ENHANCED TEXT DATA SECURITY USING PRESENT- IDL BLOCK CIPHER FOR INDUSTRIAL IOT (IIOT)

V. MUTHU GANESHAN
Research Scholar,
The Gandhigram Rural institute
(Deemed to be University),
Gandhigram, Dindigul.
muthuct8@gmail.com

S .SIVAGURUNATHAN
Assistant Professor,
The Gandhigram Rural institute
(Deemed to be University),
Gandhigram, Dindigul.
svgrnth@gmail.com

***Abstract*— Automation is an essential process in smart industry. Industry 4.0 is the evolution of smart industry, in which manufacturing with dynamic production plays a major role. Large numbers of products are manufactured with proper datasets. These datasets can be secured by various types of security algorithms. Light Weight Block Cipher (LWBC) is suitable for IIoT datasets with data generated from resource constrained devices. Various new ciphers are developed in LWBC. PRESENT algorithm is standardized as per cryptography metrics and the number of rounds is limited to 31. Latency time may be high. In this article, we have proposed PRESENT-IDL (identical) block cipher to minimum number of rounds with effective enhanced security to the dataset.**

Keywords — *Security, IDL Block Cipher, Industrial IOT.*

I. INTRODUCTION

IIoT is emerging in developing countries due to its effective manufacturing and production system. IIoT consists of IoT devices, hardware, software and network. Sensors fit on devices and work for which command is given by programmer. Sensors can acquire only low energy because of its characteristics. Sensors carry the data via signals and share with other devices for the process. Data must be secured from various types of attacks. Light Weighty Cryptography (LWC) is specially designed for low power constrained devices. Number of logic gates used in IIoT applications is called Gate Equivalence (GE). Radio Frequency Identification (RFID) has 200 to 2000 logic gates but only 20 to 200 logic gates are used in RFID for security purpose. The whole range of IoT devices are called GATE AREA (GA). We have to measure how many GEs are used in GA in an application. As per cryptographic classifications, LWC has Block Cipher, Stream Cipher, Hash function and Message Authentication Codes (MAC). Block cipher consists of plaintext converted to block of bits, stream cipher has of plaintext bits without block and hash function is a one-way function. After giving the plain text input it gives hexadecimal string output. MAC is used for authentication purpose. Based on these classifications, Block cipher has some classifications like Substitution Permutation Networks (SPN), Feistel Networks. Add-Rotate XOR (ARX), Non-Linear Feed Back Shift Register (NLFSR) method and hybrid block cipher method. SPN process a plaintext number

of rounds of substitutions and permutations. Feistel networks split the plain text block and apply the diffusion function and concatenate to next round. ARX is a combination of XOR operations. NLFSR processes the plaintext block of stream ciphers. Hybrid method consists of two or more cipher methods. PRESENT algorithm is a branch of SPN. PRESENT variations are I-PRESENTTM (innovative) and PRESENT- GRP (Grouping permutation of bits). Minimizing the number of rounds using substitution and permutation makes cipher text efficient.

This article includes Related Work in 2. Existing Method in 3. Proposed Method in 4. Results and Discussion in 5 and Conclusion in 6.

II. EXISTING SYSTEM

LWC comprises of the energy, power, cost and computations. LWC can be applied for low powered devices. Optimizing the computation gives highly efficient result.

PRESENT

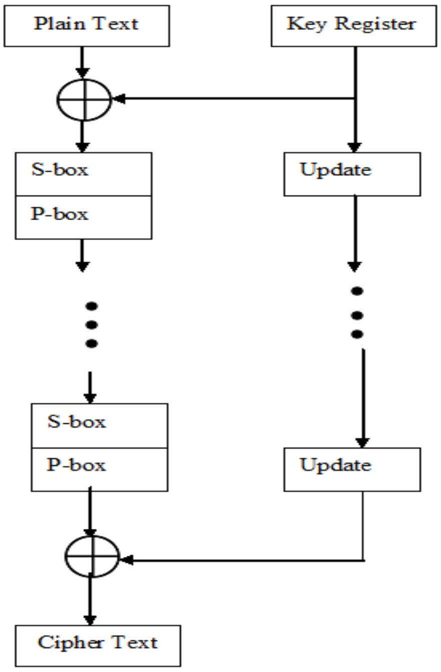


Fig 1. PRESENT

Algorithm Steps

```
generate Round keys()
for i=1 to 31 do
addRoundKey (STATE, Ki )
S-Box(STATE)
P-Box(STATE)
end for
addRoundKey(STATE,K32 )
```

