Analysis of Cryptographic Algorithms for IoT Security

Varsha Raghav
North Cap University
Gurugram,India
Varsharaghav23@gmail.com

Supriya Raheja
North Cap University
Gurugram,India
Supriya@ncuindia.edu

***Abstract*---"Internet of Things" enables a network in which intelligent machines interact and communicate with other machines, objects and infrastructure over the internet. A vast amount of data is being generated, stored and extracted for further analysis to get valuable information. However, the base of this intelligent network is internet which leads the new challenges in terms of security and privacy. This paper discusses the detailed description of Internet of things and its security challenges. An analysis and comparison of Asymmetric cryptographic algorithms (RSA, ECC) is also presented.**

Keyword*: Internet of Things (IoT), Asymmetric algorithms, RSA, ECC, Security.*

I. INTRODUCTION

The term Internet-of-Things was first coined as an idea in 1999 by Kevin Ashton, which has now evolved into a reality that interconnects real world sensors, electronic devices and systems to the Internet [3]. This new paradigm improvise the existing Internet into a smart Internet of Things which is created around interconnections of various intelligent varied objects such as vehicle, habitats and habitat occupants into the physical world [1,5]. Presence of intelligent objects makes it a significant research topic [2].

Prevalent connectivity, computation and storage are some of the key requirements in designing of various IoT solutions. The accelerated growth of IoT shifts the paradigm towards a cyber-physical paradigm, due to the integration of the computing technology with interconnected smart objects/things which has the ability to control its key operations [4,12]. This connectivity helps us to capture more and more data but at the same time, it leads to many security and privacy concerns for the end users [11].

However, US Intelligence council stated that by 2025, Internet-of-things will connect everything to human's life [8,9,10]. Moreover, it's not a single technology; rather it is an agglomeration of several technologies that work together in tandem [6] which further raises the concern of security. With this aim, the paper has been focusing on the need of security in IoT.

The paper is organized as follows: Section 1 briefly describes the security services and security challenges of IoT. Section 2 discusses the detailed description and comparison of two important cryptographic algorithms: RSA and ECC algorithms. Section 3 depicts the comparison between RSA and ECC and Section 4,5,6 represent the issues related to IoT along with the desired solution.

II. IoT AND It's SECURITY

Most of the recent systems such as shopping system, infrastructure management system, health monitoring and transportation systems, are progressively relying on IoT based systems. Here, the major concern raises with the security of data transferred. IoT systems consist of four layers: sensing layer, networking layer, service layer and interface layers as mentioned in Table. 1. Each layer provides a security protocol that helps in achieving security services before transferring data from one layer to another [20].

Table 1. Different Layers of IoT

Layers	**Description**
Sensing Layer	This layer is integrated with existing hardware(RFID, sensors, actuators etc) to sense the physical world and acquire data
Networking layer	This layer provides the basic networking support and data transfer over wireless or wired network
Service Layer	This layer creates and manages services
Interface Layer	This layer provides interaction methods to users and other applications

ISBN: 978-1-5386-4119-4/18/$31.00 ©2018 IEEE

But, still there are chances of certain security threats on these different layers like eavesdropping, data tempering, session hijacking etc. Different possible security threats on each layer are given in figure 1 which raises the concern for further security on the layers.

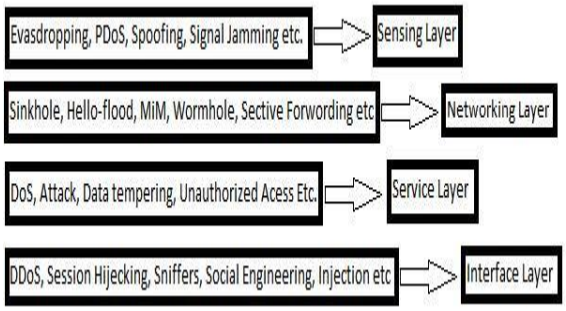

Figure 1. Various Security threats on IoT Layers

Security requirements for IOT are studied from different sources [13, 27, 28] and summarized as following:

1) *Confidentiality:* It is required to protect the data from illegitimate [37]. It deals with the protection of information from unauthorized person.
2) *Data Integrity:* It identifies alterations as data may get changed by an unauthorized party. It just provides a means for detection of manipulated data.
3) *Authentication:* It verifies that the data has been sent by an identified sender.
4) *Non-Repudiation:* The original sender of the data cannot deny the transmission of data to a recipient. A node cannot refuse sending a message which it has been previously sent [30]. It is suitable to those situations where chances of dispute can occur over exchange of data.

