International Journal of Engineering &Technology, 7 (1.7) (2018) 10-14

International Journal of Engineering & Technology

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

Review paper



An investigation on cryptographic algorithms usage in IoT contexts

R H Aswathy [1] *, N Malarvizhi [2]

[1] *Research Scholar, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India*

[2] *Professor, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India*

**Corresponding author E-mail: rhaswathy@gmail.com*

Abstract

The broad vision of IoT focuses the highly increasing the electronic devices and application in which leads to the growth of technology. The enormous amounts of constrained devices areinterlinked, communicate and coordinate with each other to fulfill its task.IoT mainly concentrate on low energy, Resourceconstraint, self organization and short range of communication. In this heterogeneous environment of IoT,Privacy and security are the greatest challenge. The secure information exchange is most critical pitfall to ensure the system security.In this paper we discussed and analyzed about various security algorithms likeTriple DES, AES, Blowfish and ECCwith their structure,block size,key generation, number of roundswith differentsettings. In order to analyze the efficiency of all said algorithms, we made an experimenton algorithms works on constrained devices in different contexts, all our experiments shows that ECC is the most suitable security algorithm in IOT contexts.

Keywords: IoT (Internet of Things); AES (Advanced Encryption Standard); ECC (Elliptic Curve Cryptography); DES (Data Encryption Standard).

1. Introduction

Internet of Things is the networking of uniquely identifiable computing device. IoT is initially begat by Kevin Ashton in 1999 and well known to Auto-ID focus, MIT [1].IoT is a system of interrelated computing items, such as RFID tags, sensors, actuators, and cell phones, digital machines, and people that provides the ability to transfer data over a network without requiring human-to-computer or human-to-human interactions.[2].The application of IoT is tremendous such as healthcare, environment surveillance, energy management, building automation, Smart home, smart cities, banking, vehicle monitoring and transportation. According to the report of Garner [3],IoT smart objects will generate more than $300 billion revenue in 2020[2,3].Many no of PC's, smart phones, Tablets reaches around is 7.5 billion by 2020.The communication between the huge network and complex interconnection will generate enormous amount of data. Researches forecasted that each and every human being is surrounded with 50 devices by 2020 and generate massive amount of data. During this generation, the growing IoT technology rapidly faces many challenges and risks. To Deal this enormous data Energy consumption, Encryption and decryption of data, Self organization, and minimum range of communication are the most challenging factors. Researches forecasted that, the Smart City business sector is assessed at several billion dollars by 2020, around 16 billion are spending yearly [4].Along with this, security information transmission is the most critical thing in IoT. Many of the security algorithms are enforced to safe transmission of data. In this ubiquitous network, the input and output function of underlying computation are more tightly coupled with privacy of IoT paradigm. Sensor/actuator-based frameworks have been produced autonomously of the IoT vision of open information sharing. It is important that the security, protection, and individual dangers emerging from open access to information are addressed, assessed and evaluated. The design of most secure and privacy-preserving solution of next generation IoT components is a critical issue. The vulnerability of hyper connected society evolving many protection mechanisms. The earlier cryptographic techniques can be ruptured by modern computation techniques. Many modern cryptographic algorithms are virtually unbreakable and used to protect the connected society without any strong security foundations, threads, malfunction and attacks in the IoT will outweigh its benefits. Protection mechanisms are used in our traditional network is not enough to ensure the security of the digital world. The current security protocols and mechanisms should empower the security goal of IoT.

