Light Weight Energy Transfer Module Using DPR

Priti Lahane[1], *Mansi Vanmali*[2], *Kalyani Borse*[3], *Sujata Sanap*[4], *Arati Sonawane*[5]

1 Assistant Professor, Department of Information Technology, MET's Institute of Engineering, Maharashtra, India
2,3,4,5 Student, Department of Information Technology, MET's Institute of Engineering, Maharashtra, India

ABSTRACT

The scale and fields of IOT (Internet of Things)-based applications are increasing every day. Applications designed for enhanced IOT applications are one of the current growth drivers of today's industry. In the process of realizing this kind of IOT system, optimizing such applications to achieve the lowest power consumption, maximize functionality and best performance is an important part. During this period, data security is the main challenge for such Internet of Things (IOT) applications. Therefore, we must consider the available power budget and improve data security. Unfortunately, the issue of low power budget does not essentially mean that other performance requirements are relaxed. Therefore, this article is aimed at designers of IOT devices, including sensors, wireless communication devices, and near field communication devices. . It will focus on how to use automatic power consumption methods to enhance existing design capabilities, thereby reducing power consumption with the best data security technology, without affecting existing performance.
In this article, we have included some encryption technologies that provide different power consumption and security levels for IOT applications. From a given security module, some modes provide a higher security level at the expense of high power consumption, while some modes provide lower power consumption and a lower security level. Mainly perform dynamic partial reconfiguration (DPR) to adaptively configure the hardware security module according to the available power budget. The DPR control module of the system improves energy efficiency by maintaining data security and dynamically selecting the best transmission power budget with the least energy consumption. For a given power limit, the DPR controller configures the safety components using a safety method that meets the available power limit.

Keyword : - *Internet of Things (IOT), Security, Dynamic Partial Reconfiguration (DPR), Dynamic Encryption Modes, Competition for Authenticated Encryption: Security, Applicability and sturdiness.*

1. INTRODUCTION

The Internet of Things creates new value by connecting various devices to the network, but as recently seen in the era of certain applications, the Internet of Things also leads to security threats becoming an important issue. We can observe that more and more electronic applications require more secure communication technology, and with the improvement of security, we must also pay attention to the available power budget, which is one of the biggest limitations in daily electronic applications. If you observe that the traditional encryption technology modes RSA, AES, ECC provide almost the same level of security, and the key size is smaller, you can reduce power consumption, speed up calculations and take up minimal memory. This is very useful for different IOT applications, as they are often forced to demand their processing speed and functionality. This work includes software and hardware implementations using the latest encryption algorithm models (such as ACORN, Pi-Cipher, JAMBU, MORUS, etc.). [1]

The progress of most IOT applications depends on two main factors, namely security and privacy. IOT application developers mainly design or consider using low-power IOT devices to implement IOT applications. If the security level provided is not sufficient to proceed as expected, the risk of security data being attacked will increase. Data encryption is used to protect our private information by designing more secure and more co mplex

encryption algorithms. The main motto of this complex mathematical cryptographic algorithm is to develop a cryptographic framework that can accomplish privacy, verification and information respectability. Nonetheless, the restricted estimation of the accessible force spending plan is the principle challenge for low-power IOT gadgets, and contrasted with the necessary anticipated worth, this power limit provides weaker data security. We know that low-power IOT gadgets are basically battery-based gadgets. Therefore, we must use a battery pack with high power storage or another solution to minimize the power budget to realize a rechargeable battery pack. Rechargeable batteries depend on energy sources, such as solar energy, wind energy, etc. This energy source cannot provide constant power conditions. Depending on the available power budget, the utilization of this source raises different questions about the level of data security. This article proposes dynamic partial reconfiguration (DPR)

We try to find out which encryption mode is more reasonable for low-power IOT applications by considering the available power budget.

2. LITERATURE SURVEY

The Literature study depends on the investigation of many existing frameworks that give highlights, for example, information security modes and force utilization of every framework. Numerous conventions are utilized in correspondence from objects. The convention characterized in the gadget gives the transmission of program bundles and messages on the organization. Every convention has its own remarkable encryption, pressure, and mistake checking/amendment, where a ton of exploration and lab research are consistently led. [2] The gadget should trade some security boundaries to guarantee information security. Because of high energy utilization, exchange expenses and security, there are right now some encryption strategies that are not viable with IOT. The way toward deciding the convention to be utilized relies upon the necessities of the application. [3] In IOT gadgets, CoAP is embraced because of its straightforward interface and use. The amazing information convention encryption work further backings the new WPA3 standard.