PRESENT Algorithm shown in Fig.1 is a 64-bit plain text ex-or ed with key. S-box and P-box perform the operations on ex-or ed plaintext and key until 31 rounds. After all rounds key ex-or ed with final round of s-box and p-box and it gives a cipher text. All these rounds consist of linear bitwise permutation and nonlinear substitution techniques. Key size may be applied to 80 to 128 bits [6, 7, 8, 9 and 10].

I-PRESENT

Involution- PRESENT consists of 64-bit block and 30 times generated 64 bits of round keys. Master key schedules the keys. Here S-Box and P-Box are nonlinear mixing of the bits. It is also called as S-Transformation and P-Transformation. Decryption operation takes more time than encryption. Totally I-Present takes 30 Rounds. I-PRESENT variants are I- PREENT-80 and I-PRESENT-128. [11,12,13,14 and 15].

Algorithm

```
I-Present (State, Subkey) {
for (i=0;i<15;i++)
MixKey(state,subkey[i]);
STrans(state); PTrans(state);
}
Invo(state)
for (i=15; i<0;i--)
PTransInv(state), STransInv(state);
MixKey(state,subkey[i]);
}
}
```

Above mentioned I-Present algorithm has two parameters state and sub key. State is denoted as current value and sub key is denoted as current key for the round. Both are ex-or ed in mixkey function. STrans and Ptrans Substitution are denoted as Transformation and Permutation Transformation. State has 32 bits. It is divided into two 16 bits for PTrans and STrans in 4x4 bits ratio. Inov(state) prints cipher text and decryption process is done.

PRESENT – GRP

PRESENT with Group of bits Permutation (GRP) is an evolution from PRESENT and PRESENT variants. 128-bit keys are generated by this algorithm with unique keys for every round. A block contains 8 bits each. Sub sequent blocks are together paired. So, plaintext bits are calculated as 27=128 bits. P-Box and S-Box operations are performed on the subsequent pairs.

Algorithm

```
for (i=0;i<n;i++)
{
   for (j=0;j<p;j++)
   {
    for(k=0;k<c;k++)
    {
        Temp = x [(2*p*k) + j];
        x[(2*p*k) + j] = x[(2*p*k) + j + p]
        x[(2*p*k) + j + p] = Temp;
     }
   }
p/=2;
c*=2;
}
```

Above algorithm analyzed the time efficiency and number of rounds. PRESENT has 32 rounds, I-PRESENT has transformation and inverse transformation and takes more time to decryption and in PRESNET-GRP each round generates unique keys. These increase the latency time for data [16].

III. PROPOSED METHOD

PRESENT-IDL (identical) block cipher is shown in Fig 2 PRESENT-IDL is designed with 64-bit block plain text with 80-bit keys. Then Number of S-Box and P-Box rounds is six. Final round is ex-or ed with key with previous round of cipher text. Cipher text bits are negated, on the final round S- Box and P-Box. Now all bits are displayed as "0". Bits are identical in cipher text. Hash the cipher text for additional layer of security and we get hashed cipher text.

