International Journal of Engineering & Technology, 7 (4.6) (2018) 418-422

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Secure and Lightweight Cryptographic Scheme for Iot Based Applications

R.Aakash[1*], Dr.M.B.Mukesh Krishnan[2]

[1]*PG Student - SRM Institute Of Science And Technology, Chennai, India*
[2]*Associate Professor, SRM Institute Of Science And Technology, Chennai, India*
**Corresponding author E-mail: aakash_rb@srmuniv.edu.in*

Abstract

Internet of Things is a collection of devices like home appliances and automobiles considering anything that is fixed with electronics, software applications and sensors which can be used to bridge the gap between physical world and a computerised system allowing direct connections between the two thereby reducing the human efforts and provides future enhancements and other economic benefits. With the recent development in IOT and the increase in the usage of wireless technologies gives us a chance for growth in various applications like Education, Agricultural benefits and other Medical sectors. With the increase in the use of IOT with the incorporation of wireless technologies there is an increase in security threats against secrecy and privacy and are often prone to breaches that cause access points to those data vulnerable to attacks. Therefore we need an authentication scheme that is both energy efficient and not resource clogging which also provides methods to transfer data with no issues to confidentiality which is a major concern to the users. We need a light-weight cryptographic algorithm that offers protection against various attacks including Man in the Middle attack and Masquerading attacks.

Keywords: *Authentication; Lightweight Cryptography; Internet of things;*

1. Introduction

Internet of Things is a collection of devices like home appliances and automobiles and other items that is fixed with electronics, software applications and sensors which can be used to bridge the gap between physical world and a computerized system allowing direct connections between the two thereby reducing the human efforts and provides future enhancements and other economic benefits. With the recent development in IOT and the increase in the usage of wireless technologies gives us a chance for growth in various applications like Education, Agricultural benefits and other Medical sectors. With the increase in the use of IOT with the incorporation of wireless technologies, there is an increase in security threats against secrecy and privacy and are often prone to breaches that cause access points to those data, vulnerable to attacks. Traditional cryptographic algorithms cannot be directly used on IOT devices because the size of the key, the no. of rounds and the no. of keys being used has much larger resource intake and high power consumption which cannot be used on low resource and less memory intake devices. So it is not possible to use any of the traditional existing cryptographic algorithm in devices that has limited resource, small memory size and only supports very low power consumption. Therefore we need an authentication scheme that is both energy efficient and not resource clogging which also provides methods to transfer data with no issues to confidentiality which is a major concern to the users. The is a need for a lightweight cryptographic scheme which is nothing but a protocol that can be used for implementation in IOT devices like medical care devices and RFID sensors and other smart cards that offers protection against various attacks like impersonation attacks and man in the middle attacks. And another thing to be considered is that people are often made to choose between the two: cost, productivity and safety. Theoretically, it is easy to choose two of the three design goals of the algorithm but it is practically impossible to choose all the three simultaneously.

2. Requirement Analysis

In IOT applications, the sensors present in it can collect delicate data from the environment and the processed information is given to the users who are eligible to access that data. The raw information that is collected is analyzed and certain decisions are taken. These decisions are very important and should not be tampered with. It is important that the system must satisfy all the properties like confidentiality, authentication of the IOT device and integrity of the data that is being transferred. An attacker can take over a sensor at any point of time and add false data or even the attacker can take over the server and transmit false data to the cloud. Both the sensor and the server has to be authenticated before the data transmission. In addition to it, the authentication protocol has to be lightweight because of the resource constraints of the IOT device. Therefore, there is a need for a design that ensures that the information should be accessible only to users that are authorized to access the data and also must protect users privacy while the services has to be provided as such. In order to face these challenges there is a need for lightweight and a scalable cryptographic scheme that protects sensitive data generated from various IOT devices in a heterogeneous environment.

