A
Dissertation On

“IOT SECURITY USING PUF AND ENCRYPTION TECHNIQUE”

Submitted in Partial Fulfilment of the Requirement
For the Award of Degree of

Master of Technology

In

Software Technology

By

Prateek Kumar Jain
University Roll No. 2K14/SWT/511

Under the Esteemed Guidance of
Mr. Manoj Kumar
Associate Professor
Computer Science & Engineering

COMPUTER SCIENCE & ENGINEERING DEPARTMENT
DELHI TECHNOLOGICAL UNIVERSITY
DELHI – 110042, INDIA

STUDENT UNDERTAKING

Delhi Technological University
(Government of Delhi NCR)
Bawana Road, New Delhi-42

This is to certify that the thesis entitled **"IOT SECURITY USING PUF AND ENCRYPTION TECHNIQUE"** done by me for the Major project for the award of degree of **Master of Technology** Degree in **Software Engineering** in the **Department of Computer Science & Engineering**, Delhi Technological University, New Delhi is an authentic work carried out by me under the guidance of Dr. Rajni Jindal.

Signature:
Student Name
Prateek Kumar Jain
2K14/SWT/511

Above Statement given by Student is Correct.

Project Guide:
Mr. Manoj Kumar
Associate Professor, Department of Computer Science & Engineering,
Delhi Technological University, Delhi

DELHI TECHNOLOGICAL UNIVERSITY

DELHI-110042

DECLARATION

I PRATEEK KUMAR JAIN, Roll No. 2K14/SWT/511, student of MTech (Software Technology), hereby declare that the thesis entitled **“IOT SECURITY USING PUF AND ENCRYPTION TECHNIQUE”** which is being submitted by me to the **Delhi Technological University**, in partial fulfillment of the requirements for the award of the degree of **Master of Technology in Software Technology** is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition. The material contained in this thesis has not been submitted to any university or institution for the award of any degree.

Place: Delhi

Prateek Kumar Jain
2K14/SWT/511

DATE:

SIGNATURE

DELHI TECHNOLOGICAL UNIVERSITY

DELHI-110042

CERTIFICATE

This is to certify that thesis entitled **"IOT SECURITY USING PUF AND ENCRYPTION TECHNIQUE",** is a bona fide work done by Mr. Prateek Kumar Jain (Roll No: 2K14/SWT/511) in partial fulfillment of the requirements for the award of **Master of Technology Degree in Software Technology** at Delhi Technological University, Delhi, is an authentic work carried out by him under my supervision and guidance. The content embodied in this thesis has not been submitted by him earlier to any University or Institution for the award of any Degree or Diploma to the best of my knowledge and belief.

DATE:

SIGNATURE:

Project Guide:
Mr. Manoj Kumar
Associate Professor, Department of Computer Science & Engineering
Delhi Technological University, Delhi

ACKNOWLEDGEMENT

I take this opportunity to express my deep sense of gratitude and respect towards my guide **Mr. Manoj Kumar, Associate Professor & Head (Computer Centre), Department of Computer Science & Engineering.**

I am very much indebted to her for her generosity, expertise and guidance i have received from her while working on this project. Without her support and timely guidance, the completion of the project would have seemed a far-fetched dream. In this respect I find myself lucky to have my guide. He has guided not only with the subject matter, but also taught the proper style and techniques of documentation and presentation. I would also like to take this opportunity to present my sincere regards **Mr. Manoj Kumar, SUPERVISOR,** Associate Professor, DTU for extending their support and valuable Guidance.

Besides my guide, I would like to thank **Dr. Rajni Jindal** Professor and HOD, entire teaching and non-teaching staff in the Department of Computer Engineering, DTU for all their help during my tenure at DTU. Kudos to all my friends at DTU for thought provoking discussion and making study joyful.

PRATEEK KUMAR JAIN
MTech, Software Engineering
2K14/SWT/511

ABSTRACT

Today I can say that we are living in the world of IOT where more than half world's people are using internet. IoT has started capturing the market all over the world. Nearly all household appliances are available and consumer can buy them. Even though increasing popularity and acceptance of IoT enabled devices "Security of device and information" is big concern.

Lack of security leaves the customer potentially exposed to various risk factors. Risk might be ranging daily routine data theft to great financial risk, even in some cases there is life threating risk for specific or group of persons. On analyzing various devices, I come to know that many are not devices enforced strong passwords are not devices applied, or brute-force attacks is not protected, physical replacement of faulty sensors or wiretapping the traffic. As per approximation, every two among ten applications of mobile which are being used for managing and handling IOT devices are vulnerable and are not using SSL for communication data encryption.

We already know many potential weaknesses that could affect IoT system. Apart from soft attack like phishing, service interruption, virus infection, there is also possibility of physically interfere IoT network. IoT involve billions of sensors spreading all around the world. Many of them are not physically protected. Attacker could access those sensors/devices and manipulate them or replace them. Captured data through sensors is also not safe if transmitted without encrypting them. Further many devices don't have such power to perform heavy encryption.

In this project I am proposing a PUF (Physically unclonable function) and light weight encryption technique-based solution. PUF is class of new hardware security primitives. It promises a paradigm shift in security problems and challenges. It has a very simple architecture and can solve problem of energy-constrained IoT devices. I am using PUF functionality with hardware sensors. Since PUF function cannot be cloned therefore sensors are safe and any modification or replacement can be easily detected. Further data received from sensors will be encrypted using light weigh encryption technique.

