International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

A Survey on Securing IOT Based Devices Using Cryptanalysis

Saumya Priya

School of Computing Science, Galgotias University, Greater Noida, India

Abstract: ***With the advancement of technologies in last few decades, the need and use of IOT devices has been increasing drastically. Internet of Things (IOT) refers to the physical devices around the globe that are connected over the internet that helps us to share the data conveniently and accurately. The main components of any IOT device are sensor, actuator and computer devices which are attached to a particular object that is connected to internet and helps in transfer of data from source to destination. There is no denying the fact that IOT devices play vital role in providing a good quality of life but at the same time it is very important to provide security to an IOT device such that our confidential information cannot be hacked. In this research paper, we will see various cryptographic algorithms that provide security to IOT devices in order to protect it from security attacks.***

Keywords: IOT, security attacks, cryptography, SIT algorithm, IDEA algorithm, blowfish algorithm, RSA algorithm

1. Introduction

The term internet of things (IOT) was first coined in 1998. IOT refers to uniquely identifiable objects, things and their virtual representations over the internet [1]. IOT works as an interface between different machines and helps them in interaction known as machine to machine interaction. With the more and more use of IOT devices in our day to day life, we can save our time and complete our work more efficiently. The connectivity is not only limited to laptops and smartphones but it's going towards connected gadgets, cars, smart home, smart cities, healthcare, accessories etc. Basically, IOT devices provide connectivity across the world.

1.1. Architecture of IOT Devices

IOT is a network of devices that can sense, accumulate and transfer data over the network without any human intervention. Architecture of IOT is divided into four stages.

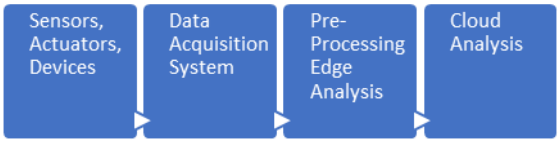


Figure: Architecture of IOT Device

Sensors and Actuators help to emit access and process the signal. Data processed by sensor is in analogue form. Data Acquisition Systems converts analogue streams into digital form and aggregates it for further use. Edge Analytics performs the pre- processing of data. Data is then forwarded to cloud- based system.

1.2. Security in IOT

Security is one of the major aspects that must be kept in mind while designing any IOT device. To prevent the confidential data that we share over the internet it is very important to apply some security algorithms. Security Attacks are further divided into active attack and passive attack. In case of active attack, attacker modifies the data to mislead the user while in case of passive attack; attacker collects the important information and uses it further but does not affect system resources.

2. Literature Survey

Cryptography is defined as hiding the code in order to provide security. The prefix "Crypt" means "hidden" and "Graphic" means "writing". It is simply the study of techniques for secure data transmission between sender and receiver such that any unauthorised person can't access the data. Let us consider a scenario where a person "X" sends some piece of information to "Y" over the internet, meanwhile a person "Z" somehow manages to get the access of data before the receiver. In this situation Y can change the data or can use the confidential information for some cryptographic algorithms are used to provide security.

Sender sends the information in form of plain text. Plain text is converted into Cipher text with the help of Key. Conversion of plain text into cipher text is known as encryption. Cipher text is sent to the receiver, receiver decrypts the message with the help of key. Conversion of cipher text into plain text is known as decryption. Key is piece of information used to determine functional output of cryptographic algorithm [2]. Cryptography is further divided into two categories:

Symmetric Key Cryptography is a cryptographic technique where there is only one key known as public key is used for both encryption and decryption technique. Private Key cryptography is another name of symmetric cryptography.

Asymmetric Key Cryptography or public key cryptography is a process where we use one public key and one private key for encryption and decryption process. Plain text is converted into cipher text with the help of sender's private key. Encrypted message is sent to the receiver and is converted to plain text with the help of public key. Private Key is not known to sender only while public key is known to both sender and receiver.