Copyright © 2018 R.Aakash, DR.M.B.Mukesh Krishnan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

3. IOT Device Challenges

3.1 Energy Consumption

Most of the IOT devices is built with very low resources and constrained energy. Applying cryptographic algorithms depends on the sensor and how the communication actually takes place. Another thing that has to be considered, is the calculation of how the energy consumption affects the available power. The energy spent by the sensor and the microprocessor used for the computation and also the communication between the array of sensors is very much more expensive than the actual computation that takes place inside the sensor. The quantity of the energy actually needed for the cryptographic algorithm should not be calculated separately, it must be calculated as a proportional value to the clock cycles needed for the cryptographic operations or the maximum number of rounds that the encryption uses.

3.2 Memory Occupation

The IOT sensors has very limited memory like the energy resources. For example, considering a project with an IOT sensor fitted with a tiny OS occupies 2400 bytes of memory. It will have only 3600 bytes of memory for the cryptographic application which is not sufficient. This is also another important metric that has to be considered while writing the cryptographic algorithm.

3.3 Execution Time

For example, the medical field always ignores about the security and emphases on the lifesaving and the emergency services part. This may cause information leakage and data breaches which will cause a lot of problems. Therefore the security part of the architecture must also be considered as well as the emergencies. There must be a balance between them. The times it takes to execute an algorithm must also consider the key setup time. That is, the number of round keys required and also the time it takes to generate those keys. The lifetime of the battery and the energy consumption can be minimized by the fast operation of the cryptographic algorithm. We also have to consider all the three parameters like the memory, energy consumption and also the executing time of the algorithm as they affect each other.

4. IOT Security Challenges

4.1 Security and Data Protection

The IOT devices are wireless in nature and they share delicate information which are now publically accessible and they are now vulnerable to attacks like man in the middle attack and other malicious attacks. We need some cryptographic algorithms that ensures that the data is not being tampered with while being transferred wirelessly. Those IOT devices does not have enough power to have traditional algorithms installed. So we need some lightweight cryptographic algorithms that has less energy consumption and should not pose any problems to the efficiency of the system.

4.2 Authentication and Identity management

This is a very important part of any security model. Every node in the network must be able to authenticate other nodes in the network after identifying them. It guarantees the identity of the IOT nodes before any communication happens between them. We need a method to authenticate each node before the actual transfer of data takes place.

4.3 Privacy

Securing the data is very important as the data is very delicate and must not reach the hands of the wrong person. We need to make sure that the users feel comfortable before they transfer any data. Ownership of every node must be established. We must ensure that the data will not be used without the knowledge of the user when transferred over the internet. Each smart node must have supporting policies that must be established before they come in contact with each other and the data transfer happens between them. They must be compatible with each other before transferring any information.

5. Mathematical Methodology

Considering all possible implementations of a given cipher can be ordered according to their algorithm size, RAM size and the time it takes for the execution.
Scenario 1: This consists of both the encryption and decryption and also the key expansion. Consider for a given implementation for a given device d , we can calculate the performance parameter **pi,d** which is the aggregation of all metrics like the RAM size, the execution time and also the size of the code, **vi,di,m** is the value of metric for a given implementation on a device d

$$p_{i,d} = \sum_{m \in M} w_m \frac{v_{i,d,m}}{\min_i(v_{i,d,m})},$$

and **mini(vi,d,m)** is the smallest value of the metric for all the possible implementations of a given device d. We consider the value of **wm** as 1 for both the scenarios. Consider i1, i2, i3 as the implementations of three different devices. We can now calculate the FOM (Figure of Merit) which is the average value of performance of all the three devices.

$$\mathrm{FOM}(i_1, i_2, i_3) = \frac{p_{i_1,AVR} + p_{i_2,MSP} + p_{i_3,ARM}}{3}$$

Scenario 2: We are selecting the best cipher with the best possible implementation. Using the balanced implementation of the above equation we have wm = 1

$$p_{i,d} = \sum_{m \in \{\mathrm{code,\ RAM}\}} w_m \frac{v_{i,d,m}}{\max_i(v_{i,d,m})},$$

maxi(vi,d,m) is the maximum amount of RAM present on the device d.