3. PROPOSED WORK

This paper works center around lightweight and low force devouring calculation for encryption and decoding information utilizing distinctive numerical calculation. While stroll around a few calculations for the proposed work, we centered diverse encryption modes like ACORN, JAMBU, MORUS and so forth for encryption perspective. We have proposed an improvement in existing encryption modes utilized with accessible force spending thinking about. We need to demonstrate how ACORN calculation is discovered to be superior to others taking everything into account. This examination zeroed in on two plan initially is Dynamic Partial reconfiguration and second Static Partial reconfiguration.

The Implementation of Light Weight Energy Transfer Module Using DPR is shown in Fig 1 First Admin Log in to System, then Admin Start the Sensors in this Paper we are going to Use 3 Sensors for Comparison the Final Result. The three Different Sensors Collect the Data, then the Sensors Encrypt the Data Using ACORN, MORUS, and JAMBU. System will calculate the Time Required for Encryption of these three Algorithm. System Compare the Result that is Minimum time and Minimum Power Required for these Three Algorithms with the help of DPR and Display the Result. Again in the Software Side MD 5 Hashing Algorithm is Used for the Security Purpose. MD5 procedure a changing length of messages a rigid length output of 128 bit.The input message is separated up into chunks of 512 bit blocks. The message us stuff so that length is divided by 512.

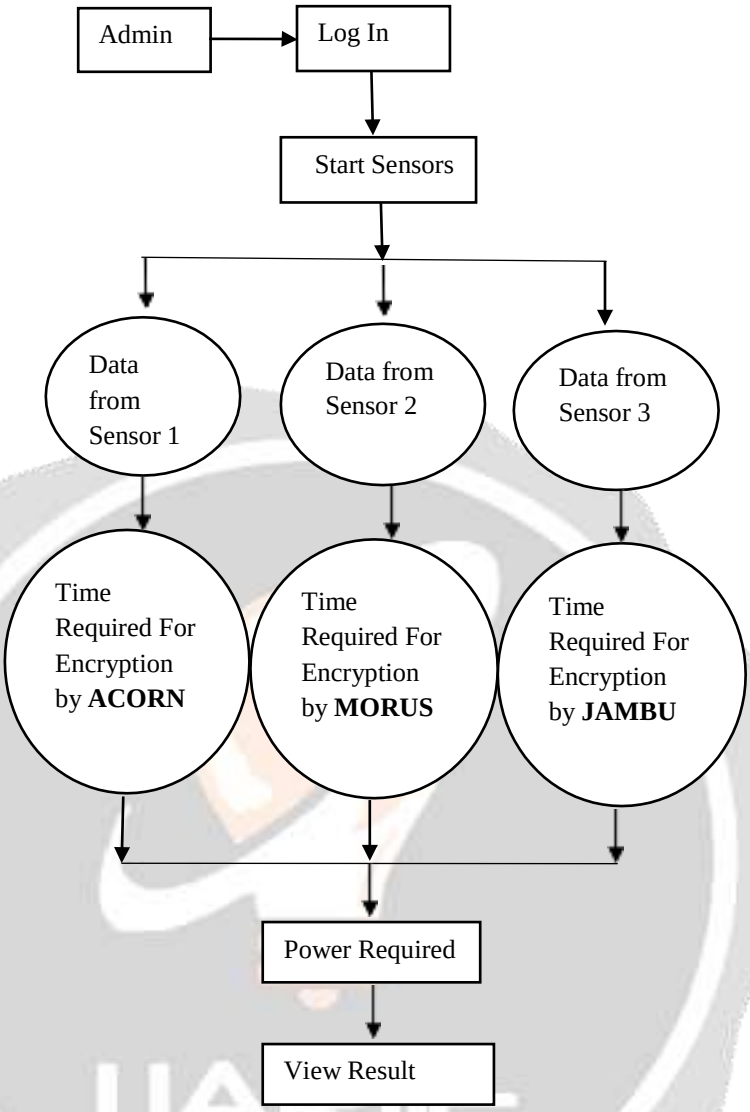

Fig - 1: Proposed Work Of Power Consumption

4. METHODOLOGY

The selected encryption mode adopted the "Certified Encryption Competition: Security, Applicability and Reliability" (CAESAR). The selected candidate is following.