For achieving these security requirements, there are some security challenges which IoT based system must handle. The major security challenges in designing and building IoT devices/systems are as follows [7,29]:

IoT devices are resource constraint devices so for the efficient working of devices there should be very intricate security solutions.

Authentication to various network securities.

Management of privacy concerns.

Provide Strong integrity and confidentiality services which cannot be easily compromised.

Designed to operate autonomously with no backup facility.

Allow for evolution in case of unidentified risk.

Authentication is one of the most challenging aspect of security requirement for IoT, where key plays a very important role in it. Author[32] proposed a signature based key scheme that proves out to be the more secure scheme by providing more functionality features. The practicability of this key scheme is shown by NS2 simulator and it is also tested for security under Burrows-Abadi-Needham logic, considers informal security analysis and formal security verification. As cryptographic processing is one of the main tasks in security mechanism for data on IoT, the next section discusses the two main cryptographic schemes RSA and ECC.

III. CRYPTOGRAPHIC ALGORITMS FOR IoT

Cryptographic processing in security includes the operations generally used to provide guarantee of the privacy of data. It may include encryption, decryption, key generation, signature generation etc. It allows only the authorized people to read and process the data on IoT as data is transmitting on the untrusted medium, Internet. Cryptographic algorithms are broadly classified into two categories Symmetric and Asymmetric [35].

The basic issue involve with symmetric key cryptography is that anyone who gain access to symmetric key can read/modify/send message without knowledge of the recipient. However, Asymmetric cryptography solves this issue as it uses public keys and private keys that are mathematically connected to each other. Public keys are known by everyone whereas private keys are secret keys and known by owners only. For encryption and decryption public and private both keys are used. Public key/Private key pairs can be generated relatively easily and used for encryption and decryption. The implementation of cryptographic system possesses various requirements and challenges in resource constraint environment. Energy and power consumption are the two important aspects of public key systems [26]. In this section, authors describe the two different asymmetric algorithms used in IoT.

RSA

This algorithm was designed by Rivest, Shamir and Adleman. RSA works on the principle of generating public and private key pairs by choosing two huge prime numbers [19]. In public key encryption standard, the private key is kept secret but the public key is known to everyone [21]. This algorithm uses two large prime numbers for generating the key pair. It is estimated that the complexity of guessing the plaintext from single key and from the cipher text equals to the decomposition of product of those two prime numbers [22]. Different steps are involved to encrypt and decrypt files by RSA. These are as follows:

Key Generation

Each person who wants to be the part of communication needs to generate a key pair. The procedure for generating the key is given:

1. Generate the n (RSA modulus)
2. Select p and q (two prime numbers)
3. Calculate n = p * q
4. Find e

Here, e is the derived number which is greater than 1 and less than (p-1)(q-1). Finally, (n,e) pair forms the public-key. Private key d is generated from calculating p, q and e as in equation (1). d is the inverse of e mod (p-1) (q-1).

$$de = 1 \bmod (p-1)(q-1) \quad (1)$$

Encryption

Let us assume that a sender would like to send a message to receiver whose public key is (n,e).The Plaintext P is a series of number less than n. Then the text can be encrypted using equation (2).

$$C=P^e \bmod n \quad (2)$$

Decryption

Now, suppose the receiver of public key pair (n,e) has received a Ciphertext C. The plaintext (P) can be generated further using equation (3).

$$P=C^d \bmod n \quad (3)$$

Security of this algorithm mainly depends upon the difficulty in factorization of large numbers.

