# Enhanced Algorithm Implementation for Low Powered IoT Devices using Authenticator to Improve Data Integrity

Sheeba DM
*Research Scholar*
VISTAS, Chennai, INDIA
sheebadm@gmail.com

Dr. S. Jayalakshmi
*Dept of Computer Applications*
VISTAS, Chennai, INDIA
jai.scs@velsuniv.ac.in

***Abstract*—Internet of Things enables many industries to connect to end customers and provide seamless products and services delivery. Due to easy access to network, availability of devices, penetration of IoT services exponentially Growing. Meanwhile, Ensuring the Data Security and Integrity of devices connected to network is paramount. In this work, we bring the efficient way of implementing Secure Algorithm for low powered devices and enhancing the encryption and decryption process. In addition to the data security, to enhance node integrity with less power, Authenticator and intermediate network manager introduced which will acts as a firewall and manager of data flow. To demonstrate the approach, same is implemented using low cost Arduino Uno, Raspberry Pi boards. Arduino Uno used to demonstrate low powered encryption process using EDIA Algorithm and raspberry pi used as nodal manager to manage the integrity of nodes in a low-powered environment. Data Security and Integrity is ensured by the way of enhanced Algorithm and Integrity through BlockChain and results are provided and discussed. Finally result and future enhancement are explained.**

***Keywords—IoT Security, Data Integrity, Low powered IoT Devices, Lightweight Algorithm for IoT***

## I. INTRODUCTION

The Internet of Things (IoT) is rapidly growing in practical usage and industrial purpose in current information era. The increase of Things is rapid and ever growing in the field of research community since it received major attention by providing ease of use and convenience in day to day life [1]. Internet of Things is objects which can process information using sensors and communicate the same to other devices connected to internet. Since access to internet connectivity is increased and also cost associated with it is low; the number of devices or things connected to internet is ever increasing. So these factors enable real growth for IoT [2]. Everyone is interested in IoT and willing to access the sensors or gadgets from around the world 24*7; this necessitates the need of information security, data protection in the IoT devices to be more stringent [3]. IoT devices are attached to physical devices or components where it is enabled to send real time data to IoT data platforms, which will intern analyze, understand, and provide real-time decisions based on rules configured in it. IoT platforms are cloud enabled and got large processing power and can interact with thousands of sensors and gadgets and provide secure communications protocols on top of existing mobile network, internet or wireless connections. By the way of enabling existing computing devices through internet, we also need to ensure the privacy concerns, data theft and information security in IoT platforms and devices.

In order to provide the safe communication medium and robust security platform, need of the hour is to maximize information security controls and data encryption standards [4].

### *A. Overview of IoT Applications:*

Recent year's, number of IoT devices connected to internet is increasing in steady manner. This includes Smart Homes, Door Locks, Temperature control, Refrigerator, Air conditioner, Television etc [5]. Each of the devices connected to Internet constantly sends or receive real-time data using sensors. An estimate on the number of connected devices says there will be more than 50 billion nodes by 2020 and we crossed all of the estimates and rapidly connected devices are growing [6].

IoT Application development and implementation is taking central stage during this decade, where each of the electronic equipment is embedded with the sensors and ability to communicate with internet or local wireless modems [7]. Hospital management and patient care is improved through real-time data capture and communicating over the internet to regularly monitor the health status rather waiting for periodic health checks. [8]. Availability of broadband or mobile network and cost of getting the devices increased the IoT usage in Home and industrial sector [10].

Following are the sectors in which IoT applications are adapted to improve the customer experience. Wearable's – To monitor heart beat, calorie spent etc., Health – To monitor high-risk patients, Traffic Monitoring – Live traffic movement, accident tracking etc., Fleet Management – Monitoring Geo location, Performance analysis, identification of best routes etc., Agriculture – To monitor soil moisture, Level of acidity, Acidity etc., Smart Grid Energy saving - Use of Intelligent energy meters [11 -16].

Given that rate of adaptation of IoT is very high and rapidly growing, Internet of Things should also provide adequate security measures within it to ensure the information security, data protection and fraud detection so that best advantage of IoT can be used without any harm[17].

*B. IoT Security Threats:*

In order to widely engage industry patrons and research community in IoT applications, It should have enough checks and balances in terms of ensuring data security, improved privacy controls. If not then it might cause threat to the data integrity. Basically due to limited bandwidth, low processing power and easy to access physical hardware possess high security threat to IoT applications and it might cause damage to industry, economy and serious privacy concern [18-21].

IoT devices are prone to security attacks since physical hardware devices are small in size and not supervised always. So it becomes more difficult to control the external environment [22]. IoT devices are powered by small power sources and computationally inexpensive, this enables attackers over wireless medium or physical damaging of the IoT nodes. In order to provide wide range of security measures, we need to ensure privacy concerns and data security are addressed through efficient algorithm so that no data leak happens from the device [23]. Existing algorithms which are widely used may not provide appropriate efficiency due to limitations in computational resources and energy requirement where IoT devices are not equipped to handle large algorithms with less power.

IoT data is used in decision making, reporting and to connect to downstream systems. Mostly devices and sensors actively utilized for monitoring from environments. Data manipulation and protection is the essential part of providing IoT services, In order to accomplish the same we use the secure algorithms and IoT platforms [24].

The architecture of any IoT device or gadget is having 3 layers in common,
Hardware / physical components

1. Interfacing sensors to get the environment data around the device
2. Presentation layer which is responsible for display the results to the consumer or to interconnected devices.

Hardware components include Sensors – Optical, Proximity, Velocity / displacement, Temperature, Moisture, Acoustic, Flow, Chemical / Gas etc., some of the components which are actively monitor the environment and provide signal to the IoT platform[25]. Although IoT devices are enabled with the computational power, it cannot process large amount of data or processes to interpret and provide meaningful information. So IoT devices need an additional layer to handle the received data from actual devices.

In order to sense and communicate the required data out of IoT device, every device has a interpretation layer where it can sense and capture required data in compatible layout either in xml, json, comma separated format. Captured information then encrypted using the algorithm which ensures the data security and integrity from each node [26].