In future I will explore a how to store safely vast amount of data generated through billions of sensors.

TABLE OF CONTENTS

CERTIFICATE ....[i]

ACKNOWLEDGEMENT...[ii]

ABSTRACT ....[iii]

TABLE OF CONTENTS ....[iv]

LIST OF FIGURES ....[vi]

LIST OF TABLES ....[vii]

CHAPTER 1

INTRODUCTION 1

1.1. GRENRAL CONCEPTS 1

1.2. MOTIVATION 2

1.3. PROBLEM STATEMENT 2

1.4. SCOPE OF THE THESIS.. 3

CHAPTER 2

LITERATURE SURVEY.. 4

2.1. Sensors 4

2.2. Internet enabled devices... 4

2.3. Servers 4

2.4. Cloud system/database system 5

2.5. PUF(Physically Unclonable function) 5

2.6. Encryption and Decryption.. 5

CHAPTER 3

PROPOSED WORK.. 6

CHAPTER 4

PROPOSED METHODOLOGY... 8

4.1. PUF (Physically unclonable function).. 8

4.2. PUF-Based Authentication 9

4.3. PUF-Based encryption/decryption 10

4.4. Encryption/Decryption using light weight Encryption methods 11

4.4.1 Key Generation Process 12

4.4.2 Encryption Process 15

4.4.3 Decryption Process 17

CHAPTER 5

EXPERIMENTS & RESULTS 18

5.1. RESULTS 18

CHAPTER 6

CONCLUSION AND FUTURE WORK 19

REFERENCES 20

LIST OF FIGURES

Figure 1: Authentication of PUF device, encryption and decryption of data 7

Figure 2: PUF circuit 8

Figure 3: PUF based Authentication 9

Figure 4: A PUF-Based Encryption Scheme 10

Figure 5: A PUF-Based Decryption Scheme 11

Figure 6: Nonlinear and Linear transformations function (F-Function) 13

Figure 7: Encryption Process 16

LIST OF TABLES

Table 1: Notations 12

Table 2: P table... 13

Table 3: Q table 15

CHAPTER 1. INTRODUCTION

1.1 General Concepts

There are so many different definitions are given for Internet of Things (IoT). I would like to describe it as:

Internet of Things can be considered a heterogeneous collection of billions of things/objects or items like sensors, computing devices, storage devices and various smart devices which are directly/indirectly capable of connecting with Internet or with other device with are capable to connect with internet.

The advancement in technology has been changing the way of our life and digital information has now become a social infrastructure [1]. The IoT is envisaged to be made of several heterogeneous devices with unique identifiers [2] . By 2020 it is anticipated that the IoT paradigm will include approximately 20 billion connected devices [3]. Since IoT is collection of lots of devices so it provides a large number of areas and at different levels where attacker can target for various networks. In previous days, attackers were not sophisticated and they don’t have enough profit from hijacking IoT devices. But in current days attack is quite profitable and various ransomware are found to be spreading through these IoT devices. In Future proof-of-concept would be reality.

At current time attackers are not quite active, but in future these attackers wouldn’t stay at back foot. IoT could be attacked at its weakness. In many IoT device do not include keyboard therefore password and other configuration is done from remote location. Many venders do not use process which forces user to change password and default password is present in the device. Sometime user changes password to some predictable password. RFID like identification technologies have empowered the concept of Internet of Things by enabling the unique identification of things [4].

Apart from attacking on default password, sensors deployed on physically accessible location could also be attached. Sensor could be replaced and wrong data could be generated or actual data traffic over the air could be monitored.

1.2. MOTIVATION

As Internet of things is gaining more and more popularity, its scope is also increasing. Everyday thousands of new devices are joining this vast network. IoT based business are growing. Many IoT based health services and surveillance services are increasing. There dependency on IoT increasing. These services mainly involve sensors which continuously collect data and send to cloud system or server using an internet enabled device where this collected data is stored, processed and shared for various purpose such as business, research work, safety, transport, traffic regulation, etc. There are so many devices which are connected and could communicate with each other for their physical and logical capabilities and properties. They can also retrieve and store information from its surrounding spaces using various sensors. These connected devices have capability to find out various predictions based on past events and current situations. These can be used in decision making activities.

Since many times these sensors are placed on the location where these are not physically protected. Further collected data can be accessed by attacker if raw data is shared over internet. Therefore, the proposed solutions from an IoT networking perspective must take into account the scalability of IoT nodes as well as the operational cost of deploying the networking infrastructure [5].

Due to the inherent vulnerabilities of the Internet, security and privacy issues should be considered and addressed before the Internet of Things is widely deployed [6]. Fog/edge computing has been proposed to be integrated with Internet of Things (IoT) to enable computing services devices deployed at network edge, aiming to improve the user's experience and resilience of the services in case of failures [7]

Since these day many small devices are available which can be connected to internet and shared data but these devices have limited processing capability and power (battery). Therefore, some mechanism is required to protect or authenticate physical sensor so that it is not manipulated or replaced.

1.3 PROBLEM STATEMENT

In current world, IoT has picked up race and trillions of IoT enabled devices are now in market. Many people are using them for their business, health, education, research, security or other monitoring work. Although IoT is composed of sensors, internet enabled devices, internet, database system, servers and web portals but mainly data is collected through then sensors which are physically located at various places where intruder can easily access them. These sensors provide data to internet enabled device which finally transfer it to some server and database system where data is processed and stored.