4.1 ACORN

4.2 MORUS

4.3 JAMBU

This work led a relative investigation of these encryption modes, including two phases. The primary stage is to execute every encryption mode independently. Next, from the viewpoint of intensity utilization, territory usage, and throughput, quantitative correlations are made on the chose encryption modes to choose the most reasonable mode for low-power IOT applications. The subsequent stage is to execute the DPR idea in the chose encryption mode. The accompanying boundaries in the usage are helpful for lightweight encryption.

• Size (circuit size, ROM/RAM size)

• Power supply

• Energy utilization

• Processing speed (throughput, inactivity)

The principal phase of deciding the chance of acknowledgment in a gadget is size will be size. Force is especially significant for a gadget, and force utilization is significant for battery-controlled gadgets. High throughput is significant for gadgets with huge information transmission, and low inactivity is significant for ongoing control handling. Since the force relies upon equipment, for example, the circuit size or the processor utilized, the size turns into a reference point for the gentility and intensity of the encryption technique. Because of execution time, power utilization relies upon preparing speed. Throughput relies upon equal handling as far as security.

4.1 ACORN

ACORN is an authenticated encryption (AEAD) algorithm based on stream ciphers with associated data. The AEAD scheme also allows information to be included that does not require encryption but also requires honesty and authenticity to be assured. ACORN uses a 128-bit key, an initialization vector (IV) of 128 bits, and produces an authentication tag of 128 bits. Its internal state has a length of 293 bits and As shown in Figure 3 below, it consists of six LFSRs. ACORN

relies on three main functions: the function for generating output key streams, the nonlinear feedback function and the function for updating status.

4.2 MORUS

MORUS is a superior confirmed encryption calculation submitted to the CAESAR rivalry and was as of late shortlisted. The Authentication Encryption (AE) plot consolidates the elements of a symmetric encryption conspire and a message validation code. Different outcomes won't compromise the total MORUS, however different parts of the exploration configuration help to comprehend its points of interest and impediments. [6]

4.3 JAMBU

JAMBU utilized k-piece mystery key K and n-bit public irregular number IV to verify the variable-length related information AD, and scrambles and validates the variable-length plaintext P. The encryption cycle of JAMBU incorporates 5 phases: filling, introduction, preparing of related information, handling of plain content, and end/label age. [7]
A significant pattern in the current advancement of encryption innovation is to plan lightweight encryption natives, on the grounds that the interest for ease implanted frameworks keeps on developing. [8]

JAMBU is a lightweight validation encryption mode submitted to the CAESAR rivalry. JAMBU is the littlest square code validation encryption mode in the CAESAR rivalry. [9]

Validated encryption is an exceptionally valuable encryption crude, which gives both security and credibility when sending information. [10]

5. ARCHITECTURE

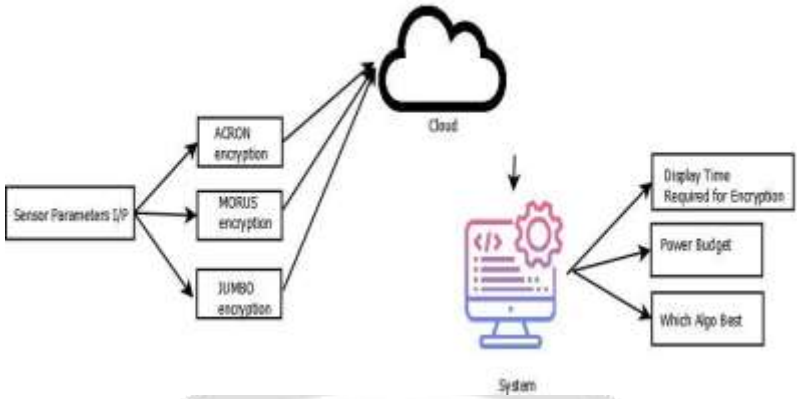

Fig - 1: Architecture Daigram

In architecture diagram we take parameters from sensor as a enter. Then every sensor will carry out encryption operation.it takes temperature sensors that continuously advantage records then sensor perform encryption operation i.e encryption from ACORN, MORUS, JAMBU. That encrypted information is shared on Cloud then, system will get admission to that cloud records encrypted by sensor and machine will calculate Time, energy Required for those algorithms. Then show Which set of rules is nice for the strength IOT devices.

