International Journal of Control and Automation
Vol. 13, No. 4, (2020), pp. 1010 – 1018

Cryptographic Algorithms for Secure Internet of Things

Kapil Mehta[1], Yogesh Kumar[2], Harjeet Singh Sidhu[3]
Department of Computer Science and Engineering
Chandigarh Group of Colleges, Landran, Mohali
CT University, Ludhiana, Punjab, India
BHSBIET, Lehragaga, Punjab

Abstract

As billions of devices are connected with one another, IoT (Internet of Things) that promises technology solutions for solving daily lives of people. The increasing demand of Internet computing through physical devices transforms the living style of people in every manner. This is only possible with the computing intelligence of physical devices or objects connected with each other irrespective of their nature of homogeneity or heterogeneity connected through the Internet called IoT (Internet of Things). The connectivity of such intelligent devices leads to various security challenges that may lead to various security problems in the network. Security in the widespread manner revolves around privacy, trust, identification and access control during communication between various devices. So, according to the taxonomy of IoT framework, various Security Algorithms are available to deal with the security concerns of users using IoT enabled devices. In this paper, different research challenges and important security solution algorithms are discussed and analyzed to prevent attacks or cover various security measures. The most likely measures are well approved by various research scholars working in this area. This paper is a holistic overview of the available solutions or the research status of different key technology algorithms for IoT Security. This paper also surveys the Light Weight Cryptography solutions for IoT.

Keywords: *Internet of Things; Computing Intelligence; Security; Privacy.*

1. Introduction

People can connect with one another to access everything with the Internet through IoT. The term IoT refers to uniquely identified objects and their abstract virtual representation in Internet-like structure. It is the technology that allows human to machine connectivity or machine to machine connectivity both. More devices connect with each other; more data will be generated by such devices. The large sets of data generated by such devices have high volume, high velocity and different variety. Such a large set of data called Big Data; due to which Security is at high risk. Security is the tremendous issue during any communication or interaction between people or devices over the network. Applications of IoT extend in various areas like Health Care, Smart Homes, Smart Cities, Agriculture, Banking and Lifestyle. While doing online payments for booking a Hotel, transferring amount to other person's account etc all situations demand security. Currently, IoT is the most popular term, as various industrial applications related to IoT will arise. Examples include Cyber Systems-Transportation and Physical, Mobile-to-Mobile communication. Due to the Security perspective, there are few challenges: 1) IoT works through Internet whether it is traditional, mobile or sensor network. 2) Issues due to communication perspective between the nodes over a network. So, it is the

ISSN: 2005-4297 IJCA

prime concern of taking care of authentication and access mechanisms. Failing so, chances of hacking or attacking the information increases.
The main issues in IoT Security are as below:

1.1 Confidentiality: - It assures to protect information to be accessed by unauthorized parties. It depends upon administrator to whom to give access to sensitive data. For Example, if someone's bank account number is displayed on public portal then that information can be accessed by third parties or may be misused by hackers. To avoid such issues, confidentiality of data should be reached.

1.2 Integrity: - It relates to the validity or fidelity of data. While transmitting data from sender to receiver, data can be changed through the network. Integrity assures that data sent should be exactly inputted to the destination. Data should be free from any corruption, maliciousness or unauthorized access.

1.3 Availability: - It ensures that data is available at the instant when users need it. It involves where the data is stored and how it can be reached. Availability allows reliable access to the data to be avoided by unauthorized users.

So, there is a need of latest emerging technologies that meet the requirements of Security.