Here, problem is that intruder can access I sensors and can modify or replace them. Further they can monitor the traffic and receive important information. These activities could cause breach of security of IoT and could be reason for major loss. “Privacy and security in IOT, is proven one of the most challenging areas, with a number of published works about them the last years.” [8]

An ideal solution should be good enough to authenticate and verify these sensors from which data is being collected and shouldn’t allow intruders to get information from mentoring data traffic. Further,

These devices have limited processing and storage capability and less battery power therefore solution need to be designed keep in mind these restrictions.

I am proposing a solution which uses PUF (Physically unclonable function) and light weight encryption of transferred traffic.

1.4 SCOPE OF THIS THESIS

In this Project. I have focused on the physical sensor device’s protection by authenticating sensor and verifying them. In this way we can assure that data which we are receiving are correct and further encrypting data using light weight encryption algorithm which can be further shared to IoT network. Encryption help to protect data from intruder who is monitoring traffic and light weight encryption help to minimize the requirement of memory, processing power and hence battery power.

CHAPTER 2. LITERATURE REVIEW

All over the internet, thesis, research work, assignment work etc. provide various definition of IoT.

M. Syafiq Mispan, Mark Zwolinski and Basel Halak define IoT as “The Internet of Things (IoT) consists of numerous inter-connected resource-constrained devices such as sensors nodes and actuators, which are linked to the Internet” [3].

I would like to provide more detailed definition of IoT as ‘Internet of Things’ is the realization of concept that all the things over the world are connected to a heterogeneous network. IoT include Sensors, internet enabled wireless devices, internet enabled wired devices, servers, protocols which enable smooth flow of information, security software’s and devices, Database system/cloud system, and web portals. Further if I define IoT in minimum words then will say “A logically connected world”.

2.1 Sensor

A sensor are the physical devices which can measure some value from its surrounding environment. For example, a thermometer could measure the current. Speedometer could measure the speed. There is various type of sensor. In general term sensor are physical device which sense the surrounding environment. Sensors are the end point in the IoT network.

2.2. Internet enabled devices

These are the devices which have the capability to transferred information which is collected through various sensors or from other means, to the internet whether on the other hand server and a database system is connected.

2.3 Servers

Servers are computer system which have vast processing power. Server could be a single computer or as set of inter connected computers. These have sufficient memory, processing power and power supply. Most of the IoT server run all the time. Main task of these server is to process the data and provide the information whenever required.

2. 4 Cloud system/database system

A cloud or database system is the place where retrieved data and processed data is stored for the further use. Cloud system have trillions of exabyte storage space. It has its own authentication, verification, validation, and other security protocols to keep data safe.

2.5 Security Software

There is so many security software which are continuously running the keep data safe from various attack from intruders and malicious programs.

2.6 PUF

For data retrieval we need to find answer of few queries: Important characteristics of data retrieved? Is data is static, user information such as “user id, name, gender”; or dynamic data such as user’s tweet and its network? Which kind of data is important for analysis? How it will be processed? What is actual size of data collected? It is very easier to keep finding of certain keyword associated with any hashtag rather than keyword which is not associated.

2.7 Encryption and Decryption:

Encryption is a technique or process by which we convert plain text or data into code form which is called cypher text. This cypher text looks meaningless. If someone receive this cypher text then he can’t receive any information from this without decoding it. Decryption is a technique or process by which we convert coded cypher text into plain text.

CHAPTER 3. PROPOSED WORK

I am proposing a solution with the help of PUF and light weight encryption algorithm.

In my proposed solution I am using a PUF enabled device in PUF enabled device is the device which cannot be replicated hence therefore It is fully protected from unauthorized attack to the network.

Initially Server will apply multiple challenges to the PUF enabled sensor and generate it response this response will be saved in the database. This challenge and response will be later used to authenticate the PUF enabled sensor.

Once challenge-response is generated and saved at the server database PUF enable sensor is deployed to the field.

After deploying sensor data is being generated by the sensor and these sensors are equipped with the PUF. These sensors could vary in their functionality such as it could measure current, it can measure pollution, it can measure blood pressure or heart rate. Once data is captured These PUF enabled sensor have the capability to encrypt them based on the challenge. Since server already have the response for each challenge it can decrypt it at its end.

Once data is generated and encrypted at hardware level then it transfers to the Internet enabled device which have more capability then just a sensor. Now I am using processing capability of Internet enable device to receive the data from sensor and then used RC5 based light weight encryption algorithm to encrypt and decrypt.

RC5 based encryption algorithm consist of 3 parts, expansion of key, encryption process and decryption process. RC5 based encryption provide flexibility to variate in size of key, number of round and block size.

Large size of key and more number of round in encryption provide more security of data. While sorter key length and less number of round in encryption process are vulnerable to break encoding. Based on the Internet privacy protection mechanism with the characteristics of Internet of things, preference-based privacy protection mechanism for the Internet of things can be integrated in future [9].

Following diagram show the authentication of PUF device, encryption and decryption of data.