6. IMPLEMENTATION

In Implementation there are 3 tables for 3 algorithms that is inside the following.

6.1 JAMBU Data

Following Table I depicts that There is val1, val2, val3 are the sensor parameters that is Encrypted with JUMBU algorithm at hardware side and the Encryption secret is putted interior this val1, val2, val3 Block. So here it's miles simple text of val1, val2, val3 which is easy to hack so for the security reason once more we Encrypt the val1, val2, val3 statistics at the software side with the assist of MD5 Hashing set of rules.
So this is a key of MD5 algorithm. There it's miles start time and give up time required for JUMBU Encryption algorithm. right here we can see that the extraordinary between start time and quit time is 3 mili second.

Value1	Value2	Value3	Start Time	End Time	Key
100194	100188	100188	1621347791	1621347794	41e4d3058d1a3b2d321c2 f4821fa4201

Table - 1 : JAMBU

6.2 MORUS Data

Following Table II depicts that MORUS is likewise equal as JUMBU. right here val1, val2, val3 are the sensor parameters which is Encrypted with MORUS set of rules at hardware aspect and the Encryption secret's putted internal this val1, val2, val3 Block.

So right here it is plain textual content of val1, val2, val3 which is straightforward to hack so for the security cause again it Encrypt the val1, val2, val3 data on the software program side with the assist of MD5 Hashing algorithm.

So that is a key of MD5 algorithm. there it's far start time and cease time required for MORUS Encryption algorithm. there we will see that the unique between start time and end time is 1 Milisecond.

Value1	Value2	Value3	Start Time	End Time	Key
100188	100188	100188	1621347791	1621347792	2661b92a45f3f3d93921a1738ce44057

Table - 2 : MORUS

6.3 ACORN Data

Following Table III depicts that ACORN is also same as JUMBU and MORUS . there val1, val2, val3 are the sensor parameters which is Encrypted with MORUS Algorithm at Hardware side and the Encryption key is putted inside this val1, val2, val3 Block. So here it is plain text of val1, val2, val3 which is easy to hack so for the Security Purpose again we Encrypt the val1, val2, val3 Data at the Software side with the help of MD5 Hashing Algorithm. So this is a key of MD5 Algorithm. Here it is Start time and End time required for MORUS Encryption Algorithm. Here the different between start time and End time is near about 0 Milisecond . That is same, so from this 3 tables of Algorithm .It is prove that ACORN takes Very less Time for Encryption as compared to JUMBU and MORUS.

Value1	Value2	Value3	Start Time	End Time	Key
100194	100188	100188	1621347572	1621347572	41e4d3058d1a3b2d321c2f4821fa4201
100194	100188	100188	1621347827	1621347827	41e4d3058d1a3b2d321c2f4821fa4201

Table - 3 : ACORN

7. RESULT AND ANALYSIS

Result obtain after implementation. Algorithms Acorn makes use of near About 1 Micro Seconds. Morus makes use of 1 Mili Seconds. Jambu makes use of 3 Mili Seconds for encryption. For this reason Acorn takes less time as evaluate to Morus and Jambu and as a consequence, it required much less Power consumption.

Algorithms	Encryption Start Time	Encryption End Time	Time (ms) Required for Encryption
JAMBU	1621347791	1621347794	3 ms
MORUS	1621347791	1621347792	1 ms
ACORN	1621347827	1621347827	1 micro sec

Table - 4 : Result

In the Below Graph X-axis is the Algorithms Names and Y-Axis is the Approximately Time Required for Encryption Process. From this Graph it is Prove that ACORN takes very Less Time as Compare to JAMBU and MORUS.

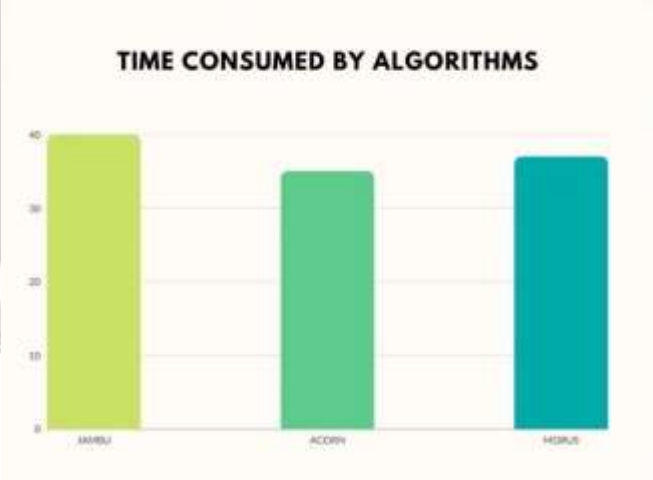

Chart – 1 : Graph of Algorithms

8. LIMITATIONS

All DPR modules are work's on batteries so there is cost required for charging of batteries.