Elliptic curve cryptography (ECC)

Victor miller and Neal Koblitz proposed this cryptography scheme. It is a method of encoding data so that only specific individuals can decode them. It primarily focusses on mathematics of elliptic curves & uses the location of points on an elliptic curve to encrypt and decrypt information [31]. It is a public key cryptography in which one encryption key known as private key is kept secret, while another known as public key is freely distributed. Public key cryptography is computationally more expensive and also shortens the lifetime of batteries or devices. It has been observed that ECC used for area efficient high throughput design. However, the use of ECC is emerging in low area as well as in low power applications [29]. ECC is preferable for the resources constraint devices because of the following features:

Security: Some cryptographic experts recommend that our communication system require a minimum of 128 bits of keys. This phenomenon believes that if we increase the key length, it helps to curb the attacks.

Performance: ECC exhibit a much improved as well as better operation. Features like key generation and certification are up to 10 times faster and require less server processing cycles.

Bandwidth requirements: The size of security key also related with the memory. The ECC keys size are 12 times smaller as compared to any other key.

Power consumption: CPU consumption from the server and client is very less in ECC which is beneficial for low power (small) devices that have limited CPU consumption capabilities.

Just like any other cryptographic algorithms, ECC also involves key generation, encryption and decryption.

As discussed, it uses the elliptic curve as shown in fig 2.

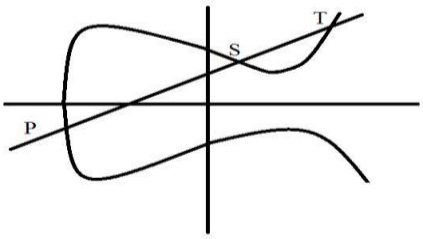

Figure 2. Diagrammatic representation of elliptic curve

This section describes the ECC algorithm in detail. Different variables used by ECC are given in Table 2. The steps followed are as follows:

Table 2. List of variables used in ECC

E	Elliptic Curve
P	Point on the elliptic curve
S	Public-key
D	Private-key (1 to n-1)
N	Maximum limit(prime number)
K	Random variable (1-(n-1))
C1, C2	CipherText
M	Message
M	Point on the curve for message m.

Key Generation Process

In ECC, there is a need to generate both the keys (public key as well as private key). The sender uses the receiver's public key to encrypt the message and receiver uses private key in order to decrypt the message.

Public key for the same can be generated using equation (4).

$$S=d*P \quad (4)$$

Encryption Process

Suppose a message m is sent which has a point M on the elliptic curve. Then the two cipher texts are generated as given in equation (5) and equation (6).

$$C1 = k * P \quad (5)$$
$$C2 = M + k * S \quad (6)$$

Decryption Process

Further decryption can be applied using equation (7). Moreover, the explanation of how it produces the original message is also given.

$$M=C2–d*C1 \quad (7)$$

Proof:

M = C2 – d * C1
M can be written as C2 –d * C1
(M + k * S) – d * (k * P)
M + k * d * P – d * k * P
M.

IV. Analysis of RSA and ECC Cryptographic Algorithms

This section presents the comparison between both algorithms RSA and ECC. Using elliptic curves for more than 25 years, the practical benefit of using these curves are well understood, they offer smaller key size[23] and more efficient implementations [24] at the same security level as RSA [25]. The security of the RSA Cryptosystem is based on the Integer Factorization Problem and the security of ECC is based on elliptic curve discrete logarithm problem [14]. The basic operation is point addition which is very expensive. That makes it very unlikely to discover a sub-exponential attack on ECC though we have few curve which are prone to this but we can easily by pass them. RSA already has a known sub-exponential attack [18]. Table 3 illustrates the cryptographic key length for both RSA and ECC. The key size of ECC is much smaller as compared to RSA [15].

Table 3. RSA and ECC key lengths

	Minimum size (bits of public keys)	
Security bits	***RSA***	***ECC***
80	1024	160
112	2048	224
128	3072	256
192	7630	384
256	15360	512

Security mechanism of both the algorithms is summarized in Table 4 [16,17]. From the Table 4, it can be analyzed that both algorithms have its own pro's and con's. It is very difficult to say which one is more better as compare to other for IoT security.