6. Security against Generic Cryptographic Attacks

Information-theoretic framework is a model used to analyze the security against the attacks like generic cryptographic attacks. It uses the statistical conditions and not the deterministic conditions. Like how an outcome of a dice can be known only after it's actually been rolled, the output of the ideal state cannot be found until its actually being queried. Hence only the amount of information collected is the only required thing than how actually the data is processed. The occurrences of cryptographic attacks are often high and have to be dealt with quickly, considering an hypothesis where two type of errors can take place , either choosing the null hypothesis when its actually the alternative which is correct or choosing the alternate hypothesis instead of choosing the null hypothesis.

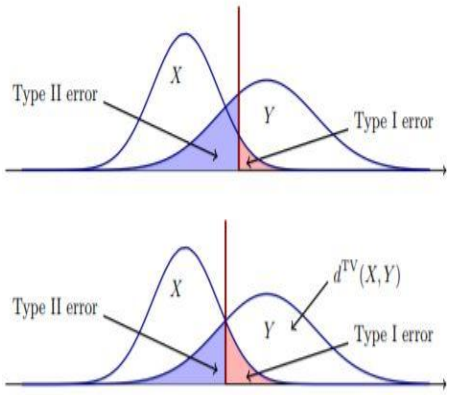


Figure 1: Hypothesis Diagram with respect to ideal world and real world scenario

The information-theoretic framework not only significantly rationalizes the security analysis; it can be used even if the algorithm is changed in the future like if any future enchantments are made. For example the collision resistance is calculated by analyzing on how many messages does it actually need for the collision to happen with adequately high probability and not by using the latest updated algorithm to find the collision effectively. For instance, we know that it is not a compulsion to save all the data and its hash values in the table. Collisions for messages which are significant are found to be with lower memory requirements even when parallel implementation is done. We can find the difference between the real and ideal world conditions by something called as total variation distance which is written as follows,

Total Variation Distance: Consider two random variables X and Y on a given finite set Ω. The total variation distance between the two variables is given below,

$$d^{\mathrm{TV}}(X,Y) \triangleq \max_{A \subset \Omega} |\Pr[X \in A] - \Pr[Y \in A]| \ .$$

The total variation distance is the relation between the ideal world and real world basically a distance between two probability distributions and the total variation distance is value of whether the hypothesis will actually choose the right decision that also that depends on whether the probability of the error occurring is low. We have another term called as maximum adversarial advantage that is equivalent to total variation distance used to calculate the distance between two probability distributions which is given below,

Maximum Adversarial Advantage: Consider two random variables X and Y on a given finite set Ω. It does not matter whether the algorithm is probabilistic or deterministic. The input is x ∈ Ω and output is either 1 or 0 which is denoted by a variable A, and let A ∈ A. The Maximum Adversarial Advantage is given as follows,

$$d^{\mathrm{Adv}}(X,Y) \triangleq \max_{\mathcal{A} \in \mathbf{A}} |\Pr[\mathcal{A}(X) = 1] - \Pr[\mathcal{A}(Y) = 1]| \ .$$

There are a lot of pre-existent methods to calculate the total variation distance, including Patarin's H-coefficient and coupling.
We need to consider two types of queries for encryption and authentication:

- D-queries: This refers to the key which is not known to the attacker. For instance, a symmetric block encryption that has a secret key for encryption/decryption.
- T-queries: This does not possess a secret key. For instance, considering the same symmetric block encryption but there is no secret key still given to the adversary as an extra input.

The number of D-queries is kept as D which is referred as the data complexity and the number of available T-queries is kept as T which is known as the time complexity. The time complexity during the actual process is often higher.