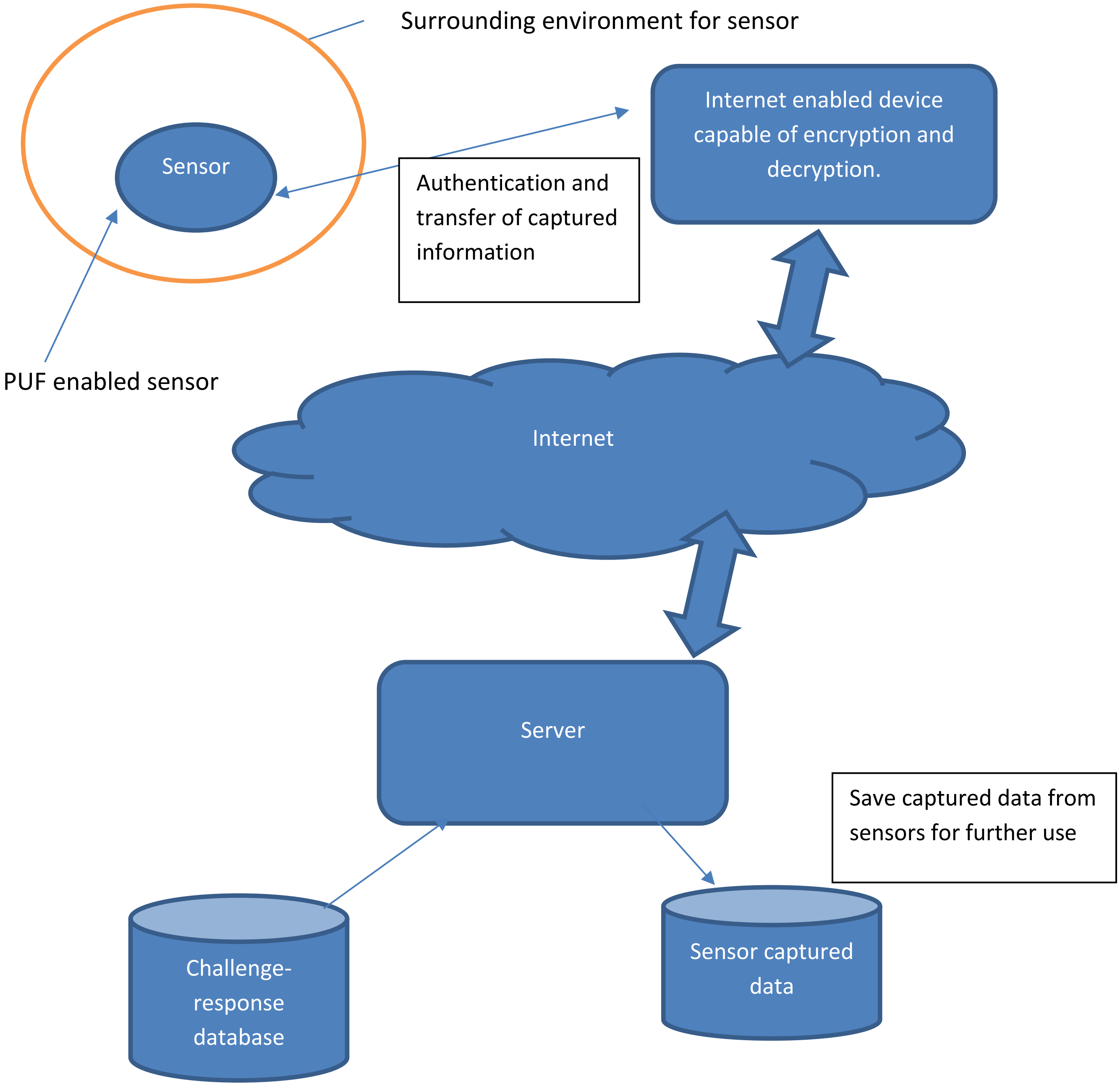

Surrounding environment for sensor
Sensor
Internet enabled device capable of encryption and decryption.
Authentication and transfer of captured information
PUF enabled sensor
Internet
Server
Save captured data from sensors for further use
Challenge-response database
Sensor captured data

Fig 3.1 Authentication of PUF device, encryption and decryption of data

CHAPTER 4. METHODOLOGY

4.1 PUF

Physically unclonable function which can be abbreviated as PUF. Silicon-based Physical unclonable device can be considered as an integrated circuit, which have capability that if it is implemented on different chips it produces different result for the same set of inputs. We can utilize this to create a unique identification like fingerprint for each physical device or sensors.