Table 4. ECC vs. RSA

Parameter	**ECC**	**RSA**
Computational Overhead	10 times lesser than RSA	More than ECC
Key Sizes	Shorter	Larger
Bandwidth Saving	More bandwidth saving than RSA	Less bandwidth saving
Key Generation	Faster	Slower
Encryption	Faster	Slower than ECC
Decryption	Slower	Faster
Small devices efficiency	More efficient	Less efficient

It can be concluded that none of the current cryptography schemes proved to be secure algorithm for IoT. They do not guarantee to maintain the level of security within the resource constraints of IoT. The strength of RSA goes down if the public key (e) is small and the two numbers (p,q) are not large prime numbers.In ECC the size of encrypted message significantly increases. So, it becomes more difficult to implement resulting implementation error which reduces the security of the algorithm. The further work is required as the present algorithms are somewhere not satisfying the requirements of IoT as they are taking more execution time, less speed and complex implementation.

V. CONCLUSION

The major challenge with the low power embedded devices with respect to security is resource consumption. The computational power available in Internet-of-Things is limited as well as insufficient for processing of any security algorithm. The battery capacity is strongly connected to quantity of computation executed which is also limited. Storage limitation is also a hurdle. Research is still going on ECC and there is vast area remain uninvestigated whereas RSA is well researched and trusted algorithm. Inspite of this each algorithm has its own advantages and shortcomings. Neither of them is fully suited to IoT environment. Thus, an alternative cryptographic algorithm can be the solution.

REFERENCES

[1] JunZheng, David Simplot-yl, Chatschik Bisdikian, Hussein Mouftah.(2011)"The internet of things [Guest Editorial]",IEEE Communications Magazine, Volume:49, Issue: 11.

[2] Ina Kim, Moon-Ki Back, Hyung-Jun Yim and Kyu-Chul Lee*.(2015)" RFID Adaptor for Detecting and Handling Data Events in Internet of Things", Indian Journal of Science and Technology, Vol 8(S5), 140–148.

[3] IoannisAndrea,ChrysostomosChrysostomou,George Hadjichristofi.(2015) "Internet of Things: Security Vulnerabilities and Challenges", IEEE Symposium on Computers and Communication (ISCC).

[4] Gourav Misra1, Vivek Kumar1, Arun Agarwal1, Kabita Agarwal2.(2016)"Internet of Things (IoT) – A Technological Analysis and Survey on Vision, Concepts, Challenges, Innovation Directions, Technologies, and Applications (An Upcoming or Future Generation Computer Communication System Technology)", American Journal of Electrical and Electronic Engineering, Vol. 4, No. 1, 23-32.

[5] Luigi Atzori a, Antonio Iera b, Giacomo Morabito c.(2016) "The Internet of Things: A survey", ELSEVIER.

[6] Pallavi Sethi, Smruti R. Sarangi.(2017)"Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering.

[7] Jun-Ya Lee,Wei-Cheng Lin, Kaohsiung, Taiwan, Yu-Hung Huang. (2014) "A Lightweight Authentication Protocol for Internet of Things", IEEE.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8] Omar Said, Mehedi Masud.(2013)" Towards Internet of Things: Survey and Future Vision", International Journal of Computer Networks (IJCN), Volume (5) : Issue (1).

[9] Luigi A., Antonio I,Giacomo M.(2010) "The Internet of Things: A survey", Science Direct journal of Computer Networks, Volume 54, Pages: 2787–2805.

[10] JayavardhanaGubbi,aRajkumarBuyya,b*Slaven Marusic,aMarimuthu Palaniswamia.(2013)" Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", ELSEVIER Future Generation Computer Systems 29,1645 – 1660.

[11] Borgohain, Tuhin, Kumar, Uday, Sanyal, Sugata.(2015)" Survey of Security and Privacy Issues of Internet of Things", International Journal of Advanced Networking Applications. 6. 2372-2378.

[12] Andrew Whitmore, Anurag Agarwal,Li Da Xu.(2014) "The Internet of Things—A survey of topics and trends", Springer.

[13] T.Kavitha1, D.Sridharan2.(2010)"Security Vulnerabilities In Wireless Sensor Networks: A Survey", Journal of Information Assurance and Security 5, 031-044.

[14] Dindayal Mahto, Member, IAENG, Danish Ali Khan, Member, IAENG and Dilip Kumar Yadav.(2016)"Security Analysis of Elliptic Curve Cryptography and RSA", Proceedings of the World Congress on Engineering 2016 Vol I WCE 2016.