7. Lightweight Mutual Authentication

Authentication plays an important role in providing the first line of security between the user and the server. It also protects all the devices in the network. Before starting the session in an uncertain environment, authentication has to take place between the two sides to verify the identity of the devices. Using a smart card also solves drawbacks of using only the password as the authenticating factor. Authentication using smart cards provide great application and slowly becomes a research source. A lightweight mutual authentication is a method of providing a way to authenticate each other device identity without using a lot of resources of the IOT device. The method must be a short communication with very low computational power required and also provides good security. But, if there is any presence of a backdoor or a vulnerability in the defective authentication method can cause an adversary to attack. It is very tough to find these vulnerabilities unless a thorough cryptanalysis process is done. Therefore, we need a new lightweight independent authentication scheme that must have these functionalities included
Secrecy - Even when one of the messages gets compromised, it should not affect the other messages. A single particular value must not compromise the entire message stream
Anonymous user - The user's identity is kept very secure that means no passwords or verification tables must be stored and during the transmission there must be no plaintext transfer of data during the authentication procedure.
Mutual verification - The methodology must provide methods for both sides of the communication to verify. That is the server must be able to verify the user and vice versa
Session key - The methodology should deliver session key for messages during the exchange.

8. Proposed Methodology

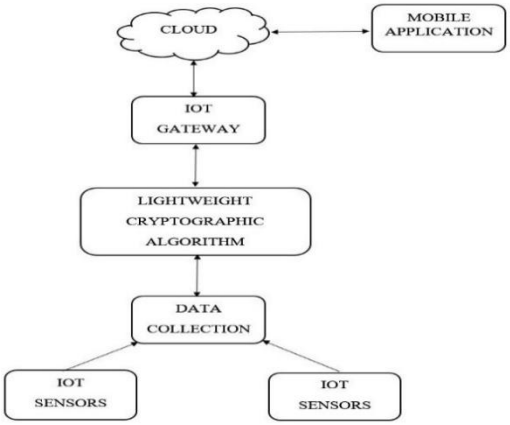


Figure 2: Architecture Diagram

8.1 Data collection

We know that an IOT device has three main components, Hardware layer, Middleware layer and Presentation Layer. Hardware layer has the collection of sensors, the middleware layer has tools required for computation and storage and the presentation layer includes the tools accessible by different platforms. It is very difficult to collect all the data that is collected from billions of sensors so the middleware layer is used by the sensor to choose the most important data which is need for the processing. Consequent-

ly the IOT architecture does not provide the abundant storage to accomplish the required actions in the process of authentication and integrity of data. For instance, taking an RFID tag we cannot achieve the process of constant communication between the device and the server and also the communication between the nodes,. Confidentially has to be provided where the data is not tampered with and the originality of the data has to be preserved. No alteration must go unseen. An RFID tag mostly remains unused for a long amount of time so it is easier for adversary to access the data stored in the memory and tamper it so the entire operation gets ruined.

8.2 Lightweight Cryptographic Scheme

A. Key Expansion - The most important part in the process of encryption/decryption is the key because the entire data security depends on the key. If the adversary gets to know about the key the secrecy/privacy of the data is lost. Hence necessary action has be taken in making the intensity of the key as difficult as possible to crack. For instance, the encryption of a fiestal cipher since it consists of several rounds and each rounds requires a different key. The encryption/decryption of the lightweight algorithm requires 10 rounds so we need 10 different keys for each round. We need a key expansion block that is used to create 10 unique keys from the given primary key. The key expansion operations will produce confusion and diffusion on the given primary key and will create ten different keys for each round. These keys which are generated are used in the encryption and decryption process which will remain tough to crack during the attack. To provide security against brute force attacks and exhaustive search attacks, we need the primary key kt to be of 64 bit length so the amount of tries an attacker has to perform to crack the key is more than 2 kt-1 times. Suppose we have a lightweight cryptographic algorithm that is about 64 bit block size. The key which is of size 64 bits is obtained from the user and this will be the input to the key expansion block. The key expansion block will have a lot of operations including confusion and diffusion and the output of this will have 10 unique keys for the five rounds of the algorithm.