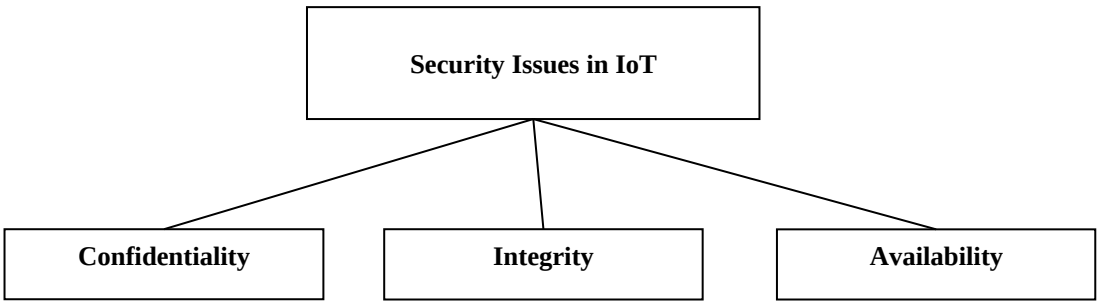

Fig.1- Issues in IoT Security

The trio of Confidentiality, Integrity and availability is shown above. The main objective of this trio is to avoid Security related issues in the IoT. During communication between human-human and machine- machine, these three objectives should be achieved. Due to the increased complexity of IoT networks, various security concerns or challenges are faced by such networks. Attackers can attack any communication device in the network and can gain access to the private data that will affect sensitivity and confidentiality. This is the lack of Confidentiality, Integrity and availability that leads to security challenges that disrupt the widespread adoption of this technology [1].

1.4 SECURITY CHALLENGES IN IoT

1.4.1 **Processing Power: -** As humans are getting more dependent on IoT Devices, many of them have limited low power, memory or other storage issues. Such low power devices always face various attacks like power analysis attacks etc. It is very difficult for low power devices to use complex encryption algorithms in which High-End Security is a

ISSN: 2005-4297 IJCA

major concern. So, it is a huge demand to reduce the battery limitations or to use the efficient encryption algorithms so that there will be no compromise in processing the applications.

1.4.2 **Authorization & Authentication: -** To access the services offered by IoT Devices, Identity of the users should be registered with the help of Authorization and Authentication mechanisms. Authentication can be achieved by setting strong passwords and certificates so that security can never be compromised.

1.4.3 **Secure and Efficient Communication: -** During communication between devices, the main aspect is Security. Before sending a message from source to destination, encryption is necessary. The best practice is to adopt Security standards like TLS so that efficient communication can be made.

1.4.4 **Ensuring Data Privacy & Integrity: -** Once the data has been transmitted over the network, it will be processed and stored at some place. Maintenance of privacy of that data is a challenging task so that no third party can hack or theft that data so it should be stored in compliance with regulatory frameworks. Data that will be no longer required should be disposed off from storage. There should also be scalable approach mechanisms to ensure that the integrity of data should be maintained, no other person can modify the data easily.

1.4.5 **High Availability: -** As Humans completely rely on IoT devices, then there is a high need of availability of data so that physical things can be managed by IoT devices. IoT devices should get full protection against various cyber or malicious attacks so that no information can be lost or it can recover quickly whenever problems arise.

1.4.6 **Detect Vulnerabilities and Incidents: -** A System is said to be complex that truly depends on the connectivity figure of devices as every device is of different nature having different configurations and protocols. In this case, it is very difficult to detect any vulnerability or attack in the System. There should be any Security Intelligence approach to detect when an incident occurs.

This paper is organized Section-wise as mentioned here: Section 1 is the Introduction section. Section 2 provides the brief of literature or related work. Section 3 introduces the Cryptographic algorithms for IoT. Section 4 presents the Conclusion and Future Scope.

2. Related Work

Security is being a most talkative issue for researchers today, as plenty of publications highlighting various issues related to the security and privacy of users in IoT. Only authentication and authorization techniques do not work for security, there is a need of device authentication too which is a biggest challenge.

Chen et al. [4] implemented a model which is based on access control of capability for distributed IoT environment. This model guarantees end-to-end security by using

ISSN: 2005-4297 IJCA

token passing mechanisms and IPSec. Users can request a single token for group access for the efficient communication between devices.

User-controlled access model was proposed by Rivera et al. [5] which is useful for providing different types of levels of access to agents.

Gaikwad et al. [6] proposed secure authentication system for smart homes with the use of IoT. It uses hash algorithms and advanced encryption standard for security.

Mahalle et al. [7] proposed a lightweight and secure authentication scheme for the verification of the nodes of the network. It minimizes the handshaking pressure that will ensure the usage of less resources and helps in power saving. This scheme is more robust and secure over any threats or attacks.

Panwar et al. [8] proposed mechanism of security for IoT that will use datagrams and digital certificate that will make more robust authentication and replaces the preshared process.

Park et al. [9] simplify the certificate structure and created the authentication of common devices that will be applied on resource constrained IoT environment.

Siddiqui presented a data transfer protocol that connects IoT devices called Constrained Application Protocol (CoAP). This Protocol uses an open-source implementation of CoAP along with Datagram Transport Layer Security (DTLS) for the data transfer between IoT Devices in a more secure form.