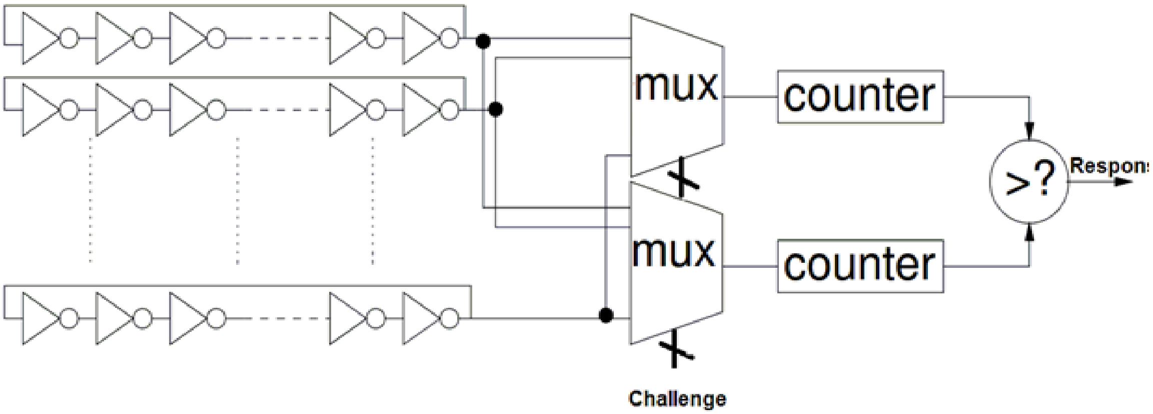


Fig. 4.1 PUF circuit

To illustrate the PUF circuit operating functionality, Above figure is showing a PUF. It is generic ring oscillators-based PUF. This PUF circuit include 1 comparator, 2 multiplexers, few ROs which are also call Ring Oscillators. Each of these oscillators possess a unique frequency. This frequency is varying and depend upon the delay characteristics of inverters. Due to manufacturing variation this frequency varies.

There are two multiplexer which select and compare two different ROs. Again, there are two counter blocks which count the oscillation numbers in a fixed time interval for the selected ROs. After interval completed, output of both counters are compared. Now depend on the counter which have highest value,1 or 0 value is set in output of PUF. Hence based on input and selected ROs and delay of inverters determine the frequency of oscillation. This frequency varies with respect to chip. Thus, this PUF can generate and authenticate unique identities or signature for each and every hardware device.

4.2 PUF-Based Authentication

To create a trustworthy environment in IoT network we much authenticate the device from which input is being generated.

Initial step to authenticate device is to check whether it is authorised device or not. In open environment third party have access to sensor device and therefore it can be manipulated or replaced. firstly, I apply randomly chosen a large set of challenges and save the corresponding response into our database. After stored challenge-response in database deploy the sensor device.

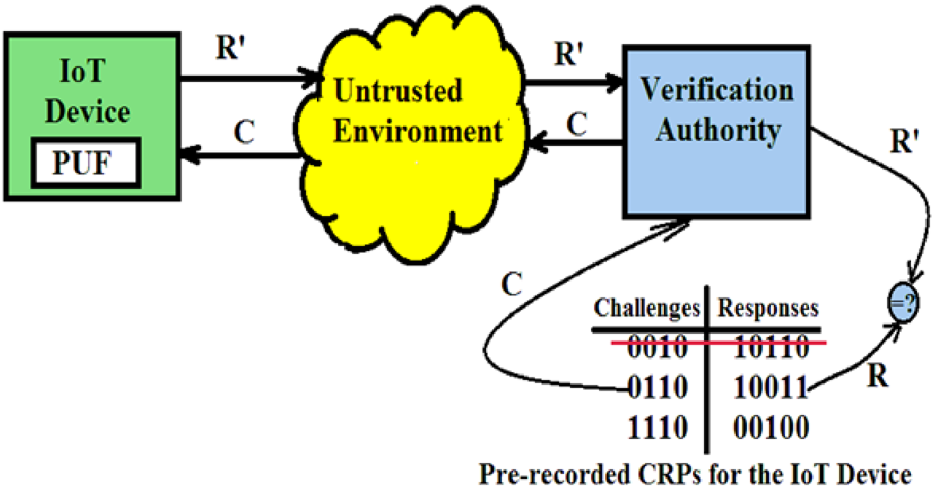


Fig 4.2 PUF based Authentication

In the next step of verification of the device. I select a random challenge which is not being used earlier.

Provide this challenge to PUF device and record its response. PUF device is authenticate only if its response is matched with pre-recorded responses.

4.3 Encryption and Decryption for PUF-Based device

Confidentiality and privacy of data is achieved through encryption. In order to encrypt the data first we provide challenge (C) to PUF device and retrieve its response (R) then apply it to Error correction codes (ECC) along with syndrome bit which has been precomputed for each challenge-response code. which generate the Key. Next XORed the key with plain text to generate ciphertext

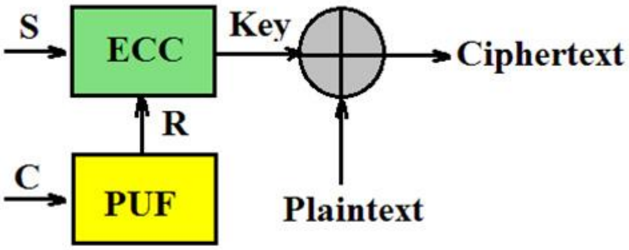
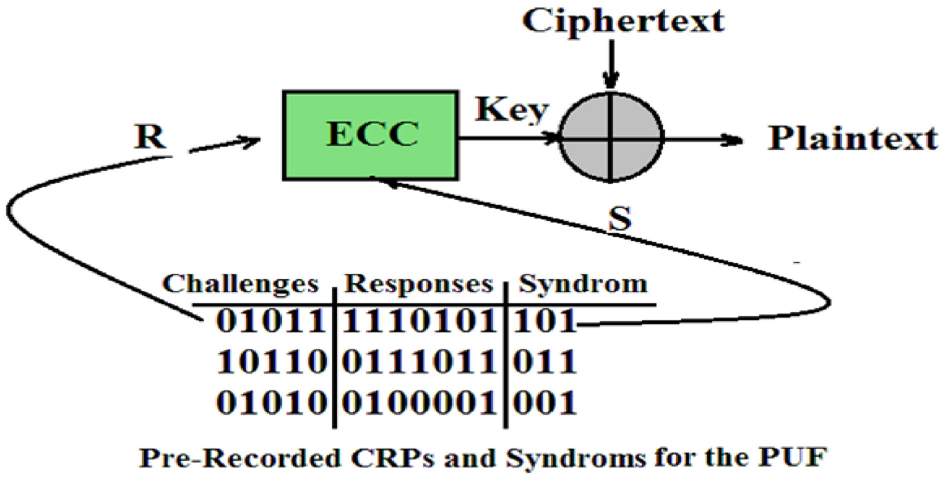