Data confidentiality plays a major role in any system where customer data or real-time feeds are communicated [27]. To provide secure communication channel, data is encrypted and hidden from adversaries, the same approach is adapted in IoT data exchange to ensure privacy. Since IoT devices contains small peripherals and might be unmonitored for a long period of days, this prone to data theft and physical attacks where attackers can have access to memory of the device and can retrieve the data. So strong data encryption and key expansion to be highly secure and cannot be retrieved at ease [28].

To safeguard the IoT devices from network attacks, data theft and ensure data integrity, there are several algorithms proposed and implemented in IoT nodes like RC6, LEA, AES etc., but when the IoT devices are power constrained and has less computational capacity, we need a better algorithm with less number of rounds and higher encryption rates[29]. Also to ensure data integrity, message channel between IoT device and IoT platform should be more secure and cannot be interrupted through any attack [30-35].

*C. Need for Enhanced Algorithm & Data Integrity*

IoT attacks are increasing by two-third in recent days and as per SonicWall report, during 2019-2020 IoT attacks grew by 66% and In 2020 number of attacks increased from 34.3 to 56.9 million attacks [36]. Attack on IoT devices are categorized into man-in-the-middle attack when someone interfering in existing communication protocol, physical attack by capturing hardware memory, denial of service attack where services are temporarily disconnected with malware [37].

Data Encryption assists in effective way of converting the plain text to cipher text and reduce the possibility of data theft but there are still inefficiencies in the existing algorithms where it cannot cater to less powered and low computational IoT gadgets[38]. So to provide better way of protecting the gadgets and devices from the known attacks and safeguard data from intruders, Enhanced version of IoT algorithm proposed and new architecture proposed to connect the IoT devices to the high computational devices using BlockChain. Improved algorithm helps in faster encryption and communication to nodal manager, where nodal manager is responsible for protecting the IoT nodes from external interferences and attacks by utilizing the BlockChain to mint the data to the blocks [39].

This paper enumerates the Enhanced Algorithm for Less powered and computationally weak IoT devices and which can be connected to a node manager within the premises where IoT devices and gadgets are implemented and also provides a new Architecture to introduce the BlockChain in Node manager to address data integrity and IoT device integrity within the network [42]. Below is the structure of rest of this paper; Brief literature survey of Algorithms and usage of Authenticator is discussed in Section II, Enhanced IoT algorithm design and architecture, Effective use of Lightweight BlockChain in

IoT devices, Integrating IoT devices with the node manager and managing the IoT network is discussed in Section III, finally results and evaluation is done in Section IV then conclusion, future work is detailed in Section V.

## II. IoT Algorithms and Blockchain :

Lightweight cryptography and its necessity are explained in [43-46] and it provides the drawbacks of existing algorithms in case of low powered and resource constrained devices. If any node present on the network is attacked and gained control, then whole IoT network is vulnerable to the series of attacks [47]. So it suggests block ciphers are possible alternatives to enable constrained devices through secure mediums.

Crypto analysis attacks like linear, differential are impossible in Feistel cipher based on algorithm LBlock. It is enabled with confusion layers of function S-Box and 4 bit confusion and diffusion. All of the features are defined through plaintext of 64 bit long input and cipher key of 80 bits [48]. With block size 64 bits and 80, 128 bit long keys, PRESENT algorithm is Substitution–permutation block cipher mechanism where about 31 XOR is performed on the round keys. Again similar to LBlock, S-Box function with single 4 bits used in 16 cycles. This is likely to fail for side channel and invasive hardware attacks [49].

MCrypton is a 64 bit block cipher with 64/96/128 key length options. It is based on the Crypton architecture and limited version of the functions is implemented for the power constrained devices. R-function is used to transform the 4 bits of input through substitution and permutation [50-55]. Encryption process involves key generation through s-box and constant rotation of bits using the matrix. There is a possible MITM attack in small IoT nodes.

SIMON algorithm proposed by NSA is hardware optimized implementation; it is a Feistel structure and provides facility for variety of devices [56]. Block size and key length are defined as n and 2n respectively. Maximum block size recommended by SIMON is 128 bits and it is strongly alternative for AES. It is flexible to be implemented in any IoT boards and gadgets without any issues in hardware compatibility [57]. LILLIPUT algorithm provides optimized block cipher where block size is 64 bit and key length 80 bits. It is implemented using S-Box approach similar to PRESENT and key generation sequence is of DES. Each round function is done at 1 byte [58].

KLEIN block cipher is based on SP network and provides 64 bit blocks and key length varies from 64 – 96 bits. Authentication of Messages and Hash values are used in this and keys are not constant, Keys are dynamically interchanged with set of predefined values. Related key attacks and for 64 bit, key recovery attacks is possible [59].

Mica2 platform is used to implement the following algorithms and find the effectiveness of Block Cipher. They are RC5, TEA and XXTEA [60-63]; and found that these algorithms are consuming more energy and initial key recovery can be achieved when rounds are increased and key frequently altered for the given device. So Literature survey shows that many of the algorithms are providing efficient way of protecting the plain text while securing communication between IoT nodes, but when it comes to Data Integrity many algorithms failed to provide enough measures [64]. So we bring the lightweight block chain possibilities in the IoT environment to ensure that data Integrity provided within every node and every communication happens in IoT platforms [65].

Ali and team proposed the SmartHome setup where the IoT nodes can be organized in a private network and high computational device within the node acts as a node manager and provides the Authentication, Routing of packets in case if more traffic within the network and it can mint, indexed itself in a BlockChain within the SmartHome setup. Lei explained about BlockChain architecture for Vehicle communication, where whenever a vehicle moves to a new area, Details about the vehicle and its key parameters are communicated to available heterogeneous BlockChain cluster [66]. This will provide real-time movement of vehicles with key parameters for any regulators or vehicle tracking communities whoever interested in the data about vehicle. Also it reduces the payload encryption and decryption through gateway in order to send or receive over a mobile networks and it addresses the security concerns available on legacy mechanism of sending the data to nodes.