[15] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid.(2012) "Recommendation for key management part 1: General (revision 3)," NIST Special Publication 800-57, pp. 1–147.

[16] The Study Material.http://www.the studymaterial. com / presentation seminar/ electronics-presentation /248-ellip.html?start=3.

[17] V.B. Kute et al,"A software comparison of RSA & ECC", IJCSA Vol 2, No.1, April/May 2009.

[18] Rounak Sinha, Hemant Kumar Srivastava, Sumita Gupta,(2013)" Performance Based Comparison Study of RSA and Elliptic Curve Cryptography", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, ISSN 2229-5518.

[19] Rivest RL, Shamir A, Adleman L.," A method for obtaining digital signatures and public-key cryptosystems", Commun ACM. 1978; 21(2):120–6.

[20] Isha and Ashish Kr. Luhach*.(2016)"Analysis of Lightweight Cryptographic Solutions for Internet of Things", Indian Journal of Science and Technology, Vol 9(28),DOI: 10.17485/ijst/2016/v9i28/98382.

[21] Abdullah Al Hasib ,Abul Ahsan ,Md. Mahmudul Haque.(2008)" A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography" Third International Conference on Convergence and Hybrid Information Technology.

[22] Xiaofei Tang Xin Zhou.(2011)" Research and Implementation of RSA Algorithm for Encryption and Decryption", The 6th International Forum on Strategic Technology.

[23] A. K. Lenstra, E. R. Verheul.(2001)" Selecting cryptographic key sizes", Journal of Cryptology, 14(4):255.

[24] D. J. Bernstein ,T. Lange.(2013)" eBACS: ECRYPT Benchmarking of Cryptographic Systems" http://bench.cr.yp.to.

[25] R. L. Rivest, A. Shamir, and L. Adleman," A method for obtaining digital signatures and public-key cryptosystems".

[26] Vivek Katiyar, Kamlesh Dutta, Syona Gupta.(2010)" A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment ",International Journal of Computer Applications (0975 – 8887) Volume 11– No.10.

[27] Erdal Çayırcı, Chunming Rong.(2009)"Security in Wireless Ad Hoc and Sensor Networks", A John Wiley and Sons, Ltd, Publication.

[28] Yi Qian and Kejie Lu and David Tipper.(2007) "A Design For Secure And Survivable Wireless Sensor Networks", IEEE Wireless Communications, Pp. 30 – 37.

[29] Sabrina Sicari, Cinzia Cappiello, Francesco De Pellegrini, Daniele Miorandi, Alberto Coen-Porisini.(2014)" A security-and quality-aware system architecture for Internet of Things", Springer.

[30] Ayuso, Jesús & Marin, Leandro & Jara, Antonio J. & Skarmeta, Antonio.(2010)" Optimization of Public Key Cryptography (RSA and ECC) for 16-bits Devices based on 6LoWPAN", 1st International Workshop on the Security of the Internet of Things, Tokyo, Japan.

[31] Younsung Choi 1, Donghoon Lee 1, Jiye Kim 1, Jaewook Jung 1, Junghyun Nam 2, Dongho Won 1.(2014)" Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography ",Sensors 2014.

[32] Sravani Challa,Mohammad Wazid,Ashok Kumar Das,Neeraj Kumar,Alavalapati Goutham Reddy, Eun-Jun Yoon,Kee-Young Yoo,"Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications", IEEE Access,Volume:5,Page No. 3028-3043,DOI: 10.1109/ ACCESS. 2017.2676119.

[33] Sourabh Chandra, Smita Paira.(2014)"A comparative survey of symmetric and asymmetric key cryptography", International Conference on Electronics, Communication and Computational Engineering (ICECCE).

[34] Khan, R., Khan, S. U., Zaheer, R., & Khan, S.(2012)" Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges", 10th International Conference on Frontiers of Information Technology (FIT): Proceedings.

[35] Sourabh Chandra, Smita Pair.(2014)"A comparative survey of symmetric and asymmetric key cryptography", International Conference on Electronics, Communication and Computational Engineering (ICECCE).

.