Fig 4.3 A PUF-Based Encryption Scheme

Once data is encrypted it can be decrypted on the other side using Response and syndrome code. I apply both at Error correction code which generate the Key. Now XORed this Key with ciphertext to retrieve plaintext.



Challenges	Responses	Syndrom
01011	1110101	101
10110	0111011	011
01010	0100001	001

Pre-Recorded CRPs and Syndroms for the PUF

Fig 4.4 A PUF-Based Decryption Scheme

4.4 Encryption/Decryption using light weight Encryption methods

As per requirement we need some light we need some light weight encryption algorithm which can be run on devices that have limited resources in term of memory, processing power, and power supply or battery size.

On analysing multiple encryption method, I come out with RC5 algorithm which have the capability to run some minimum resources and also have the flexibility to variate parameters based on requirement.

“The RC algorithm, which consists of three components a key expansion algorithm an encryption algorithm and a decryption algorithm” [10]. SIT is a symmetric key block cipher that constitutes of 64-bit key and plain-text [11].

My algorithm is symmetric key algorithm. This algorithm can used with 16. 32,64 or 128-bit Key. Several round of encryption is performed and each round consist some mathematical calculation to create diffusion and confusion. Number of round can be varying from 8 to 20. But as the number of round decreases encryption become weak and could be decode. Too high number of round could cause consumption of resource and time.

This encryption/decryption algorithm itself contain 3 vital components.

1. Key Generation
2. Encryption
3. Decryption

4.4.1. Key Generation Process

A key generation process consists of some complex mathematical operations. To maintain trust on security we need to keep larger key length.

I am using following notations during explanation of algorithm and mathematical functionality.

Table 4.1 Notations

Notation	Functions
µ	XOR
Ω	XNOR
±	Concatenation

Following are the steps are performed to generate Key

1. In the first move, 64-bit initial cipher key (S_c) is divided into 4 parts each of 64 bit

2. A function F is performed on these 16-bit data. Hence four F functions blocks are used. Initial 16 bits for each function F is obtained by intermixing or substitution process of cipher key as shown in below equation

$$S_{b_{if}} = \sum_{j=1}^{4} S_{c_{4(j-1)+i}} \tag{4.1}$$

3. In next step, I passed the 16-bit of $\left(S_{b_{if}}\right)$to f-function to get $S_{a_{if}}$.

$$S_{a_{if}} = f\left(S_{b_{if}}\right) \tag{4.2}$$

4. F-function is comprised of two tables P and Q. These tables perform non-linear and linear transformations which produce diffusion and confusion.

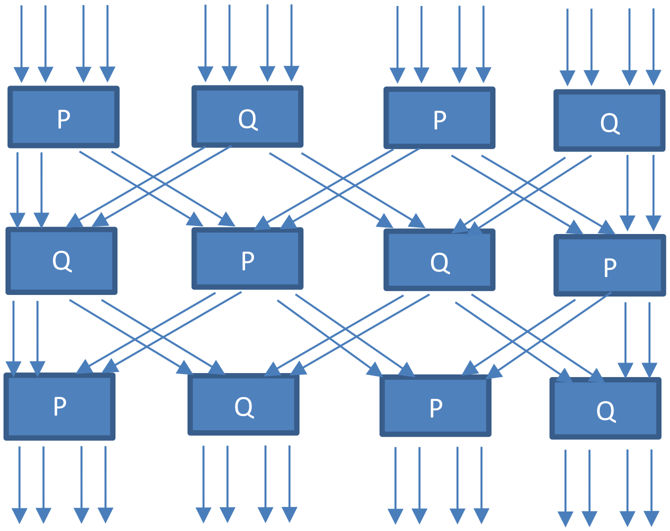


Fig. 4.5 Nonlinear and Linear transformations function (F –function)

5. Transformation made using P and Q.

Table: 4.2 P - table

S_{ci}	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$P(S_{ci})$	F	8	7	0	5	E	C	B	D	A	9	6	4	3	2	1