Agriculture Supply chain presented by Tian and team where the IoT nodes are integrated together to get the data either through RFID sensors or other sensing objects. Data captured is handled through the BlockChain [67]. Data availability ensured over transparent mechanism of Blocks where anyone interested in the data can access in the BlockChain network without any data authorization or Integrity issues. This also reduces the food wastage and on time planned availability of food materials through supply chain and BlockChain.

## III. Enhanced IoT Algorithm Design and Architecture

Enhanced algorithm (*EDIA* Enhanced Algorithm for Data Integrity and Authentication) for IoT devices utilizes widely used Substitution Permutation network and Feistel Cipher [68-69]. This is a dynamic algorithm where properties of both the SP and Feistel together brought in to improve the security of IoT nodes in a lesser number of encryption rounds compared to existing available algorithms where it ranges from 20 to 64 rounds based on size of the key[70]. IoT nodes are constrained on resources and power so bringing down encryption iterations to minimal with higher complex key generation ensures a better cipher text out in a controlled environment. Well known algorithms of Block Cipher substitution permutation network and Feistel Architecture as well, below is the list of widely used in IoT devices and Gadgets.

| *SP Network* | *Feistel Architecture* |
|---|---|
| AES [46] | DES [61] |
| 3Way [52] | Blowfish [59] |
| PRESENT [54] | SF [58] |
| SHARK [56] | Camelia [60] |
| SAFER [55] | LWE [60] |

*Tab 1: Block Cipher Categories*

Advantage of using the Feistel over the SP network as in AES, is to reduce the complexity of implementing the encryption, decryption on a separate processes [41]. On other hand we have very similar process of generating cipher text $C_t$ and back to plain text $P_t$.

EDIA is 64 bit symmetric key block cipher where both the key and plain text are in same length and encrypted using ***n*** number of times based on complexity requirements of the system. Encryption process involves both bit shuffling and key shuffling, both is combined in order to bring a better results in the power constrained nodes of IoT. It is proposed to use 5 rounds of encryption process using the key length of 16 bits of 64 bit original key [40]. To eliminate key searching attacks, 64 bit key plays a major role here because doing a $2^t$ number of iterations is more complex and retrieval of key is made more complex.

| *Key – Configuration* | *Example* |
|---|---|
| Firmware ID | ADZ23CXRFVCV |
| Current Date Timestamp | 20201020 11:10:20 |
| Version ID | 1.1 |
| Checksum | A0 (A-Z,0-9) |

*Tab 2: Key Configuration*

The key is formatted based on predefined sequence of fields as in Table 2 and based on the checksum generated out of the current timestamp and firmware ID defined in the system. Checksum logic is determined for each of the IoT node or gadget such a way that only the sender and receiver agree to it. In case of any error in the key configuration checksum or timestamp generation, this will lead to mismatch in key expansion block of the algorithm. In order to make the key search as, much difficult as possible, Complexity of the process is

*KeyConfig =C ( K ( FirmwareID, Time, Version), FuncKey )*

| | |
|---|---|
| *C* | *CheckSum Function* |
| *K* | *KeyGeneration Function* |
| *FuncKey* | *Encryption - E / Decryption - D* |

The resultant 64 bit key is not a plaintext or some default key provided by the IoT device, but combination of functions provides more complexity to key generation and expansion. Complexity of the key is ensured by 4 key values and also by the checksum logic implemented to generate 2 byte validator. Along with these predefined checks, we have 5 keys part of the key expansion and it also provides additional security measure based on earlier configured keys [71-74]. To reduce the processing complexity of the IoT node based on its ability, we can get the key generated by the node manager in the network and utilize in the node.

*A. Key Schedule / Expansion:*

*EDIA* algorithm uses 64bits key in mathematical functions to get the four 16 bits round keys (Kr). Each key is used in the Encryption rounds where sub key taken and substitution, permutation is continuously done on the input plain text in order to receive the cipher text out of encryption process. Every round is responsible to get as much as possible confusion and diffusion. *EDIA* is architecture to take key input from key configuration section and it has Bit Randomizar, Confusion and Diffusion function and MasterKey Generator. All of these ensures key complexity and attackers cannot retrieve the original key or sub keys.

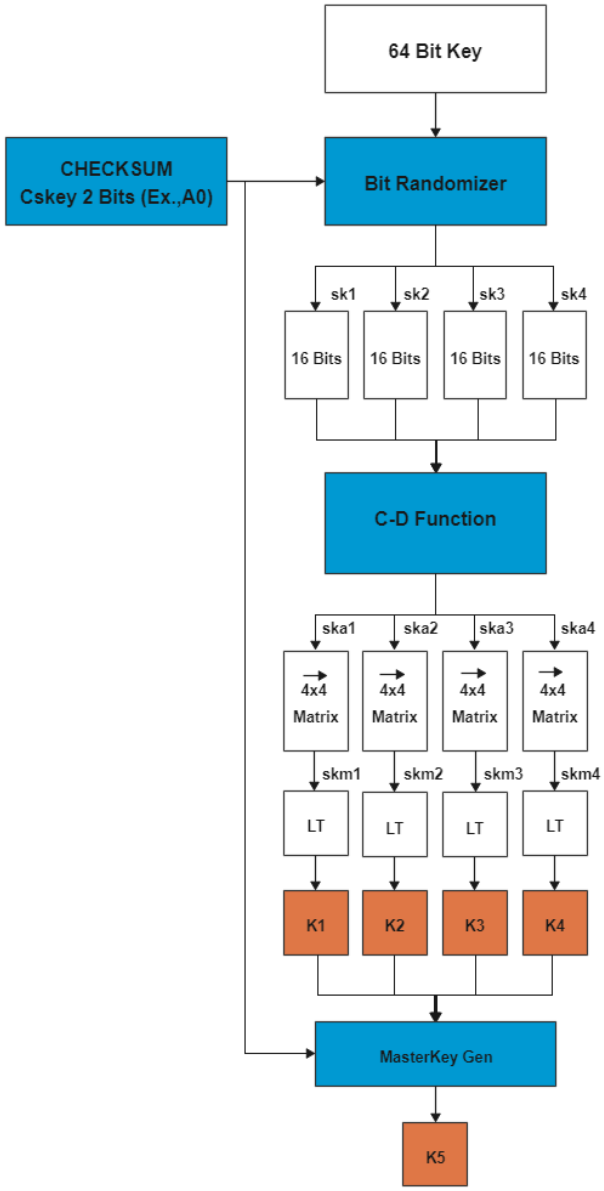


***Fig.1. Key Expansion Process***

*Bit Randomizer:* The purpose of it is to randomize the bits from main key to 4 * 16 bits sub keys (sk1, sk2, sk3, sk4) where every key is combination of 4 * 4 bits from the key configuration. 64 bits key is divided into 16 bits of interim keys based on the first Checksum bit provided.