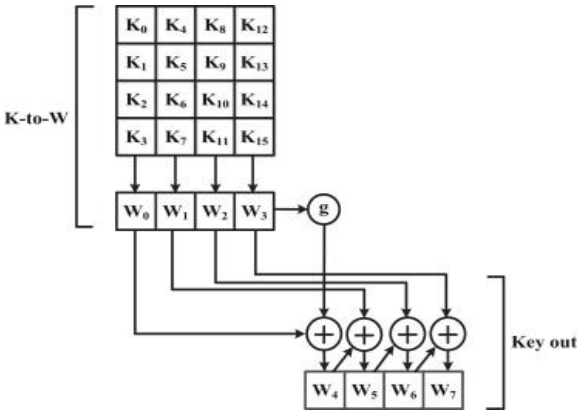


Figure 3: Example Key Expansion diagram

B. Lightweight Cryptography – This is the lightweight cryptographic algorithm that much be suitable for reserved environments like health care sensors, RFID cards and portable devices like smart watch. The lightweight cryptographic algorithm must work on devices that has very limited resources and must not decrease the efficiency of the device at the same time must provide the best in the forms of secrecy and privacy. In general a cryptographic algorithm must of 80 or 128 block size but this is of about 64 bit block size with a 64 bit cipher key because of the significantly reduced amount of resources available in the device. Typically a healthcare application will have about 128 bit block size and other IOT applications will have about 64-128 bit security. We need the lightweight cryptographic algorithm must be fast and compact and also less power consuming which actually providing the required amount of security for the users.

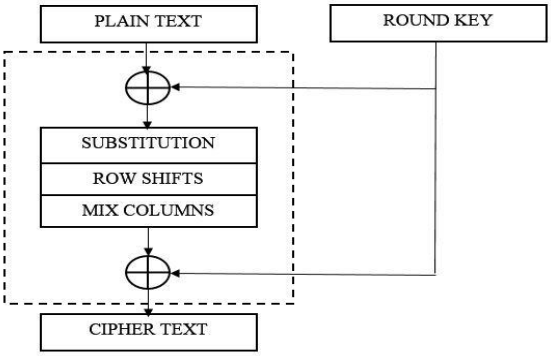


Figure 4: Round Function

9. IOT Gateway

A few sensors will produce a large number of data points every second. A gateway will provide a place to pre-process that information locally at the edge before sending it to the cloud. At the point when the information is aggregated, summarized and tactically analysed at the edge, it diminishes the volume of information that should be sent to the cloud, which hugely affects reaction times and system transmission costs. Another advantage of an IoT entry way is that it can give some extra security to the IoT network and the information it transports. The gateway often regulated the information from being transferred in both the directions, it also protects the data which is transferred to the cloud from data breaches and leakage and also protects the IOT nodes from being compromised by malicious adversaries with detection against data tampering, and random number generators and also modifying the crypto engines.

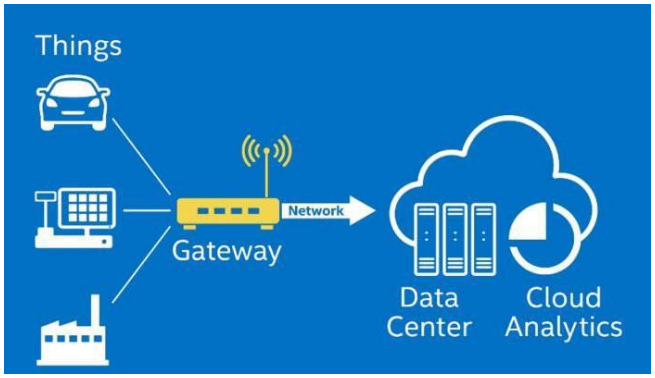


Figure 5: IOT Gateway Scenario

10. Conclusion

Internet of Things is a collection of devices like home appliances and automobiles and other items that is fixed with electronics, software applications and sensors which can be used to bridge the gap between physical world and a computerized system allowing direct connections between the two thereby reducing the human efforts and provides future enhancements and other economic benefits. The IOT provides the complete automation of everything which is around us. Even though there has been lost of research done around IOT and its applications there is always a lot more to explore in it. With the increase in the amount of attention by various industries and government, there has been a lot of research

done in this field and has resulted in various successful projects. Considering some of the constraints in IOT like the architecture and the secrecy and data privacy has attained a lot of attention. While there are some other concerns like the reliability, the performance and also the availability of resources which still need a lot more of consideration. There is a requirement of a method or an approach that ensures that the data is accessible to only the authorized users. They must also provide protection of user's privacy and anonymity. To overcome all these challenges we need a lightweight cryptographic scheme that protects data from adversaries also providing the proper functionality of the IOT devices in a heterogeneous environment.