6. Each f-function output is arranged in 4x4 matrix. And named these matrices Sm as shown in below.

$$S_{m1} = \begin{bmatrix} Sa1f1 & Sa1f2 & Sa1f3 & Sa1f4 \\ Sa1f5 & Sa1f6 & Sa1f7 & Sa1f8 \\ Sa1f9 & Sa1f10 & Sa1f11 & Sa1f12 \\ Sa1f13 & Sa1f14 & Sa1f15 & Sa1f16 \end{bmatrix} \tag{4.3}$$

$$S_{m2} = \begin{bmatrix} Sa2f1 & Sa2f2 & Sa2f3 & Sa2f4 \\ Sa2f5 & Sa2f6 & Sa2f7 & Sa2f8 \\ Sa2f9 & Sa2f10 & Sa2f11 & Sa2f12 \\ Sa2f13 & Sa2f14 & Sa2f15 & Sa2f16 \end{bmatrix} \tag{4.4}$$

$$S_{m3} = \begin{bmatrix} Sa3f1 & Sa3f2 & Sa3f3 & Sa3f4 \\ Sa3f5 & Sa3f6 & Sa3f7 & Sa3f8 \\ Sa3f9 & Sa3f10 & Sa3f11 & Sa3f12 \\ Sa3f13 & Sa3f14 & Sa3f15 & Sa3f16 \end{bmatrix} \tag{4.5}$$

$$S_{m4} = \begin{bmatrix} Sa4f1 & Sa4f2 & Sa4f3 & Sa4f4 \\ Sa4f5 & Sa4f6 & Sa4f7 & Sa4f8 \\ Sa4f9 & Sa4f10 & Sa4f11 & Sa4f12 \\ Sa4f13 & Sa4f14 & Sa4f15 & Sa4f16 \end{bmatrix} \tag{4.6}$$

7. Then these 4 matrices are arranged in array of 16 bits and we get round key(Sr). This bit’s arrangement is shown by the equation.

$$S1 = a4 \pm a3 \pm a2 \pm a12 \pm a8 \pm a7 \pm a11 \pm a9 \pm a10 \pm a13 \pm a1 \pm a5 \pm a6 \pm a16 \pm a15 \pm a14 \tag{4.6}$$

$$S2 = b1 \pm b2 \pm b14 \pm b10 \pm b7 \pm b11 \pm b5 \pm b9 \pm b13 \pm b15 \pm b6 \pm b3 \pm b16 \pm b12 \pm b8 \pm b4 \tag{4.7}$$

$$S3 = c8 \pm c10 \pm c11 \pm c12 \pm c16 \pm c15 \pm c14 \pm c2 \pm c1 \pm c7 \pm c5 \pm c6 \pm c9 \pm c3 \pm c4 \pm c13 \tag{4.8}$$

$$S4 = d13 \pm d6 \pm d10 \pm d9 \pm d5 \pm d15 \pm d14 \pm d3 \pm d1 \pm d2 \pm d4 \pm d8 \pm d7 \pm d11 \pm d12 \pm 16 \tag{4.9}$$

8. Then I performed XOR operation among 4 round keys and get fifth key as shown below

$$S_{m5} = \mu\,{}^{4}_{1}(S_i) \tag{4.10}$$

Table: 4.3 Q - Table

S_{ci}	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$Q(S_{ci})$	7	6	8	E	B	0	4	F	2	C	3	D	1	A	9	5

4.4.2. Encryption Process

Once Key is generated we use that key to encrypt the data. Now I consider input data is given in length of 2 w-bit let suppose P and Q. Till now expansion of key has been performed. Array of S[0…m-1] is computed. Following is the pseudo-code for the algorithm.

```
P= P+S[0];
Q=Q+S[0];

For i =1 to r do
    P = ((P µ Q) <<<Q + S[2*i];
```

Q = ((Q µ P) <<<Q + S[2*i+1];

As the result of this algorithm output will be in P and Q registers.

This is a very simple algorithm to implement. This RC5 base algorithm where both registers get updated. This is dual faster than DES algorithm. In DES algorithm only one register gets updated in one round.

