keys.

For a processor with a capability of P Flops and an average of C cycles required to encrypt one block of data, then the no. of encryption operations(O) that can be carried out in M years using N systems can be calculated as:

$$O = (P / C) * 60 * 60 * 24 * 365 * M * N$$

Assuming the processor capability of 5.3 TFlops, an optimized energy is consumed by EELWE64 with 32 iterations taking an average of 9 cycles per block of encryption. Assuming the effective lifetime of a health-related data is around 100 years, number of encryption operations(O) that can be carried out in 100 years using 100 systems can be:

$$O = (5.3 * 10^{12} / 9) * 60 * 60 * 24 * 365 * 100 * 100$$
$$= 1.8571 * 10^{23}$$

$$= 2^{77.3}$$ (between 1 zettabyte(2^{70}) to 1 yottabyte(2^{80})

This means that an intruder should perform $2^{77.3}$ operations in order to break the algorithm. Based on this, an effective key length of 78 should be enough to secure data from an adversary. Since the key lengths are preferred to be powers of 2, an 80-bit key is recommended for EELWE algorithm.

As per the Moore's law [14], the cost of any fixed attack effort drops by a factor of 2 for every 18 months. So, to have same amount of protection once for every 18 months the level of security should be incremented by one, assuming the speed is not affected. Given a cipher with security level γ, the year Y(γ) till which the cipher will provide adequate protection is calculated as:

$$Y(\gamma) = \text{Proposed Year} + 3(\gamma - 56)/2$$

Though an 80-bit key is taken, the encryption procedure of EELWE includes key scheduling, where an 80-bit key is expanded to 254-bit key. Hence the γ value is equal to 254 for EELWE. The year till which the EELWE algorithm will provide an adequate protection can be calculated as:

$$Y(254) = 2020 + 3(254 - 56)/2$$
$$= 2317$$

From the above calculation, it is proved that EELWE algorithm is secured till the year 2317.

For applications like HSN's where the energy available is constrained, the desired property in the block ciphers is to offerhigh security with less energy consumption. The existing metrics however do not consider security as a parameter and energy consumption metric alone however will not reveal any information on the security being offered by the cipher. Hence, there must be a method to measure the trade-off between the security provided by a cipher and energy consumed, so as to maximize security gain. So, a metric called MSEC (Metric for Security v/s Energy Consumption) has been used to quantify the security v/s energy consumption trade-off for any cipher based on best attack the cipher can resist.

The MSEC value is calculated as:

MSEC = (No.of Secured years left) / (Normalized energy)

Where the normalized energy is the energy consumed by a EELWE cipher normalized w.r.t the energy consumed byother algorithm. EELWE has exhibited better MSEC value when normalized w.r.t to LBLOCK. The no. of secured years lefts can be calculated as:

No.of Secured Years left = Y(γ) – Current Year
No. of Secured years left for EELWE
= 2317 – 2020
= 297 years

MSEC(EELWE) = 297 / Normalized Energy
= 928.13

Table 2 : MSEC values of different algorithms

Algorithm	**Energy Consumption (µJ/byte)**	**MSEC Value**
AES-128	4.31	23.2
DES	21.8	-0.18
DESXL	24.15	7.78
HIGHT	5.37	19.37
IDEA	9.87	10.84
KLEIN-80	7.0	5.0
mCRYPTON-64	21.5	-0.09
PRESENT	0.292	116.44
PICCOLO-80	0.506	71.15
LBLOCK	0.125	264
LED-64	9.758	1.13
TEA	0.182	38.46
XTEA	0.258	403.1
SEA	0.376	146.28
EELWE	0.0406	928.13

5. RESULTS

The energy consumption of EELWE along with existing algorithms are shown in Fig.3. MSEC of different algorithms are shown in Table2 and resultant graph is shown in Fig.4. A larger metric value indicates better security v/s energy consumption trade-off while a negative metric value indicates that the cipher is no longer safe to use for current technology. Fig.5 depicts how the MSEC value is being affected w.r.t to the energy consumed by an encryption algorithm.

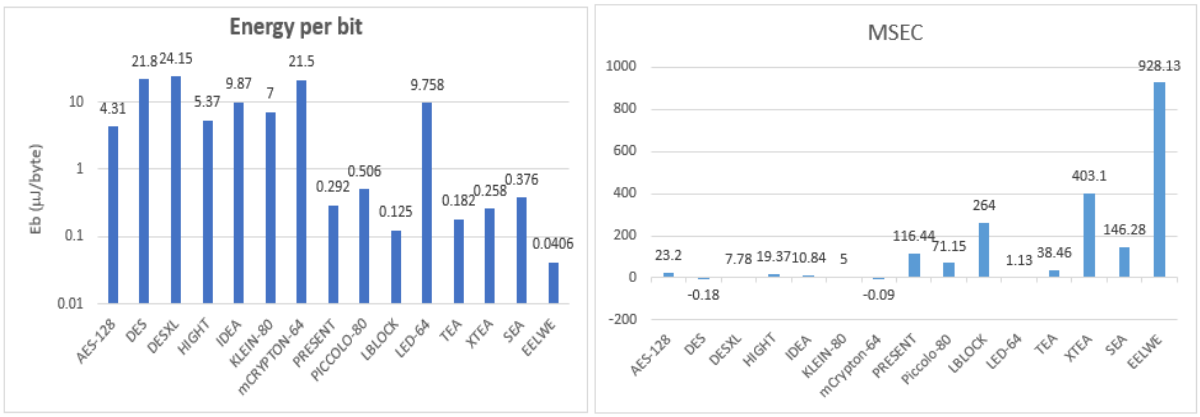

Figure 4: Energy Consumption of different algorithmsFigure 4: MSEC value of different algorithms