| ***Bit Randomizer – Key text 1st Randomization*** |
|---|
| 1. Input: 64 Bits Key (Kp) using Firmware, Tstamp, Ver, Checksum |
| 2. Output: 4 * 16 Bits Sub Keys |
| 3. P_Array[16] = Key |
| 4. Get the first bit of Checksum(1:1) |
| 5. IF Csum = = Alphabet Sequence → Randomize |
| 6. A-G → Randomize (P_Array[1, 5, 9, 13]) |
| 7. H-N → Randomize (P_Array[16, 12, 8, 4]) |
| 8. O-T → Randomize (P_Array[2, 6, 10, 14]) |
| 9. U-Z → Randomize (P_Array[3, 7, 11, 15]) |
| 10. Repeat Step 6 to Step 9. END |

*Tab 3: Bit Randomizer Method*

*C-D Function:* Confusion and Diffusion methodology used to shuffle the bits based on the predefined bits shuffling tables. Both C & D Tables includes the bits as Cipher Keys.

| **$K_c$ Cipher Key** | **C Transformation** | **D Transformation** |
|---|---|---|
| **0** | E | 6 |
| **1** | 3 | 1 |
| **2** | A | B |
| **3** | 9 | 5 |
| **4** | F | 0 |
| **5** | 2 | E |
| **6** | C | 3 |
| **7** | 8 | A |
| **8** | D | 9 |
| **9** | 7 | F |
| **A** | 4 | 4 |
| **B** | 6 | 2 |
| **C** | 1 | C |
| **D** | B | 8 |
| **E** | 5 | D |
| **F** | 0 | 7 |

*Tab 4: C – D Function Transformation*

The C-D Function produces the Four 4*4 matrices $sk_{m1}$, $sk_{m2}$, $sk_{m3}$, $sk_{m4}$ are the matrices based on C & D Transform which will have the better complexity and followed by arrangements of bits such a way that finally we will get four keys ( $K_r$).

*MasterKey Gen:* It combines the $4*K_r$ and does a XOR operation on it and it includes the second bit of checksum introduced at first key configuration. It brings 3rd level of complexity to a key expansion.

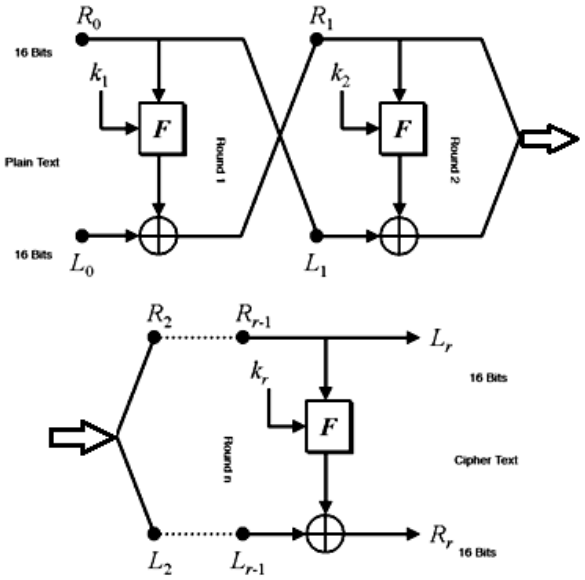


*Fig.2. Encryption Process*

*B. Encryption Process:*

Fiestel structure follows same rounds and process of encryption and decryption, below is the representation where it works on 16bits data of 4 blocks.

Encryption is done on each of 16 bits block on the input plain text $P_t$ and $C_t$ is generated at the end of each round. EDIA algorithm follows 5 rounds of encryption process where each 16 bit data is taken as input and bits are continuously altered to bring complexity in cipher text. $K_{1\text{-}5}$ are generated out of expansion is used at every round and XNOR operation and C-D confusion and Diffusion function done on the overlapped texts.

$L_o$ and $R_o$ are passed through C-D Function and utilizes C, D Transformations, also final key values are as below

$$C_t = L_{r1} + R_{r1} + L_{r2} + R_{r2}$$

The complexity of the cipher text is improved through key shuffling. Checksum of the key configuration, MasterKey Gen function where again checksum bit is included as the additional factor. So all of these increases the complexity and reduces the possibility of key searching attacks.

*C. Lightweight Blockchain for IoT devices*

BlockChain was developed and used predominantly in Financial Institutions and Bitcoin is the famous Implementation, followed by Cryptocurrency .BlockChain uses a Distributed Ledger to store the data in secure manner[75]. Addition of data is restricted through solving

complex computational puzzle. By the way of distributing the data, Attackers cannot get or tamper with the instance of data available on any network since all other nodes will not recognize the node as and when it find the discrepancy in the data.

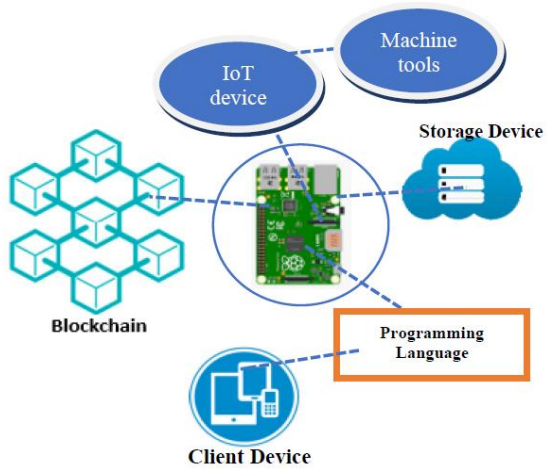


*Fig.3. Block Chain Implementation*

BlockChain Implementation in a Raspberry Pi is discussed by E Fernando, Where Ethereum Implementation is detailed and executed as a node. We propose to use the same architecture in Raspberry Pi and bring Arduino Board nodes to the network as an additional mechanism to ensure the authenticity of nodes in an IoT network[76].