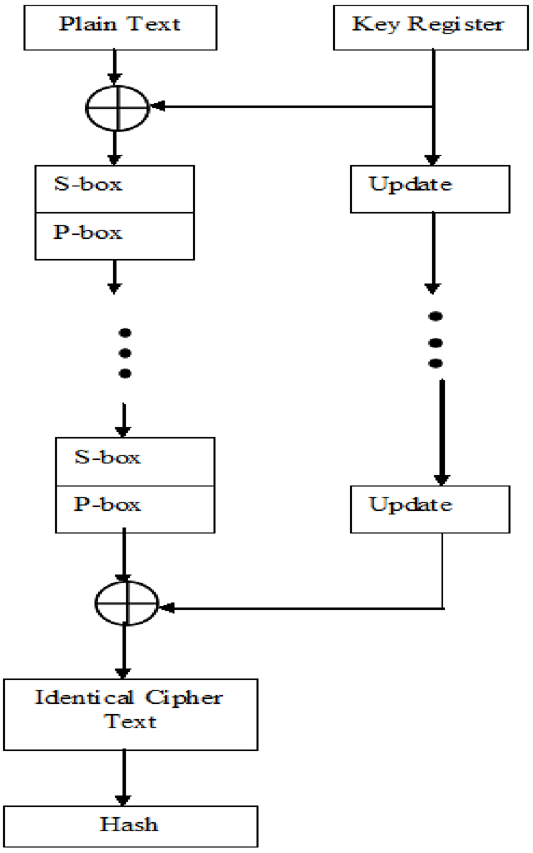


Fig 2. PRESENT-IDL

IV. RESULTS AND DISCUSSION

The results are simulated on Python 3.7 open source. and Raspberry Pi Emulator. This result shows the name of the algorithm, number of rounds applied on the algorithm, time variations and GE. Shown in table.3.1 number of rounds

TABLE 3.1
COMPARISON WITH PRESENT VARIATIONS

S. No	Name of Algorithm	Number Rounds	Encryption Time (in seconds)	Gate Equivalent (GE)
1	PRESENT	32	5.32	1570
2	I-PRESENT	31	3.12	1280
3	PRESENT-GRP	15	2.65	1215
4	PRESENT-IDL	6	1.32	917

Minimizing the number of rounds can be useful in time efficiency of encryption and decryption. Hence number of rounds must be optimized shown in fig 3.

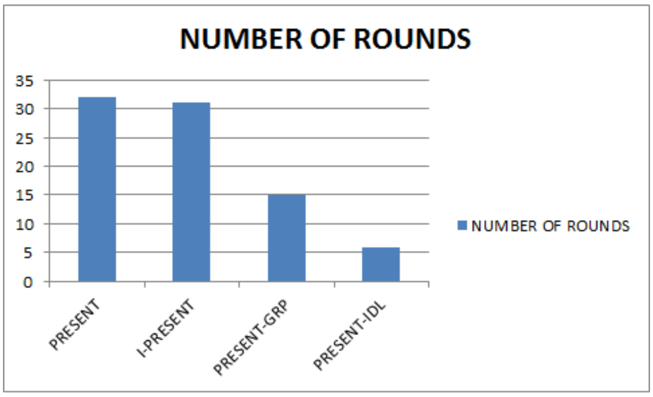
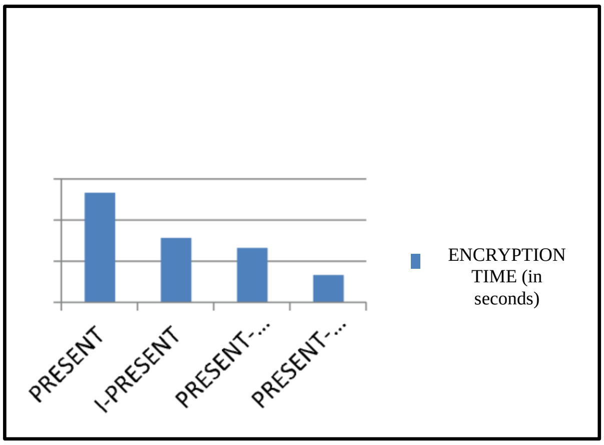


Fig 3. Number of Rounds Comparison

Encryption Time: -
Encryption and decryption time is optimized in PRESENT-IDL compared to other PRESENT variants, result shown in fig 4.



GE:
GE is totally minimized for effective data security in PRESENT-IDL. as shown in Fig 5.

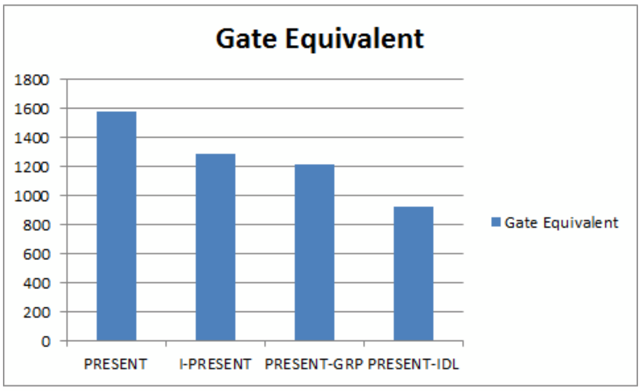


Fig 5: Number of Gate Equivalent

Discussion

This PRESENT-IDL is optimized with time efficiency in six rounds and encryption. Time is gradually decreased compared to other PRESENT variants. GE is also decreased. Minimum number GE gives a maximum efficiency to the algorithm.