2. Secure cryptographic algorithms

2.1. AES (Advanced Encryption Standard)

Advanced encryption standard is a block cipher and length is 128 bits. It is developed by Rijndael in1998.AES is very low memory requirements, so that it is more suitable for some restricted environment. AES encryption process is in a 4 * Nb (Nb is equal to the data block length divided by 32, the standard AES is 4 bytes) operation of matrix, , it is also mentioned as the "state", plaintext block is an initial value[5].AES key lengths are 128,192 or 256 bits. In this AES, the single key is used for both encryption and decryption of data. The Key size and block size are chosen individually AES algorithm can accept only block size of 128 bits and 3 keys-128,192,256 bits, based on that standard is to be defined. Substitutions and permutations are using in each round during the

Copyright © 2018 R H Aswathy, N Malarvizhi. 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.

processing of entire data block. Rounds are depending on the size of the key. The process of encryption and decryption is shown in the fig 1 and fig 2. The key size is 128, 192, 256 there are 10, 12, 14 rounds. 128 bit key is used commonly. The main characteristics of AES are to provide the protection against every known attack without compromising the speed, code, compactness and simple in design. AES Repeats 4 major process to encrypt messages. It carries 128 bit block of data and a key, gives cipher text as an output. The processes are substitute bytes, shift rows, mixed columns and add key are shown in fig 3.

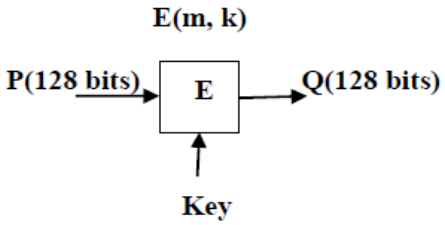


Fig .1: Encryption.

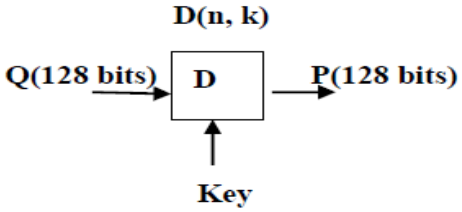


Fig. 2: Decryption.

Substitution bytes: During forward encryption process byte-by-byte substitution process is happened
Shift rows: During the forward process rows of the state array is shifted.
Mix column: During the forward process, the combination of all the bytes in each column is processed independently.

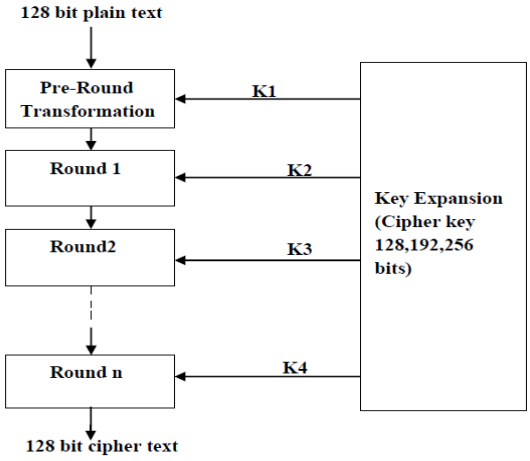


Fig. 3: AES Algorithm.

Add Round Key: During the forward, the round key is added to the outcome of previous process

2.2. Triple DES

Triple Data Encryption standard is a symmetric key block cipher algorithm, advanced version of DES. Three different keys are using the des for the three forms of plain text called key bundles. It is a 64 bit data block. The sequence operation of DES with 3 different keys is Encrypt is shown in fig 4 and decryption is shown in fig 5.

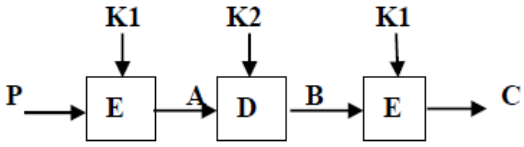


Fig. 4: Encryption.

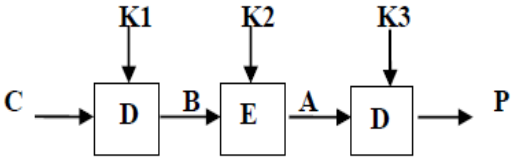


Fig. 5: Decryption.