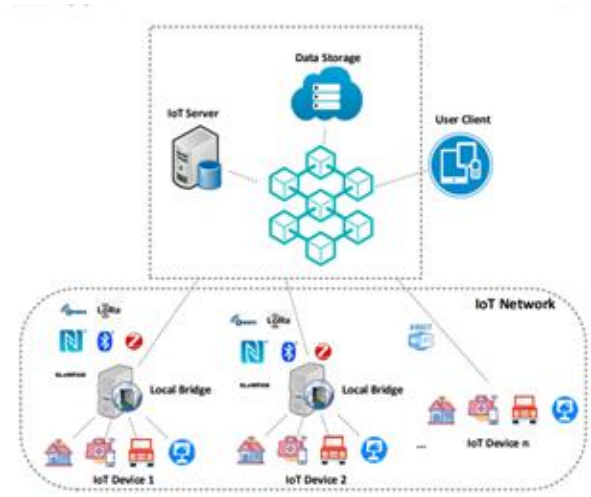


*Fig.4. Block Chain & IoT Integration*

The proposed method is to use the BlockChain in Raspberry Pi and connect the IoT nodes to a Authenticator node which will ensure that all the request and response are only from the Authenticated nodes of a private IoT network; This will ensure no other node is able to send requests to the IoT platform which saves the data in cloud or in-premise data store [77].

The Authenticator sequence is listed as a pseudo-code below which will ensure the node authenticity.

| ***IoT Node Authenticator*** | |
|---|---|
| 1. | Input: Request to add the data and Resources to Blocks |
| 2. | Output: Pass / Fail |
| 3. | Validate the Checksum and Node Physical ID |
| 4. | Solve the Node_Problem() using the Checksum |
| 5. | IF Node_Problem() = = 'Pass' |
| 6. | Access to Requested Resources |
| 7. | ELSE |
| 8. | Add the node to Review_List() |
| 9. | Send the Dummy Simulated_Response() |
| 10. | Casecade the Info to all Node Managers |
| 11. | Increase the RiskID of adjacent nodes |
| 12. | END-IF |
| 13. | Respond to the Node Request |
| 14. | Initiate the Validate Review_List Task |

*Tab 5: Authenticator Logic*

The IoT nodes are constantly send the requests to the nodal manager for any request or data addition to the IoT Platform, since all of the nodes are separated in a private network, communication to public networks are limited and ensuring the data integrity and node authorization This provides an increased workload but in order to protect the data and ensure privacy, This additional workload can be managed by a physical Hardware.

## IV. EVALUATION AND RESULTS

To evaluate the *EDIA* algorithm in any IoT device, following are the parameters which are important to be considered. Resource utilization, Average Execution Time, Maximum Power utilization, Key Complexity, Time for Encryption and Decryption using given number of rounds, Key Sensitivity for the input key.

In order to evaluate each of the parameters, Algorithm is compared with the most widely evaluated algorithms and its parameters. The resource utilization is the memory should be available for the algorithm to perform computation on the plain text and when number of rounds are increased, then any IoT device cannot hold to it if memory utilization is high, So ensuring the optimal memory utilization for the operation is necessary.

Average rounds and the time taken to genrate plain text to cipher and vice versa limits the power of the any IoT device and also limits other functions of power constrained devices so this also plays a role while evaluation algorithm for suitability. Key Search attack provides the ability to attacker to get the key and change the cipher text, sensitivity for wrong key should be high and attakers should not able to retrieve the plain text.

In order to evaluate the performance of the algorithm, It is executed in ATMega 328 Arduino board which provides ability to run the code and also input ports to receive external data as well. The execution time for encryption is 0.195 milliseconds and decryption 0.190 milliseconds. Memory utilization of algorithm while cipher text generation is 30 bytes. The results are compared to other algorithms below

| *Algorithm* | *Hardware* | *Block* | *Key Length* | *Lines* | *Memory* | *Encryption* | *Decryption* |
|---|---|---|---|---|---|---|---|
| KATAN | AVR | 64 | 80 | 338 | 18 | 72063 | 88525 |
| SKIPJACK | Power TOSSIM | 64 | 80 | 5230 | 328 | 17390 | - |
| KLEIN | AVR | 64 | 80 | 1268 | 18 | 6095 | 7658 |
| *EDIA* | ATmega 328 | 64 | 64 | 950 | 30 | 3100 | 3048 |

*Fig.5. Comparison of Number of cycles*

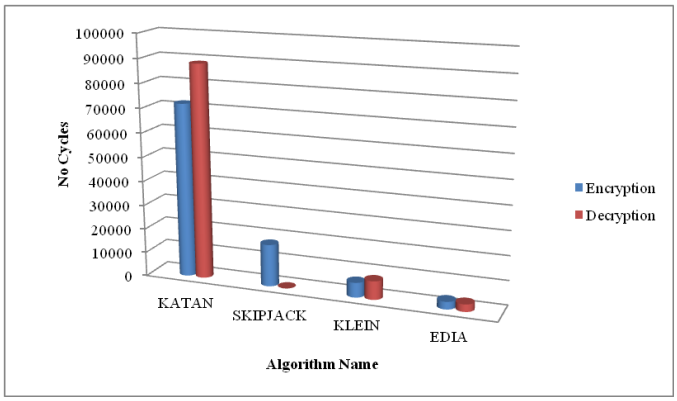


*Fig.6. Encryption & Decryption Cycles*

To evaluate the efficiency in the real-time, *EDIA* algorithm is executed in Rasperry pi environment where ,memory was 1 GB and processor 1.2 Ghz 64 bit Coretex and captured the results with other executions.