3. Cryptographic Algorithms for IoT

Security is the major measure during communication between two parties over a public or private channel. This can be achieved by enabling secure features either from sender or receiver side. For the efficient or secure communication, the following techniques can be considered:

3.1 Cryptography

Cryptography refers to the protection of information while sending through a network. Cryptography is the combination of ‘Crypto’ means ‘hidden’ and ‘graphy’ means 'writing’. It is the hidden writing technique so that no other third party instead of receiver can read the sent information. When a user sends an email, then it is secured by Secure Socket Layer technique of Cryptography. Cryptography is related to with confidentiality, integrity and authentication. Confidentiality ensures that no third person can access the data except the permission of owner. Integrity ensures that no third person can edit the data as no modification is allowed; Authentication is used for the confirmation of the identity of sender and receiver [2]. Cryptography works on the basis of key and algorithm. Encrypting and Decrypting are the processes of cryptography. Encrypting and Decrypting are used for converting plain text into cipher text and vice-versa [3]. Cryptography Algorithms can be classified into two categories:

ISSN: 2005-4297 IJCA

3.2 Symmetric Cryptography

Symmetric Cryptography works by using the same Secret key by the Source and the Destination. The same Secret Key is to be used for Encrypting and Decrypting both. Key is selected by the mutual agreement of both parties to start the conversation.

3.3 Asymmetric Cryptography

Asymmetric Cryptography works by using two different keys for encrypting and decrypting called Public key and Private Key. Public key is known to everyone and Private Key is never exposed. While sending a message, the source encrypts a message by the Public key and destination will decrypt a message by using Private Key. There are following algorithms to be discussed which deals with Symmetric and Asymmetric Cryptography both. An available suite of Cryptographic algorithms is shown below in Table 1.

Algorithm	Goal
Advanced Encryption Standard Algorithm	Confidentiality
Rivest Shamir Adelman	Digital Signature Key
Diffie-Hellman	Key Agreement

Table 1-Security Algorithm suite

It is important to understand the difference between Symmetric and Asymmetric Key Cryptography before securing the IoT. Table 2 shows the basic differences:

Cryptography Methods		
Type	**Asymmetric Key Cryptography**	**Symmetric Key Cryptography**
Keys	Uses Public Key for Encrypting and Private Key for Decrypting	Permits Encrypting and Decrypting of the message with same key.
Speed	Slow in Execution	Fast in Execution
Use	Used for securely exchanging security key	Used for Bulk Data Transmission
Number of Keys	Depends on the number of users connected (Linear Proportion)	Depends on the number of users connected (Exponential Proportion)
Implementation	Complex Hardware Implementation	Simple in Comparison
Examples	RSA,DSA,ECC	AES, DES, Blowfish, Twofish

Table 2-Comparison of Cryptographic Methods

3.4 DES (Data Encryption Standard)

DES is a block cipher that takes input as 64-bit in plain text; converts it into 64-bit cipher text after performing certain operations on it. DES uses a deterministic algorithm that can be operated on fixed length group of bits called a block. DES is

ISSN: 2005-4297 IJCA

a Symmetric Key algorithm in which two or more parties have identical key of 64 bits. Out of the available length, 56 bits are used for encrypting or decrypting a message and the left over 8 bits helps to check parity [10]. A Symmetric structure used in the construction of block ciphers is called as Feistel Network.

3.5 Triple-DES (3-DES-Data Encryption Standard)

The name 3-DES indicates that block cipher encryption algorithms are applied three times (thrice) to each block. 3-DES is proven more secure and powerful as compared to DES. This algorithm has high capability due to increase in key size that helps to ensure the security of additional encryption features.

3.6. Shortfalls

Triple DES Algorithms have more security features than single DES, but bitter slower than encryption using single DES. Due to the computational complexity, 3-DES is found as the lowest block cipher [11]. Another issue with DES is that while securely delivering a key from one party to another can introduce a security risk of modifying the message.