The keys k1, k2, k3 of 56 bits
Cipher text=Ek 3 (Dk 2 (Ek 1 (plaintext)))
The Decryption processes done in reverse of encryption
Plaintext (P) =Dk 1 (Ek 2 (Dk 3 (Cipher text)))
The encryption and decryption done in 64 blocks of data
Keying option of triple DES
Option I: k 1, k 2, k 3 are independent
Option II: k 1, k 2 are independent k 3= k 1
Option III: All keys are identical ie k 1= k 2= k 3
The block diagram of triple DES is shown in fig 6.

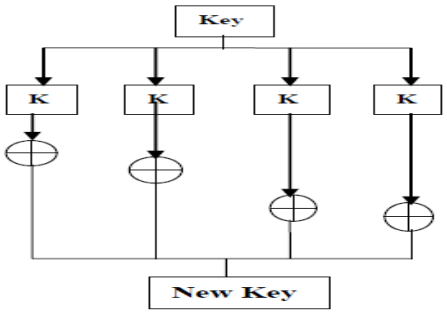


Fig. 6: Block Diagram of Key Generation.

Characteristics of Triple DES are Reliable electronic transaction, secure data communication, secure video surveillance, encrypted data storage and access control mechanism.

2.3. RSA (Rivest Shamir Adleman)

RSA ia a Cryptographic algorithm, In 1976,Ron Rivest, Adi Shamir and leonard Adleman introduced RSA algorithm. It is widely implemented in public key Cryptosystem, known as Digital signature. RSA algorithm is extensively used for popular implementation of public key Infrastructure. In paper [6], the author Mingyuan Xin proposed an algorithm for RSA, to implement a public-key cryptosystem (RSA) by using two public key and some mathematical relation. In the proven methodology of public key crypt system, encryption and decryption procedure of each participant has their own methods. The four procedures that are specific and essential in public key cryptosystem are [2], [6]

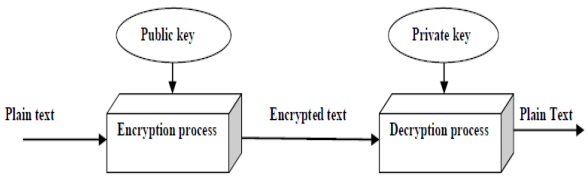


Fig. 7: Key Generation Process in RSA.

a) Deciphering and enciphering the message gives you the original message

D (E (M)) = M
b) Reverse the procedure still returns M
`E (D (M)) = M
c) E and D are easy to compute
d) The publicity of E does not compromise the secrecy of D, user cannot find but D from E.

It is a secure Public Key encryption method and Asymmetric Cryptographic algorithm. Asymmetric Cryptographic algorithm. Different keys are used for encryption and decryption process in Asymmetric method 2.

2.4. Blow fish

Widely used secure algorithm introduced by bruce schneier in the year 1994. .It is worked with block size of 64 bit with variable length key is used for encryption and decryption in blow fish algorithm. It divides the messages into fixed block size. It uses large key dependent S-boxes and is a 16 round feistal cipher, each block column has 62 bit of data. The variable-length key is used from 32 bits to 448 bits, is to provide the data security. In 1993, Blowfish was designed by Bruce Schneier, it is fast and substitute to existing encryption algorithms. [7]

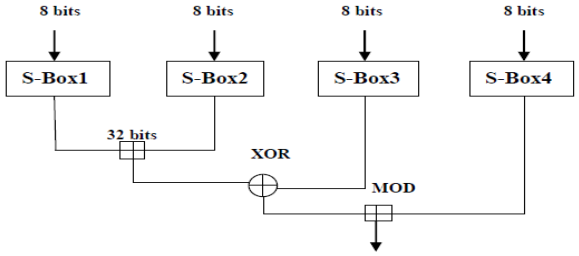


Fig. 8: Blowfish Function.

In this blow fish architecture 32 bit input can be splits into 4 Quarters and 8 bit quarters. The quarters are the input to S-boxes. The mod 2^32 is added with the function output and XORed to produce 32 bit final output. At the end the same process takes place in reverse order for decryption.