Acknowledgement

This research is supported by SRM Institute of Science and Technology that provides insight and expertise that greatly assist the research

References

[1] Nan Li , Dongxi Liu, and Surya Nepal, "Lightweight Mutual Authentication for IoT and its Applications", August 2015
[2] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in Ninth International Conference, on Computational Intelligence and Security, Dec. 2013, pp. 663-667.
[3] Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," in Cryptographic Hardware and Embedded Systems - CHES 2007 Lecture Notes in Computer Science, Springer, 2007, pp. 450-466
[4] Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. 54(15), 2787–2805 (2010)
[5] Baysal, A., Sahin, S.: RoadRunneR: a small and fast bitslice block cipher for low cost 8-bit processors. In: Güneysu, T., Leander, G., Moradi, A. (eds.) Lightweight Cryptography for Security and Privacy—LightSec 2015, Volume 9542 of Lecture Notes in Computer Science, pp. 58–76. Springer, Berlin (2016)
[6] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013)
[7] Schwabe, P., Stoffelen, K.: All the AES you need on Cortex-M3 and M4. In: Avanzi, R.M., Heys, H.M. (eds.) Selected Areas in Cryptography—SAC 2016, Volume 10532 of Lecture Notes in Computer Science, pp. 180–194. Springer, Berlin (2017)
[8] C. H. Lim and T. Korkishko, "mcrypton–a lightweight block cipher for security of low-cost rfid tags and sensors," in Information Security Applications. Springer, 2005, pp. 243–258
[9] Bogdanov A, Knežević M, Leander G, et al. {SPONGENT}: the design space of lightweight cryptographic hashing. IACR Cryptology ePrint Archive, 2011:697.
[10] Buchanan WJ, "SPONGENT." [Internet]. Available from: http://asecuritysite.com/encryption/spongent.
[11] W. Zhang et al., "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," in Science China Information Sciences, 2015, vol. 58(12), pp. 1-15.
[12] European Network of Excellence in Cryptology (ECRYPT II). Implementations of Low Cost Block Ciphers in Atmel AVR Devices.http://perso.uclouvain.be/fstandae/source_codes/ lightweight_ciphers (2015)
[13] Evans, D.: The Internet of Things: How the Next Evolution of the Internet is Changing Everything. Cisco IBSG white paper, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411 FINAL.pdf (2011)
[14] Feldhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong authentication for RFID systems using the AES algorithm. In: Joye, M., Quisquater, J.-J. (eds.) Cryptographic Hardware and Embedded Systems—CHES 2004, Volume 3156 of Lecture Notes in Computer Science, pp. 357–370. Springer
[15] Gligor, V.D.: Light-weight cryptography—How light is light? Keynote presentation at the Information Security Summer School, Florida State University. Slide deck, http://www.sait.fsu.edu/ conferences/2005/is3/resources/slides/gligorv-cryptolite.ppt (2005)
[16] https://infoscience.epfl.ch/record/203923/files/llncs.pdf
[17] http://www.cryptolux.org/index.php
[18] https://www.cosic.esat.kuleuven.be/summer_school_albena/slides/ Andrey_lightweight-bc.pdf
[19] https://eprint.iacr.org/2015/303.pdf
[20] http://lightweightcrypto.org/present/present_ches2007.pdf
[21] https://arxiv.org/pdf/1704.08688.pdf
[22] http://www.math.clemson.edu/~sgao/papers/crypto_mod.pdf
[23] https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html
[24] https://orbilu.uni.lu/bitstream/10993/33803/1/thesis.pdf
[25] https://link.springer.com/article/10.1007%2Fs13389-018-0193-x