3.7 AES (Advanced Encryption Standard)

On the basis of the principle of substitution-permutation network, AES supersedes DES that does not use a Feistel Network. It consists of 3 block ciphers-128,192 and 256 bits and each block of cipher can encrypt and decrypt data in 128-bit blocks using 128, 192 and 256 bit keys respectively. Encryption will be stronger as the key size is higher. For the conversion of plain text into cipher text, there are four possible transformations. AES will work as per the following steps:

a. Arrange data into an array or matrix.
b. Shift data rows.
c. Mix columns.
d. Performs simple XOR operation.

3.8 RSA (Rivest, Shamir, Adleman) Algorithm

In 1978, RSA was developed by Ron Rivest, Adi Shamir, and Leonard Adleman. For the exchange of keys or digital signatures or encryption of blocks of data, RSA is the best known the best known public key cryptosystems. The working principle of RSA is the use of a variable size encryption block and a key. The concept of prime numbers is used for public and private key generation. For the purposes of encryption and decryption, different keys will be used. By using the public key, Source encrypts the message whereas by the use of private key destination decrypts the message [11, 12]. In RSA, asymmetry is based, due to the factorization of the product of two large prime numbers, more difficult. Factorization is the breakdown or decomposition of prime numbers. Factorization is also called the "factoring problem" that decompose an integer into a product of smaller integers.

3.9 Diffie-Hellman Key Exchange Algorithm

Diffie-Hellman key exchange is a method of digital encryption for exchange of cryptographic keys over a public channel in a secure manner. This method avoids the direct transmission of cryptographic keys. It is also called exponential key

ISSN: 2005-4297 IJCA

exchange. Key Exchange is an approach in which cryptographic keys are exchanged between the two parties. The prime purpose of Diffie-Hellman key exchange is to build up a secure and secret key connection to establish a channel [13]. Building of a mutual secret between two devices can be utilized for the secure communication through a common public channel. This protocol is effectively assaulted by the man-in-the- middle and impersonation attack. This method is perfect for utilization in communication and is less utilized for the storage of information over a long time.

3.10 Light Weight Key Cryptography

Muhammad Tausif et al. [14] proposed Cryptographic algorithm based on Light Weight Key, for designing the best light weight cipher for Internet of things that will use sensors on the basis of physical objects for data collection and actuators for data sharing with the objects. Smart devices are having controlled and limited resources like energy or power of the battery, limited size of RAM etc [15]. So, it is advantageous to use cipher of lightweight that helps in secure communication in IoT. For the constrained environments, Light Weight cryptography is also helpful. Examples include digital cards, medical equipment and radio frequency ID tags, sensors, actuators etc [16]. During the implementation in hardware, Size of RAM, consumption of battery etc are the deciding factors for the evaluation of lightweight properties. Security and privacy are the main concerns in the IoT, without such factors, cryptography is insufficient [17].

During the implementation on hardware and software both, Lightweight cryptography affects the huge collection of resource-constrained devices. Due to the constraints of size, consumption of energy and speed, it is impossible or difficult to work for the environment where resources are limited that also affects the implementations of cryptographic algorithms [18]. Light Weight Cryptographic solutions are needed; the shortfalls are discussed in [19] [20] [21]. In case of light weight cryptography, block ciphers shown better performance in comparison to stream cipher and hash functions. mCrypton is proposed as a new block cipher [22] which has the key options of bits of size 64, 96 and 128.

4. Conclusion and Future Scope

This paper presents the important aspects of popular Secure Encryption Algorithms that works on Key Exchange. Light weight cryptographic algorithms are also discussed in this paper that moves IoT towards more security. The basics of Symmetric and Asymmetric Cryptographic Techniques have also been discussed. The trending concept of Light Weight Cryptography has also been discussed. To secure the data transmission over different networks by using different types of Services is the Conclusion. The conclusion is that there are more requirements to secure the data transmitted over different networks using different services. In this paper, various encryption techniques or algorithms have been discussed. It is here by concluded that, all the available techniques are useful for real-time Encryption. Every technique has an individual methodology to work and every technique has their own pros and cons which have been discussed above. According to consideration of all the algorithms, it can be found that RSA algorithm is most efficient in terms of throughput, speed and time. As, these algorithms work sincerely on security, and this feature can be increased further if algorithm applied to data is more than one. The Future work will be focused on exploring the algorithms for creating a more secure environment. The Future work will also focus

ISSN: 2005-4297 IJCA

on the effect of such cryptographic and time synchronization algorithms on Delay, Throughput, Control Packet overhead and many more.