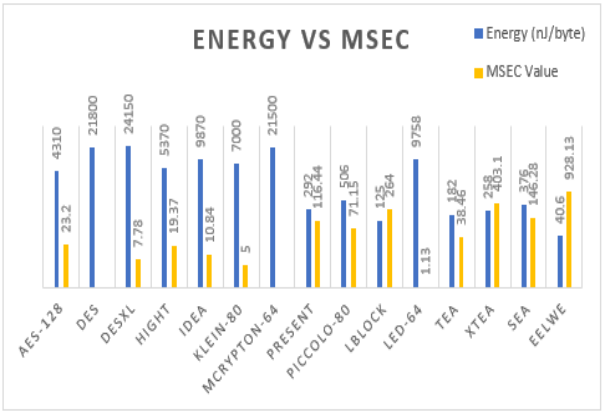

Figure 5: Energy Vs MSEC

6. CONCLUSION

For applications like HSNs where the energy availability is constrained, the desired property of a block cipher is to achieve more security at the cost of less energy. Most of the block ciphers are considered to be broken by the brute-force-like cryptanalysis. Based on the Moore's law, it is measured that EELWE is secured till the year 2317. The performance of an EELWE w.r.t security vs energy consumption is analyzed using the metric called MSEC. This metric value is inversely proportional to the energy consumed i.e.,lesser the energy consumption, greater will be metric value.EELWE has exhibited better MSEC value (928.13) compared to existing algorithms and it is concluded that EELWE algorithm will secure the data for greater number of years, before it can be broken.

REFERENCES

[1] Aminian, M., and H. Reza Naji. "A hospital healthcare monitoring system using wireless sensor networks.", Journal of. Health & Medical Informatics, Vol. 4, No.2, pp. 1-6, 2013.

[2] Radhika Rani Chintala, Narasinga Rao M R, Somu Venkateswarlu, "Review on the Security Issues in Human Sensor Networks for Healthcare Applications", International Journal of Engineering & Technology**,** vol. 7, no. 2.32, pp. 269-274, May 2018. ISSN 2227-524X.

[3] Radhika Rani Chintala, Narasinga Rao M R, Somu Venkateswarlu, "Modelling an Energy Efficient Lightweight Encryption Algorithm Suitable For Medical Applications", PONTE International Journal of Sciences and Research, Vol. 76, No. 9, pp. 109-121, Sep 2020, DOI: 10.21506/j.ponte.2020.9.8.

[4] Bassam J. Mohd, ThaierHayajneh, Athanasios V. Vasilakos, "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues", Journal of Network and Computer Applications, Vol 58, pp. 73-93, 2015, ISSN 1084-8045, https://doi.org/10.1016/j.jnca. 2015.09.001.

[5] Deepti Sehrawat, Nasib Singh Gill, "Analysis of security attacks on lightweight block ciphers and their countermeasures", Journal of Engineering and Applied Sciences, Vol. 13, No. 20, pp. 8439-8447, 2018.

[6] P. R Bassam Jamil Mohd, ThaierHayajneh, Zaid Abu Khalaf and Khalil Mustafa Ahmad Yousef, "Modeling and optimization of the lightweight HIGHT block cipher design with FPGA implementation", Security Comm. Networks, Vol. 9, pp 2200-2216, 2016.

[7] Chao Pei, YangXiao, WeiLiang, Xiaojia Han, "Trade-off of security and performance oflightweight block ciphers in Industrial WirelessSensor Networks", EURASIP Journal onWireless Communications and Networking, Vol. 117, pp. 2-18, 2018.

[8] Sohel Rana, Md. Anwar HussenWadud, Ali Azgar, Dr. Mohammod Abul Kashem, "A Survey Paper of Lightweight Block Ciphers Based on Their Different Design Architectures and Performance Metrics", International Journal of Computer Engineering and Information Technology, Vol. 11, No. 6, pp. 119-129, 2019.

[9] Sooyeon Shin, Minwoo Kim, Taekyoung Kwon, "Experimental performance analysis of lightweight block ciphers and message authentication codes for wireless sensor networks", International Journal of Distributed Sensor Networks, Vol. 13, No. 11, pp. 1-13, 2017.

[10] R. Sathish, R. Manikandan, S. Silvia Priscila, B. V. Sara and R. Mahaveerakannan, "A Report on the Impact of Information Technology and Social Media on Covid–19," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 224-230, doi: 10.1109/ICISS49785.2020.9316046.

[11] Deepti Sehrawat, Nasib Singh Gill, "A Review on Performance Evaluation Criteria and Tools for Lightweight Block Ciphers", International Journal of Advanced Trends in Computer Science and Engineering, Vol. 8, No. 3, pp. 630-639, 2019.

[12] Radhika Rani Chintala, Narasinga Rao M R, Somu Venkateswarlu, "Performance Metrics and Energy Evaluation of a Lightweight Block Cipher in Human Sensor Networks," International Journal of Advanced Trends in Computer Science and Engineering, Vol. 8, No.4, pp. 1487-1490, 2019.

[13] Alexander W. Dent, "Choosing key sizes for cryptography", in Information Security Technical Report, pp. 21-27, 2010.
[14] Manikandan, R and Dr.R.Latha (2017). "A literature survey of existing map matching algorithm for navigation technology. International journal of engineering sciences & research technology", 6(9), 326-331.Retrieved September 15, 2017.
[15] Arjen K. Lenstra, "Key Lengths", The Handbook of Information Security, 06/2004.
[16] Kaliski B., "Moore's Law. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security", Springer, Boston, MA. https:// doi.org/10.1007/978-1-4419-5906-5_420m, 2011.