*Fig.7. Execution Time Parameter*

Energy consumption is also calculated based on the encryption and decryption cycles and is approximately calculated as 160.24 µJ and total sending cycle is about 1800 µJ. With a improved key complexity and cipher, these parameters shows a optimal usage and it can be utilized for any IoT devices and gadgets.

## V. CONCLUSION

This paper enumerated Improving Data Integrity & Security through Enhanced Lightweight SPN & Feistel combined algorithm with 5 rounds of encryption process and Encryption process on Arduino Uno showed promising results on the Security Analysis. Also Nodal Manager Raspberry pi which acted as a firewall for a resource & power constrained Arduino nodes and ensured Node Integrity in IoT Network. The encryption speed and data block authenticator taken less power and time in performance parameters. Through the lightweight algorithm and Authentication process, we were able to achieve the promising results by mitigating the node tampering, node hacking attacks.

## FUTURE WORKS

In Future, Scalability can be improved through high ROM and RAM in resource constrained devices and same can be applied to high powered devices to evaluate the possibility of using this approach in normal devices in SmartHome, SmartFactory, and SmartLogistics.

## REFERENCES


[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] Fagen Li and Pan Xiong. Practical secure communication for integrating wireless sensor networks into the internet of things. Sensors Journal, IEEE, 13(10):3677–3684, Oct 2013.

[4] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, “Detecting and localizing identity-based attacks in wireless and sensor networks,” IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2418–2434, 2010.

[5] Yousefi, Afsoon, and Seyed Mahdi Jameii. "Improving the security of internet of things using encryption algorithms." In 2017 International Conference on IoT and Application (ICIOT), pp. 1-5. IEEE, 2017.

[6] R. Want and S. Dustdar, “Activating the internet of things [guest editors’ introduction],” Computer, vol. 48, no. 9, pp. 16–20, 2015.

[7] 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.

[8] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, and L. Kerr, “Security in the industrial internet of things,” 2016.

[9] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: a review,” in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.

[10] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, “Smart locks: Lessons for securing commodity internet of things devices,” in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 461–472.

[11] D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for internet of things: A survey,” Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.

[12] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka,and Eita Kobayashi. TWINE: A lightweight block cipher for multiple platforms. In LarsR. Knudsen and HuapengWu, editors, Selected Areas in Cryptography, volume 7707 of Lecture Notes in Computer Science, pages 339–354. Springer Berlin Heidelberg,2013.

[13] Bhardwaj, Isha, Ajay Kumar, and Manu Bansal. "A review on lightweight cryptography algorithms for data security and authentication in IoTs." In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 504-509. IEEE, 2017.

[14] Tao, Hai, Md Zakirul Alam Bhuiyan, Ahmed N. Abdalla, Mohammad Mehedi Hassan, Jasni Mohamad Zain, and Thaier Hayajneh. "Secured data collection with hardware-based ciphers for iot-based healthcare." IEEE Internet of Things Journal 6, no. 1 (2019): 410-420.

[15] Sadeeq, Mohammed AM, Subhi RM Zeebaree, Riyadh Qashi, Sarkar Hasan Ahmed, and Karwan Jacksi. "Internet of Things Security: A Survey." In 2018 International Conference on Advanced Science and Engineering (ICOASE), pp. 162-166. IEEE, 2018.

[16] Samir, Nagham. "ASIC and FPGA Comparative Study for IoT Lightweight Hardware Security Algorithms." Ph.D. diss., Faculty of Engineering, Cairo University, Giza, 12613, Egypt, 2018.

[17] Guruprasad, S. P., and B. S. Chandrasekar. "An evaluation framework for security algorithms performance realization on FPGA." In 2018 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), pp. 1-6. IEEE, 2018.

[18] Huang, Yin, Wei Liang, Jing Long, Jianbo Xu, and Kuan-Ching Li. "A Novel Identity Authentication for FPGA Based IP Designs." In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1531-1536. IEEE, 2018.

[19] H. J. Ban, J. Choi, and N. Kang, “Fine-grained support of security services for resource constrained internet of things,” International Journal of Distributed Sensor Networks, vol. 2016, 2016.

[20] El-Haii, Mohammed, Maroun Chamoun, Ahmad Fadlallah, and Ahmed Serhrouchni. "Analysis of Cryptographic Algorithms on IoT Hardware platforms." In 2018 2nd Cyber Security in Networking Conference (CSNet), pp. 1-5. IEEE, 2018.

[21] Venugopal, Ellappan, and Tadesse Hailu. "FPGA Based Architecture of Elliptic Curve Scalar Multiplication for IOT." In 2018 Conference on Emerging Devices and Smart Systems (ICEDSS), pp. 178-182. IEEE, 2018.

[22] Landge, Irfan A., and Hannan Satopay. "Secured IoT Through Hashing Using MD5." In 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication, and Bio-Informatics (AEEICB), pp. 1-5. IEEE, 2018.

[23] M. Ebrahim and C. W. Chong, “Secure force: A low-complexity cryptographic algorithm for wireless sensor network (wsn),” in Control System, Computing and Engineering (ICCSCE), 2013 IEEE Interna-tional Conference on. IEEE, 2013, pp. 557–562.

[24] Khan, Nuzhat, Nazmus Sakib, Ismot Jerin, Shaela Quader, and Amitabha Chakrabarty. "Performance analysis of security algorithms for IoT devices." In 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), pp. 130-133. IEEE, 2017.

[25] “Compact implementation and performance evaluation of block ciphers in attiny devices,” in International Conference on Cryptology in Africa. Springer, 2012, pp. 172–187.

[26] Goyal, Tarun Kumar, and Vineet Sahula. "Lightweight security algorithm for low power IoT devices." In 2016 International Conference on Advances in Computing, Communications, and Informatics (ICACCI), pp. 1725-1729. IEEE, 2016.

[27] Naru, Effy Raja, Hemraj Saini, and Mukesh Sharma. "A recent review on lightweight cryptography in IoT." In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)(I-SMAC), pp. 887-890. IEEE, 2017.