9. CONCLUSION

Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) Algorithms are Useful for Light Weight Energy Transfer Module.
From the Result it is Conclude that ACORN is the Fastest Algorithm For Encryption. As Time is Directly Proportional to the Power hence it also takes Low Power for the IOT Devices.

10. REFERENCES

[1] **Energy-Adaptive Lightweight Hardware Security Module using Partial Dynamic Reconfiguration for Energy Limited Internet of Things Applications,** Author: Nagham Samir1, Yousef Gamal1, Ahmed N. El-Zeiny1, Omar Mahmoud1, Ahmed Shawky1, AbdelRahman Saeed1, and Hassan Mostafa1;2

[2] IEEE 802.15 is a convenient standard for domains compatible for low-power consumption and rapid transfer.

[3] The 6LoWPAN standard enables small devices with the IEEE 802.15.4 physical layer to connect to the internet via IPv6 addressing.

[4] 2009 Third International Symposium on Intelligent Information Technology Application, **Dynamic partial reconfiguration in FPGAs,** Wang Lie, Wu Feng-yan, Dept. of Computer Science & Electronic Information, Guangxi University, Nanning,China.

[5] H. Wu, **"ACORN: A Lighweight Authenticated Cipher (v3),"** Candidate for the CAESAR Competition.

[6] **Cryptanalysis of MORUS,** Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella et al.

[7] **Cryptanalysis of JAMBU**, IACR-FSE-2015.

[8] **JAMBU lightweight authenticated encryption mode and AES-JAMBU,** H Wu, T Huang - CAESAR competition proposal, 2014 - csrc.nist.gov.

[9] **TinyJAMBU: A Family of Lightweight Authenticated Encryption Algorithms**, Hongjun Wu and Tao Huang, Division of Mathematical Sciences Nanyang Technological University, 29 March 2019.

[10] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli H. Sundmaeker, A. Bassi, et al., "Internet of Things Strategic Research Roadmap," Internet of Things-Global Technological and Societal Trends, vol , pp 9-52, 2011.

[11] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao,"A survey onSecurity and Privacy Issues in Internet-of-Things,"in IEEE Internet of Things Journal,vol. 4, pp. 1250 - 1258, April 2017.

[12] Ruinian Li, Tianyi Song, Nicholas Capurso, Jiguo Yu, Jason Couture, and Xiuzhen Cheng, "IoT Applications on Secure Smart Shopping System," in IEEE Internet of Things Journal, vol. 4, pp. 1945 - 1954, May 2017.

[13] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao, "A Survey on Internet of Things Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, pp. 1125 - 1142, March 2017.

[14] C.-I. Cluster, "Visions and Challenges for Realising the Internet of Things," European Cosmmission, 2010.

[15] M. Katsaiti, A. Rigas, I. Tzemos, and N. Sklavos, " Real-World Attacks Toward Circuits & Systems Design, Targeting Safety Invasion," in Proceedings of the 4th International Conference on Modern Circuits and System Technologies (MOCAST), 2015.

[16] U. Mamidi, "Lightweight Authenticated Encryption for FPGAs," 2016.

[17] Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales Sandoval, "Lightweight Hardware Architectures for the Present Cipher in FPGA," in IEEE Transactions on Circuits and Systems, vol 64 pp. 2544 - 2555, April 2017.

[18] Mohammed Moness; Ahmed Mahmoud Moustafa,"A Survey of Cyber Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy," in IEEE Internet of Things Journal, vol. 3,pp.134 - 145, September 2015.

[19] **Cryptanalysis of JAMBU,** Thomas Peyrin and Siang Meng Sim and Lei Wang and Guoyan Zhang, IACR-FSE-2015.

[20] **Light Weight Energy Transfer Module Using DPR** International Journal of Scientific Research in Engineering and Management (IJSREM) Volume: 05 Issue: 05 | May - 2021