3. Cryptographic Algorithm

Secure IOT (SIT) Algorithm

SIT is a lightweight encryption algorithm that provides security to IOT devices. We use a fixed length key in SIT algorithm for encryption and decryption. Length of key is 64 bits. Block cipher of 64 bits is generated after encryption. Five feistal rounds are used for encryption in SIT algorithm. Security is achieved using feistal rounds and uniform substitution – permutation network [3].

Advantages

- SIT is a key sensitive algorithm i.e. we cannot get the original data if some change is made in the key even with slight difference.
- This algorithm takes less execution time for encryption and decryption of data.
- SIT is a cost effective algorithm as it is executed on an 8 bit micro controller. Cost of 8 bit microcontroller is less than other micro controllers.
- It provides security in IOT devices and protects the device from threats.

4. Future Work

Performance of SIT algorithm can be improved if it will be executed on different hardware platforms. FPGA is a hardware that will optimize the performance by providing high throughput. Use of variable length key instead of fixed 64 bits key can provide better scalability and performance to secure IOT algorithm.

IDEA Algorithm

International Data Encryption Algorithm (IDEA) is a replacement for Data Encryption Standard (DES) algorithm. Initially, IDEA algorithm was known as Improved Proposed Encryption Standard algorithm. In 1991, James Markey and Xuejia Lai explained this algorithm for the first time. IDEA algorithm is used in symmetric key cryptography. Key size is of 128 bits .52 subkeys are generated from 128 bit key. Circular left shift operation is used for generating subkeys in different rounds. There are eight identical transformation rounds, each round uses six subkeys and each subkey is of 16 bit. After eight rounds, one half round is performed which is also called as output transformation. Four subkeys are used in last round. 64 bits plain text is taken as input and eight and half rounds of IDEA algorithm are executed. After that we get 64 bit block cipher as output. This process is known as encryption.

Advantages

- Execution time for IDEA algorithm is than asymmetric cryptography algorithms.
- It is easy to implement as simple Addition, XOR and Multiplication operations are used in each round.
- Key length is of 128 bits and circular left shift operation is used in each round. So it is difficult to break for the attackers.

Disadvantages

- IDEA algorithm keeps the information confidential but does not guarantee about authenticity and integrity of data.
- It is difficult to manage keys when number of user increases.
- A secure out of band medium is needed to share the keys between sender and receiver.

Blowfish Algorithm

Bruce Schneier introduced Blowfish algorithm in 1993 for network security. Blowfish algorithm is replacement for Data Encryption Standard (DES) and IDEA algorithm. It is a symmetric cryptographic algorithm in which only one key of variable length is used for both encryption of plain text and decryption of cipher text. For encryption, it takes 64-bit block as plain text and for decryption it takes 64-bit block cipher. It is also known as 64-bit block cipher algorithm. Encryption rate of blowfish algorithm is faster than other cryptographic algorithms. In Blowfish algorithm:

- Block size is of 64 bits.
- Length of key is not fixed. It varies from 32 bit to 448 bits.
- Number of subkeys = 18. P array is initialized.
- Number of Rounds = 16
- Number of Substitution boxes = 4.

Working of Blowfish Algorithm:

Step 1: key should be ready before encryption and decryption takes place. Key is kept inside an array. K_1, K_2, K_3……K_n [1<=n<=14]. Length of each index of array is of 32 bits.

Step 2: P array is initialized. Hexadecimal values are used to initialize the subkeys. In P array, we store 18 subkeys and each array element contains 32 entries.

P[1] = P[1] XOR K_1
P[2] = P[2] XOR K_2]
P[3] = P[3] XOR K_3…P[14]=P[14] XOR K_{14}
P [15] = P[15] XOR K_1
P[16] = P[16] XOR K_2…P[18] =P[18] XOR K_4

These values are further used for encryption and decryption.