[28] Pawar, Ankush B., and Shashikant Ghumbre. "A survey on IoT applications, security challenges, and countermeasures." In 2016 International Conference on Computing, Analytics and Security Trends (CAST), pp. 294-299. IEEE, 2016.

[29] Usman, Muhammad, Irfan Ahmed, M. Imran Aslam, Shujaat Khan, and Usman Ali Shah. "SIT: a lightweight encryption algorithm for secure internet of things." arXiv preprint arXiv: 1704.08688 (2017).

[30] Wang, Zhu, Yan Yao, Xiaojun Tong, Qinghua Luo, and Xiangyu Chen. "Dynamically Reconfigurable Encryption and Decryption System Design for the Internet of Things Information Security." Sensors 19, no. 1 (2019): 143

[31] Surendran, Susha, Amira Nassef, and Babak D. Beheshti. "A survey of cryptographic algorithms for IoT devices." In 2018 IEEE Long Island Systems, Applications, and Technology Conference (LISAT), pp. 1-8. IEEE, 2018.

[32] Hatzivasilis, George, Konstantinos Fysarakis, Ioannis Papaefstathiou, and Charalampos Manifavas. "A review of lightweight block ciphers." Journal of Cryptographic Engineering 8, no. 2 (2018): 141-184.

[33] P. Zhao, T. Peffer, R. Narayanamurthy, G. Fierro, P. Raftery, S. Kaam, and J. Kim, “Getting into the zone: how the internet of things can improve energy efficiency and demand response in a commercial building,” 2016.

[34] Y. Li, M. Hou, H. Liu, and Y. Liu, “Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of internet of things,” Information Technology and Management, vol. 13, no. 4, pp. 205–216, 2012.

[35] Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, “Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things,” in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, pp. 529–534.

[36] S. Misra, M. Maheswaran, and S. Hashmi, “Security challenges and approaches in internet of things,” 2016.

[37] M. C. Domingo, “An overview of the internet of things for people with disabilities,” Journal of Network and Computer Applications, vol. 35, no. 2, pp. 584–596, 2012.

[38] B. Karakostas, “A dns architecture for the internet of things: A case study in transport logistics,” Procedia Computer Science, vol. 19, pp. 594–601, 2013.

[39] Vyakaranal, S.; Kengond, S. Performance Analysis of Symmetric Key Cryptographic Algorithms. In Proceedings of the International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 3–5 April 2018; pp. 411–415.

[40] S. Khan, M. Ebrahim, and K. A. Khan, “Performance evaluation of secure force symmetric key algorithm,” 2015.

[41] Thomas Eisenbarth, Zheng Gong, Tim G¨uneysu, Stefan Heyse, Sebastiaan Indesteege, St´ephanie Kerckhof, Franc¸ois Koeune, Tomislav Nad, Thomas Plos, Francesco Regazzoni, Franc¸ois-Xavier Standaert, and Loic van Oldeneel tot Oldenzeel. Compact implementation and performance evaluation of block ciphers in attiny devices. In Proceedings of the 5th International Conference on Cryptology in Africa, AFRICACRYPT’12, pages 172–187, Berlin, Heidelberg,2012.Springer-Verlag.

[42] P. L. L. P. Pan Wang, Professor Sohail Chaudhry, S. Li, T. Tryfonas, and H. Li, “The internet of things: a security point of view,” Internet Research, vol. 26, no. 2, pp. 337–359, 2016.

[43] M. Ebrahim, S. Khan, and U. Khalid, “Security risk analysis in peer 2 peer system; an approach towards surmounting security challenges,” arXiv preprint arXiv:1404.5123, 2014.

[44] M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata, “Lightweight and escrow-less authenticated key agreement for the internet of things,” Computer Communications, 2016.

[45] F. Xie and H. Chen, “An efficient and robust data integrity verification algorithm based on context sensitive,” way, vol. 10, no. 4, 2016.

[46] S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, “Application of environmental internet of things on water quality management of urban scenic river,” International Journal of Sustainable Development & World Ecology, vol. 20, no. 3, pp. 216–222, 2013.

[47] S. A. Kumar, T. Vealey, and H. Srivastava, “Security in internet of things: Challenges, solutions and future directions,” in 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016, pp. 5772–5781.

[48] M. Ebrahim, S. Khan, and S. S. U. H. Mohani, “Peer-to-peer network simulators: an analytical review,” arXiv preprint arXiv:1405.0400, 2014.

[49] M. Ebrahim, S. Khan, and U. B. Khalid, “Symmetric algorithm survey: A comparative analysis,” International Journal of Computer Applica-tions (0975 – 8887), vol. 61, no. 20, 2014.

[50] K. Zhang, L. Ding, and J. Guan, “Cryptanalysis of hummingbird-2.” IACR Cryptology ePrint Archive, vol. 2012, p. 207, 2012.

[51] 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, Tech. Rep., 2013.

[52] T. Mourouzis, G. Song, N. Courtois, and M. Christofii, “Advanced differential cryptanalysis of reduced-round simon64/128 using large-round statistical distinguishers,” 2015.

[53] A. Biryukov, L. Perrin, and A. Udovenko, “Reverse-engineering the s-box of streebog, kuznyechik and stribobr1,” in Annual International Conference on the Theory and Applications of Cryptographic Tech-niques. Springer, 2016, pp. 372–402.

[54] S. Khan, M. S. Ibrahim, H. Amjad, K. A. Khan, and M. Ebrahim, “Fpga implementation of 64 bit secure force algorithm using full loop-unroll architecture,” in 2015 IEEE International Conference on Control System, Computing and Engineering (ICCSCE). IEEE, 2015, pp. 1–6.

[55] Alrowaithy, M.; Thomas, N. Investigating the Performance of C and C++ Cryptographic Libraries. In Proceedings of the 12th EAI International Conference on Performance Evaluation Methodologies and Tools, Palma, Spain, 12–15 March 2019; pp. 167–170.