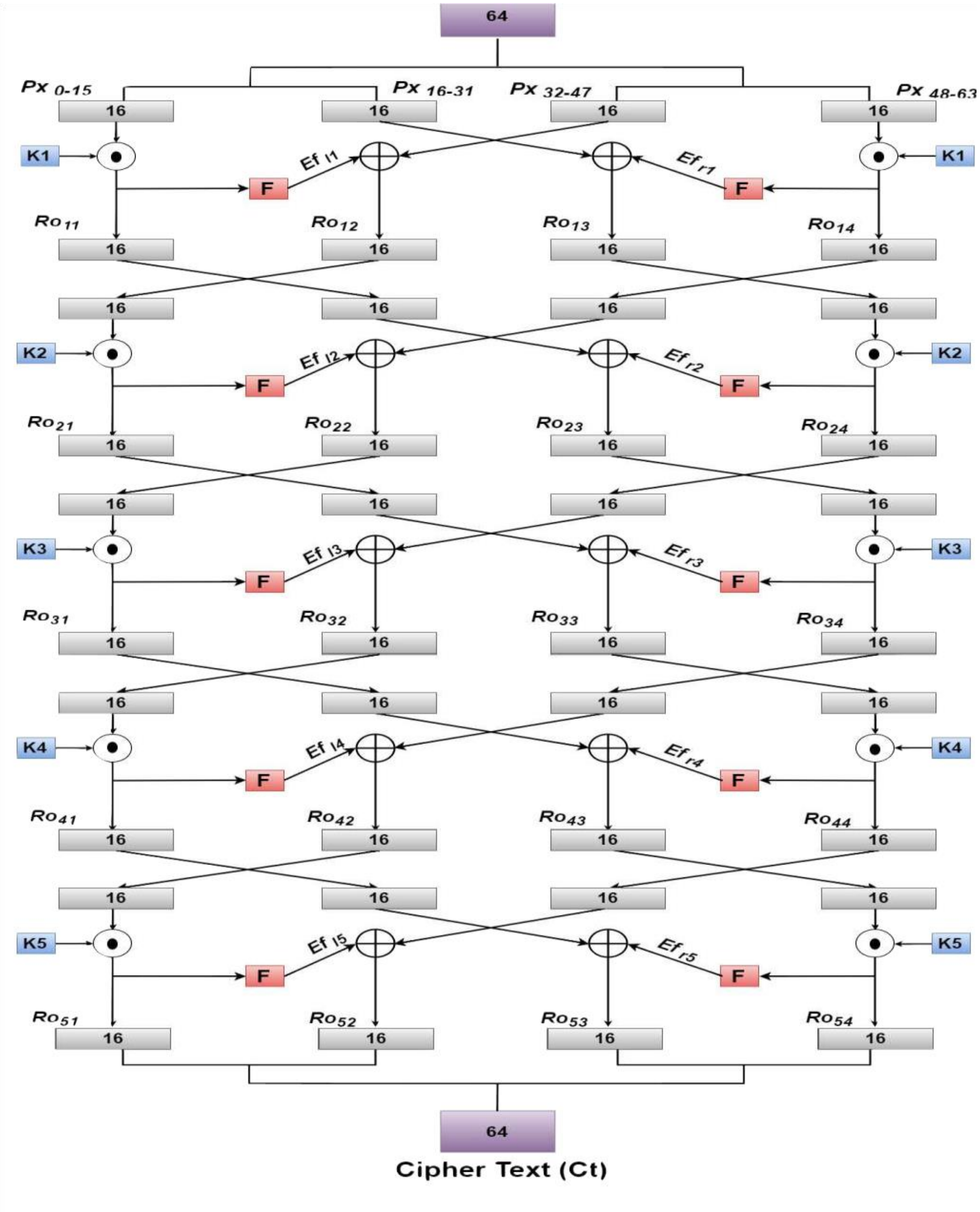


Fig. 4.6 Encryption Process

4.4.3. Decryption Process

Decryption process is just opposite to encryption process and can be easily derived from it.

Following is the algorithm for the decryption process.

```
For i =r to 1 do
    Q = (Q- S[2*i+1]>>>P) µ P;
    P = (P+ S[2*i])>>>Q) µ Q;
P= P - S[0];
Q=Q - S[0];
```

CHAPTER 5

Experiment and Result

On implementing above approach, we can authenticate and encrypt data.

Now let data is generated by PUF enabled sensor is represented below. It is the hexadecimal conversion of binary data.

Plain text: ABCDDCBAABCDDCBAABCDDCBAABCDDCBA
Key is: HF9EKD9KDEG34F35F7POJ34FDDGDHSAG

Cipher Text: LHJSOJEOIUEOIJJOODUEIP3JNDIOJD3U3SDSSF

Next round

Plain text: HJSOJEOIUEOIJJOODUEIP3JNDIOJD3U3SDSSF
Key is: HF9EKD9KDEG34F35F7POJ34FDDGDHSAG

Cipher Text: DOJNFOSHBNFHUDDOHNCLDFLDNFFDDHDZ

CHAPTER 6 Conclusion

This project proposed the security and authenticity of sensors with the help of PUF enabled sensors. This PUF help to authenticate sensors and also encrypt the generated data which help to protect it from monitoring air traffic where sensors are deployed. Further light weight encryption algorithm are used to encrypt the data at local internet enabled IoT based device. It helps end user to protect its own important data instead depending on and fully trusting other stack holders.

My experiments result shows that encouraging performance for faster encryption with authentication of generated data by authenticating sensors which generate it. It is a strong approach to ensure authenticated data and secure transfer of it to cloud storages.

This approach mainly relied on PUF enabled sensors and light weight encryption algorithm.

References

[1] D. Pishva, "Internet of Things: Security and privacy issues and possible solution," in *International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, South Korea, 2017.

[2] D. Mukhopadhyay, "PUFs as Promising Tools for Security in Internet of Things," in *IEEE Design & Test*, India, 2016.

[3] B. Halak, M. Zwolinski and M. S. Mispan, "Overview of PUF-based hardware security solutions for the internet of things," in *IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Abu Dhabi, United Arab Emirates, 2017.

[4] S. Horrow and A. Sardana, "Identity management framework for cloud based internet of things," in *Proceedings of the First International Conference on Security of Internet of Things*, Kollam, India, 2012.

[5] R. Vilalta, R. Ciungu, A. Mayoral, R. Casellas, R. Martinez, D. Pubill, J. Serra, R. Munoz and C. Verikoukis, "Improving Security in Internet of Things with Software Defined Networking," in *IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, 2016.

[6] J. Liu, Y. Xiao and C. L. P. Chen, "Authentication and Access Control in the Internet of Things," in *32nd International Conference on Distributed Computing Systems Workshops*, Macau, China, 2012.

[7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,* vol. 4, no. 5, 2017.

[8] S. Sklavos and I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations," in *IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Larnaca, Cyprus, 2016.

[9] H. Tao and W. Peiran, "Preference-Based Privacy Protection Mechanism for the Internet of Things," in *Third International Symposium on Information Science and Engineering*, Shanghai, China, 2011.

[10] R. L. Rivest, "THE RC5 ENCRYPTION ALGORITHM," CAMBRIDGE, 1997.

[11] M. Usman, I. Ahmed, M. A. Aslam, S. Khan and U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 8, no. 1, 2017.