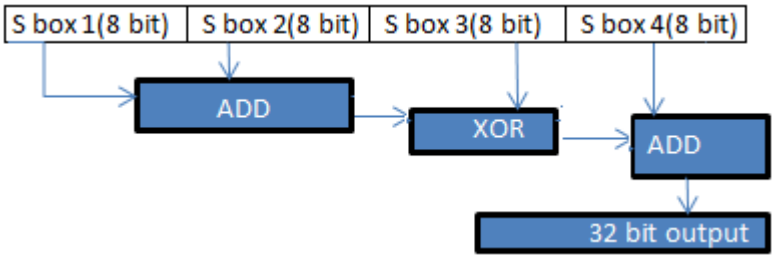
Step 3: Four substitution boxes (s boxes) are initialized. S box contains 256 entries having 32 bit in each entry. Only hexadecimal values are stored inside s box.

Encryption:

64-bit plain text is taken as an input. These 64 bits are then divided into left 32 bits and right 32 bits. Left 32 bits and P[1] undergoes XOR function and the resultant becomes right 32 bits for second round. Then the output goes inside the function F. The output of function F and right 32 bits undergoes XOR operation and the resultant becomes left 32 bits for round 2. In second round P[2] is used as subkey. This process continues till round 16. In last round, we concatenate the left 32 bits and right 32 bits and we get the cipher text of 64 bits.

Working of function:

32-bit input is divided into four parts (s boxes). Each s box takes 8 bits as input.



Advantages
Blowfish algorithm helps us to secure the data. This algorithm takes very less time for its execution. It requires less memory for its execution. It is simple as it uses basic XOR and addition modulo operation.

Disadvantages
Blowfish algorithm does not check the authenticity and integrity of the data that is being sent and received. It takes more time and provides less throughput in comparison to other algorithm while decryption. Key management is complicated when number of user increases.

RSA Algorithm
RSA stands for Rivest Shamir Aldeman. RSA algorithm was developed in 1978. It is an asymmetric key cryptography algorithm in which two keys are used. If we use public key of sender for encryption then we must use private key of sender for decryption or vice versa. Public Key is known to all users while private key is a secret key. RSA algorithm is a block cipher in which plain text and cipher text are integers.

Working of RSA algorithm:

- Select two large prime numbers p and q. large numbers are selected in order to provide better security.
- Calculate the value of n. n=p*q
- Calculate Euler's toitient function (Φ (n)).
  Φ (n) = (p-1)*(q-1)
- Choose the value of e such that Φ (n) and e are co-prime.
  1<e< Φ (n) and gcd (Φ (n), e) =1
- Calculate the value of d.
  $d= e^{-1} \bmod \Phi(n)$
- Public key ={ e, n}
- Private key ={d, n}
- Encryption:
  $C=P^e \bmod n$. Here C is cipher text and P is plain text.
- Decryption:
  $P =C^d \bmod n$. Length of plain text should be less than n.

Advantages:
It is easy to implement RSA algorithm than Elliptical Curve cryptography (ECC). Message can be authenticated easily. It checks the data repudiation by providing digital signature.

Disadvantages:
Key generation in RSA algorithm is a slow process. Complex mathematical functions are used so it is difficult to implement RSA algorithm. In this algorithm, anyone can get access to public key very easily.

5. Conclusion

In future, the use of IOT device will rise exponentially so it is important cryptographic algorithm to protect our data from threats. Various cryptographic algorithms are used to protect our confidential information on hardware or software platforms.

References

[1] R. H. Weber,"Internet of things – new security and privacy challenges," Computer Law and Security Review, vol. 26, pp.23-10, 2010.
[2] https://en.wikipedia.org/wiki/Key_(cryptography)
[3] Muhammad Usman, Irfan Ahmed, M.Imran Aslam, Shujaat Khan and Usman Ali Shah, "SIT: A lightweight encryption algorithm for secure internet of things," IJACSA, vol. 8, 2017
[4] Okamura Toshihiko, NEC Technical Journal, vol. 12(2017).
[5] www.geeksforgeeks.org/blowfish-algorithm-with-examples/amp
[6] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi" Security in the Internet of Things," A Review, ICCSEE, 2012.
[7] D.M. Trivedi, T.J. Raval, "Proposed Cryptographic Approach for Securing IOT Device," USRSET, 22-01, 2018.
[8] blog.storagecraft.com/5-common-encryption-algorithms