Acknowledgement

We are thankful to the Reviewers and Editors for their careful reading of the published manuscript and sparing time to provide many insightful comments and suggestions.

5. References

[1] Kanuparthi, Arun, et al. "Hardware and embedded security in the context of internet of things." Proceedings of the ACM workshop on Security, privacy & dependability for cyber vehicles - CyCAR '13, **2013**.
[2] Almuhammadi, Sultan, and Ahmed Al-Shaaby. "A Survey on Recent Approaches Combining Cryptography and Steganography." Computer Science & Information Technology (CS & IT), **2017**.
[3] Mustafa, Ghulam, et al. "A review of data security and cryptographic techniques in IoT based devices." Proceedings of the 2nd International Conference on Future Networks and Distributed Systems - ICFNDS '18, **2018**.
[4] Chen, Borting, et al. "S-CBAC: A secure access control model supporting group access for Internet of Things." 2015 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), **2015**.
[5] Rivera, Diego, et al. "Applying a Unified Access Control for IoT-based Intelligent Agent Systems." 2015 IEEE 8th International Conference on Service-Oriented Computing and Applications (SOCA), **2015**.
[6] Gaikwad, Pranay P., et al. "3-level secure Kerberos authentication for Smart Home Systems using IoT." 2015 1st International Conference on Next Generation Computing Technologies (NGCT), **2015.**
[7] Mahalle, Parikshit N., et al. "Threshold Cryptography-based Group Authentication (TCGA) scheme for the Internet of Things (IoT)." 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), **2014**.
[8] Panwar, Mukul, and Ajay Kumar. "Security for IoT: An effective DTLS with public certificates." International Conference on Advances in Computer Engineering and Applications, **2015**.
[9] Park, AHyeon-Ju, et al. "A Framework of Device Authentication Management in IoT Environments." 5th International Conference on IT Convergence and Security (ICITCS), **2015**.
[10] Singh, Gurpreet, and Supriya Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security." International Journal of Computer Applications, vol. 67, no. 19, **2013**, pp. 33-38.
[11] "Encryption and Decryption of data using Elliptical Curve Cryptography." International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9, **2019**, pp. 1141-1144.
[12] Al Najjar, Ali S. "Implementation Color-Images Cryptography Using RSA Algorithm." International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 11, **2017**, p. 181.
[13] Borodzhieva, Adriana N. "Software implementation of a module for encryption and decryption using the RSA algorithm." **2016** XXV International Scientific Conference Electronics (ET), 2016.
[14] "Structurally Enhanced Correlation Tracking." KSII Transactions on Internet and Information Systems, vol. 11, no. 10, **2017**.
[15] Li, Shancang, et al. "5G Internet of Things: A survey." Journal of Industrial Information Integration, vol. 10, 2018, pp. **1-9.**
[16] Gupta, Kishan C., and Indranil G. Ray. "Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications." Cryptography and Communications, vol. 7, no. 2, 2014, pp. **257-287**.
[17] Siddiqui, Farhan, et al. "Secure and lightweight communication in heterogeneous IoT environments." Internet of Things, **2019**, p. 100093.
[18] M., Ms. S. "Multi Cloud Secure Data Sharing Using Encryption and Decryption Algorithms." International Conference On Contemporary Researches in Engineering, Science, Management & Arts, **2020**.
[19] Mala, Hamid, et al. "Cryptanalysis of mCrypton-A lightweight block cipher for security of RFID tags and sensors." International Journal of Communication Systems, vol. 25, no. 4**, 2011**, pp. 415-426.
[20] Bannier, Arnaud, and Eric Filiol. "Mathematical Backdoors in Symmetric Encryption Systems - Proposal for a Backdoored AES-like Block Cipher." Proceedings of the 3rd International Conference on Information Systems Security and Privacy, **2017**.

ISSN: 2005-4297 IJCA

[21] Mohindru, Vandana, Yashwant Singh, and Ravindara Bhatt. "Securing wireless sensor networks from node clone attack: a lightweight message authentication algorithm." International Journal of Information and Computer Security 12, no. 2-3 **(2020)**: 217-233.

[22] S Vashisht, S Jain, "An energy-efficient and location-aware Medium Access Control for quality of service enhancement in unmanned aerial vehicular networks", Computers & Electrical Engineering, 4(75), 202-217, **2019**. I.F 2.18.

ISSN: 2005-4297 IJCA