[56] T. Eisenbarth, Z. Gong, T. Guneysu,¨ S. Heyse, S. Indesteege, S. Ker-ckhof, F. Koeune, T. Nad, T. Plos, F. Regazzoni et al., “Compact implementation and performance evaluation of block ciphers in at-tiny devices,” in International Conference on Cryptology in Africa. Springer, 2012, pp. 172–187.

[57] Safi, Amirhossein. "Improving the Security of the Internet of Things Using Encryption Algorithms." International Journal of Computer, Electrical, Automation, Control, and Information Engineering 11 (2017): 5.

[58] Wu, H. ACORN: A Lightweight Authenticated Cipher (v3). 2016. Available online: https://competitions.cr.yp.to/round3/acornv3.pdf (accessed on 30 July 2019).

[59] Dobraunig, C.; Eichlseder, M.; Mendel, F.; Schläffer, M. Ascon v1.2: Submission to the CAESAR Competition.2016. Available online: https://competitions.cr.yp.to/round3/asconv12.pdf (accessed on 30 July 2019).

[60] Hatzivasilis, G.; Fysarakis, K.; Papaefstathiou, I.; Manifavas, C. A review of lightweight block ciphers.J. Cryptogr. Eng. 2018, 8, 141–184.

[61] Appel, M.; Bossert, A.; Cooper, S.; Kussmaul, T.; Löffler, J.D.; Pauer, C.; Wiesmaier, A. Block ciphers for the IoT—SIMON, SPECK, KATAN, LED, TEA, PRESENT, and SEA Compared. 2016. Available online: https: //www.semanticscholar.org/paper/bc77d9dd70bacd6da036445cb6a78fea67b3b5dd (accessed on 23 July 2019).

[62] Dinu, D.; Le Corre, Y.; Khovratovich, D.; Perrin, L.; Großschädl, J.; Biryukov, A. Triathlon of lightweight block ciphers for the Internet of things. J. Cryptogr. Eng. 2018, 9, 283–302.

[63] Cazorla, M.; Gourgeon, S.; Marquet, K.; Minier, M. Survey and benchmark of lightweight block ciphers for MSP430 16-bit microcontroller. Secur. Commun. Netw. 2015, 8, 3564–3579.

[64] Saraiva, D.; Leithardt, V.; Crocker, P. Comparison and use of cryptography algorithms for ubiquitous computing.In Proceedings of the INForum, Simpósio de Informática, Guimarães, Portugal, 5–6 September 2019.

[65] Khan, N.; Sakib, N.; Jerin, I.; Quader, S.; Chakrabarty, A. Performance analysis of security algorithms for IoT devices. In Proceedings of the IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 21–23 December 2017; pp. 130–133.

[66] Surendran, S.; Nassef, A.; Beheshti, B.D. A survey of cryptographic algorithms for IoT devices. In Proceedings of the IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 4 May 2018; pp. 1–8.

[67] D. Maimut and K. Ouafi. Lightweight cryptography for rfid tags. Security Privacy, IEEE, 10(2):76–79, 2012.

[68] S. Khan, M. S. Ibrahim, M. Ebrahim, and H. Amjad, “Fpga implemen-tation of secure force (64-bit) low complexity encryption algorithm,” International Journal of Computer Network and Information Security, vol. 7, no. 12, p. 60, 2015.

[69] Da Silva, B.A.; Ochôa, I.S.; Leithardt, V. Estudo de Algoritmos Criptográficos Simétricos na Placa Beaglebone Black. Universidade do Vale do Itajaí (UNIVALI). 2018. Available online: https://www.setrem.com.br/erad2019/data/pdf/forum_ic/192077.pdf (accessed on 27 July 2019).

[70] Yilmaz, B.; Özdem˙Ir, S. Performance comparison of cryptographic algorithms in internet of things. In Proceedings of the 26th Signal Processing and Communications Applications Conference (SIU), Izmir, Turkey, 2–5 May 2018; pp. 1–4.

[71] Ochôa, I.S.; Leithardt, V.R.Q.; Zeferino, C.A.; Silva, J.S. Data Transmission Performance Analysis with Smart Grid Protocol and Cryptography Algorithms. In Proceedings of the 13th IEEE International Conference on Industry Applications (INDUSCON), São Paulo, Brazil, 12–14 November 2018; pp. 482–486.

[72] Soewito, B.; Gunawan, F.E.; Antonyová, A. Power consumption for security on mobile devices. In Proceedings of the 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS), Yogyakarta, Indonesia, 10–12 November 2016; pp. 1–4.

[73] Popov, A. Prohibiting RC4 Cipher Suites. Available online: https://tools.ietf.org/html/rfc7465 (accessed on 26 July 2019).

[74] Tsunoo, Y.; Saito, T.; Kubo, H.; Shigeri, M.; Suzaki, T.; Kawabata, T. The Most Efficient Distinguishing Attack on VMPC and RC4A. 2005.Available online:https://www.researchgate.net/publication /228914027_The_most_efficient_distinguishing_attack_on_VMPC_and_RC4A (accessed on 27 July 2019).

[75] Sibahee, M.A.A.; Lu, S.; Hussien, Z.A.; Hussain, M.A.; Mutlaq, K.A.; Abduljabbar, Z.A. The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN. In Proceedings of the International Conference on Computing Intelligence and Information System (CIIS), Nanjing, China, 21–23 April 2017; pp.308–312.

[76] Chandu, Y., KS Rakesh Kumar, Ninad Vivek Prabhukhanolkar, A. N. Anish and Sushma Rawal. "Design and implementation of hybrid encryption for the security of IOT data." In 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), pp. 1228-1231. IEEE, 2017.

[77] Bhargavan, K.; Leurent, G. On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), Vienna, Austria, 24–28 October 2016; pp. 456–467.

[78] Najm, Z.; Jap, D.; Jungk, B.; Picek, S.; Bhasin, S. On Comparing Side-channel Properties of AES and ChaCha20 on Microcontrollers. In Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Chengdu, China, 26–30 October 2018; pp. 552–555.

[79] Yang, Y.; Zheng, X.; Guo, W.; Liu, X.; Chang, V. Privacy-preserving fusion of IoT and big data for e-health. Future Gener. Comput. Syst. 2018, 86, 1437–1455.