V. CONCLUSION

This proposed PRESENT-IDL gives encryption time efficiency in minimum number of rounds and minimum number of GE. This algorithm can be applied to IoT applications and data security. This can be implemented with its PRESENT variations. It can give efficient security compare to other variations.

References

[1] Edwar Jacinto G, Holman Montiel A, Fernando Martinez S Implementation of the cryptographic algorithm present in different microcontroller type embedded software platforms", International Journal of Applied Engineering Research, Research India Publications, 2017.

[2] Nayeemudin, S. Zahoor-ul-Haq, K.V. Rameswara Reddy, P.Penchala Prasad "IoT Based Real Time Health Care Monitoring System using Lab View ", International Journal of Recent Technology and Engineering, .2019

[3] Koen Tange, Michele De Donno, Xenofon Fafoutis, Nicola Dragoni "Towards a systematic Survey of Industrial IoT Security Requirements:Research Method and Quantative Analysis", ACM, 2019.

[4] Keke Gai,Meikang Qiu "Blend Arithmetic operations on Tensor-Based Fully Homomorphic Encryption over real numbers", IEEE Transactions on industrial informatics,IEEE, 2017.

[5] Gregory Falco, Carlos Caldera, Howard Shrobe "IIoT Cyber Security Risk Modeling for SCADA Systems", Internet of Things Journal, IEEE,2018.

[6] A.Bogdanov, L.R Knudsen, G.Leander, C.Paar, A.Poschmann, Robshaw, Seurin, Vikkelsoe "PRESENT- An Ultra Light Weight Block Cipher",Springer, 2007.

[7] Amin Azmoodeh, Ali Dehghantanha, Kim kwang Raymond choo "Robust Malware Detection for Internet of (battlefield) Things Devices Using Deep Eigen space learning", sustainable Computing, IEEE, 2018.

[8] Debiao He, Mimi ha, Sherali Zeadally, Neeraj Kumar, Kaitai Liang Certificate less public key authenticated encryption with keyword search for Industrial Internet of Things",Industrial Informatics, IEEE, 2017.

[9] Jian Shen, Tianqui Zhou, xingang Liu,Yao Chung chang "A Novel Latin Square-Based Secret Sharing for M2M Communications", Industrial Informatics, IEEE, 2015.

[10] George Hatzivasilis, Konstantinos Fysarakis, Ioannis Papaefstathiou, charalampos manifavas, “A Review of lightweight block ciphers”

[11] Muhammed Reza z’aba, Norziana Jamil, Mohd Ezanee Rush, Md. Zaini Jamaludin, Ahamed Azhan Mohd Yasir “I-PRSENTTM : involutive Lightweight Block Cipher ”,Journal of Information Security, 2014.

[12] Hui Cui, Robert H.Deng, Joseph K.Liu, Xun Yi, Yingjiu Li “ServerAided Attribute-based signature with revocation for resource constrained industrial internet of things”, Industrial Informatics, IEEE, 2018.

[13] Gokai Saldamli, Levent Ertaul, Asharani Shankaralingappa “Analysis of Lightweight message Authentication codes for IoT Environments”, International Conference on Fog and Mobile edge Computing, IEEE, 2019.

[14] Mohamed H. Eldefrawy, Nuno Pereira, Mikael Gidlund, “Key Distribution protocol for Industrial internet of things without implicit certificates”, Internet of Things, IEEE,2018.

[15] Peng Xu, Shauanghong He, Wei Wang, Willy Susilo, Hai Jin “Lightweight Searchable public-key encryption for cloud assisted wireless sensor networks”,Industrial informatics, IEEE, 2017.

Gaurav Bansod, Nishchal Raval, Narayan Pisharoty “Implementation of new Lightweight encryption design for embedded security”,Information forensics and security, IEEE, 2015.