The blow fish algorithm is variable key length. The algorithm is divided into 2 subparts key expansion is a first part and data encryption is second one. Data encryption is completely 16 rounds of feistal network. Each round depends on permutation and substitution techniques.

2.5. ECC (Elliptic curve cryptography)

In 1985 Neal Koblitz and Victor S. Miller proposed Elliptic curve (EC) system, which is applied to cryptography. The Eliptic curve's problem uses discrete logarithm is more difficult to solve in finite field. The main fascination of ECC, contrasted with RSA, is that it seems to decreasing overhead and provides equivalent security for a far smaller key size [8]. The key size of ECC is small when compare to RSA or Diffie Hellman algorithm .We present the computation of Elliptic curve by using real numbers. The definition of Elliptic curve over a field E is anon-singular cubic curve with two variable say,f(a,b)=0,with an exact rational value(infinity at certain point. . The general form of elliptic curve defined by an equation form. It generates both public and private key. Key generation by ECC is shown.The Elliptic curve Cryptography is shown in fig 9.

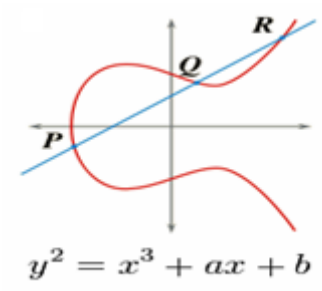


Fig. 9: Elliptic curve Cryptography.

Choose a number'd' within the range of 'n', by applying the below equation to generate a public key
d=Random value, lies within the range of (1 to n-1)
p=point of curve
q=public key
d=private key
At Encryption
Transmitting the message M, we have to represent the message using curve
Consider 'm' has the point 'M' on the curve 'E', randomly select 'k' ,represented as [1-(n-1)]
c1 and c2 are two cipher texts will be generated
C1=k * p
C2=m +k*q
The cipher text C1 and C2 will be send
At Decryption
M=c2-d*c1
'M' can be denoted as c2-d*c1c2-d*c1=(m1+k*q)-d*(k*p)(c2=m+k*q and c1=k*p) =M(Original message)

As we discussed various algorithm in cryptography, the RSA does not belongs to the lightweight algorithm, because it holding a large key size. The block ciphers are presented in cryptographic algorithm, among that various is adapted for low resource device [9].In existing research various block ciphers are proposed to achieve a good performance for AES-128 [10].The key size of ECC is smaller, high processing speed and take less memory. It can be applied smaller area of hardware implementation; it leads to faster computation in real time. An IoT context we are using constrained device to collaborate with each other through network. So 6LoWPan utilize the ECC algorithm with limited power and transmit information wirelessly using IP. The advanced encryption standard(AES) block cipher algorithm that encrypt 128 bits of data block using the symmetric keys 128,192 or 256.This algorithm is introduced to succeed of DES, but the effective attack in this DES is brute force. In such brute force attack, the attacker tries with all character combination to unseal the encryption. To overcome from disadvantage of DES, triple DES has introduced and it supersede with that. It is a standard with three times to increase the encryption level. RSA brings little less performance when compared ECC algorithms because the speed of encryption and decryption is low on constrained gadgets. The author presents(i)Smaller block size,(ii)Smaller key size,(iii)Simple rounds(iv)Simple key scheduling[11]. Smaller key size: Power consumption is depends on the size of the key, for smaller key size, it takes only limited power consumption. Simpler rounds: the lightweight block ciphers target low resource constraint devices and very less computation steps when compare to conventional block cipher algorithm. For example: Instead of 8 bit or 16 bit boxes in cryptographic algorithm, a single 4 bit S-box is used as lightweight protocol [12].The lightweight cryptographic protocols need a good customized CPU with good secure and cryptographic processors. The encryption speed can be improved by equipment module called crypto co-processor.the handling of overhead information affect the normal execution of data.

3. Performance analysis

An experiment has made by using smart home scenario where could use low constrained devices that has limited resources, battery power and memory space. Above said algorithms are applied among different types of smart space for the smart home applications. In order to convert a home as smart home, diverse IoT devices with different memory space, processing power, and battery capacities are interconnected and collaborate with each other. The scenario depicts smart sensors in a smart home network communicate with each other to execute a task by passing very light messages. Such sensors have limited battery, memory, and computation power. For instance, intelligent sensor gadgets can sense the data from smart home environment. A secure and effective communication has to be made, when a smart sensor gadget wants to send another sensing gadget.

3.1. Data size

We analyze the size of the data that is being transmitted over the network. The data is transmitted in the electronic form and size is the first parameter to consider. During the transmission of data by using ECC, it is considered as a secure model in a constrained environment.

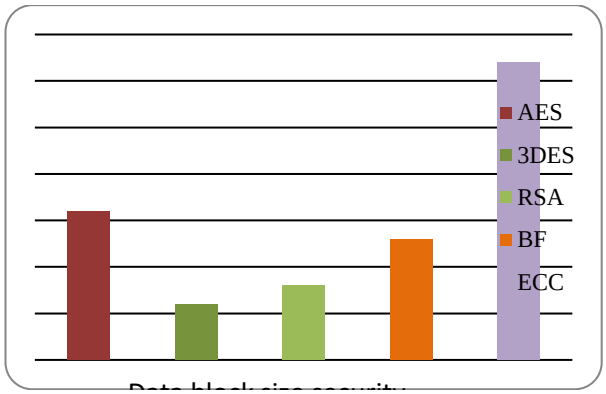
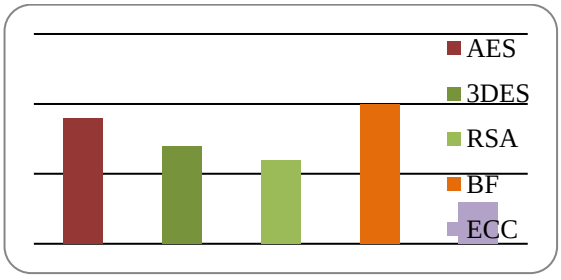


Fig. 10: Data Block Size Security.

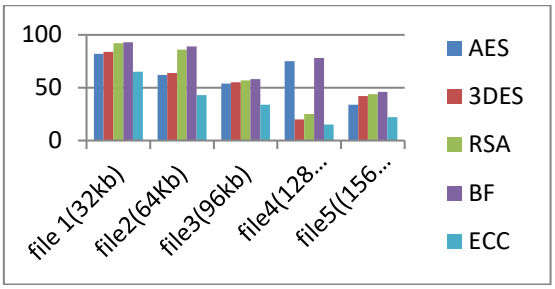
3.2. Battery power

Another important factor is battery power of smart devices; the network has been analyzed after an amount of data transmitted. The devices can be get the power by power component of source of power, diverse ways to provide the power such as main power supply, solar system, battery and many more. We may use smart battery to provide power to smart device. A device energy consumption depend on battery power.



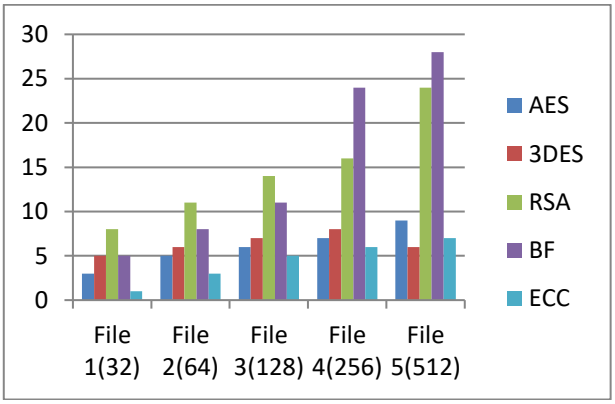
3.3. Memory space

Memory is the most vital part of IoT for the computation of data. When the complex operation is performed by a smart device, the requirement of memory is a critical factor.ECC occupies very less memory during computation.



3.4. Computation power

The adequate computation power is needed for the processing the data. As the smart device increases and it performs work intelligently. Computation power is an important metric to execute the data faster and more efficiently. More computation power require to provide solution for complex computation, altogether ECC takes less computation power to execute a task.



As mentioned in scenario the cryptographic algorithms are analyzed by using parameters such as data size, battery power, memory space and computation power, in order to find the most suitable algorithms for IoT contexts to provide security and efficient communication among the constraint smart devices. All above result shows that ECC is the most suitable cryptography algorithms in IoT Contexts.

4. Conclusion

In an IoT environment many low- resources gadgets playing significant role to perform computation. All such gadgets are limited in regards to battery life, power consumption, memory and computations. All devices which are connected in IoT contexts also face the challenges of security issue of how to maintain trust between IoT users. In order to provide best solution, we discussed different cryptography algorithms in this article and made experiment on it to evaluate the performance of algorithms in an IoT contexts. Such above said experiment shows that ECC is most effective algorithms to provide security and high performance for low resources gadgets such as constrained devices, so hardware and software implementation of such gadgets can be made by ECC algorithm may reflects good result in an IoT contexts.

References

[1] Ashton k. That 'Internet of Things' thing.RFID Journal, 2011.
[2] Saurabh Singh1 · Pradip Kumar Sharma1 · Seo Yeon Moon1 · Jong Hyuk Park1"Advanced lightweight encryption algorithms for IoT devices:survey, challenges and solution",Springer, DOI 10.1007/s12652-017-0494-4.
[3] STAMFORD (2013) Gartner says the internet of things installed basewill grow to 26 billion units by 2020. http://www.gartner.com/newsroom/id/2636073. Accessed 16 Jan 2017

[4] D. Bonino, M. T. D. Alizo, A. Alapetite, T. Gilbert, M. Axling, H. U. andJose Angel Carvajal Soto, and M. Spirito, "Almanac: Internet of things for smart cities," in *Future Internet of Things and Cloud(FiCloud), 2015 3rd International Conference on*, Aug 2015, pp. 309– 316.

[5] Mingyuan Xin,"A Mixed Encryption Algorithm Used in Internet of Things Security TransmissionSystem", Computer and Information Engineering College University of Heihe, China,IEEE 978-1-4673-9200-6/15 $31.00 © 2015 IEEE.

[6] Amare Anagaw Ayele, Dr. Vuda Sreenivasarao,June 2013"A Modified RSA Encryption Technique Based on Multiple public keys", International Journal of Innovative Research in Computer and CommunicationEngineering Vol. 1, Issue 4.

[7] Jawahar Thakur, Nagesh Kumar," DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering. Website: www.ijetae.com(ISSN 2250-2459,Volume 1, Issue 2, December 2011)

[8] Tarun Kumar Goyal,Vineet Sahula,"Lightweight Security Algorithm for Low Power IoT Devices", (ICACCI), Sept. 21-24, 2016, Jaipur, India.

[9] Fan X, Mandal K, Gong G (2013) Wg-8: "A lightweight stream cipher for resource-constrained smart devices",In: Proceeding of InternationalConference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Springer, Berlin, pp 617–632. https://doi.org/10.1007/978-3-642-37949-9_54.

[10] Iokibe K, Maeshima K, Kagotani H, Nogami Y, Toyota, Y, WatanabeT (2014) "Analysis on equivalent current source of AES-128circuit for HD power model verification", In: Proceeding of 2014 International Symposium on Electromagnetic Compatibility,Tokyo (EMC'14/Tokyo), IEEE, pp 302–305

[11] Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, Vikkelsoe C (2007),"An ultra-lightweightblock cipher. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems", Springer, Berlin, pp 450–466.

[12] Souissi R, Ben-Ammar M (2014),"An intelligent wireless sensor network temperature acquisition system with an FPGA". Wire SensNetworks.