2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. Sep 3-4, 2021

2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) | 978-1-6654-1703-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICRITO51393.2021.9596234

Comparative Analysis of Various Encryption Algorithms Used In IoT Security

Latika Kakkar
CSE
Chitkara University
Rajpura, India
latika.kakkar@chitkarauniversity.edu.in

Deepali Gupta
CSE
Chitkara University
Rajpura, India
deepali.gupta@chitkara.edu.in

Sarvesh Tanwar
CSE
AIIT Amity University
Noida, India
stanwar1521@gmail.com

Abstract—**Data security is the major concern and the encryption algorithms plays a vital role for providing security in the wireless network. Data encryption and decryption is the important technique used to provide confidentiality of data. Also security of the data transferring via network becomes extra critical when the data is large and heterogeneous in nature. Data from IoT devices exhibit various security flaws that are prone to various attacks which can affect the confidentiality, integrity, authentication of data. Thus an efficient security algorithm is required for the security of IoT devices to maintain the data confidentiality and withstand security attacks. This paper focuses on analysis of various encryption algorithms used in IoT on the basis of various parameters and to compare them so as to define the best encryption algorithm that can be used in future work.**

Keywords— ECC, RSA, Security, Signcryption, Digital Signature, IoT.

I. Introduction

IoT is a paradigm in which all the things, objects and sensors are connected to internet and thus interact among each other through heterogeneous network [1, 2]. IoT is also capable of taking decisions based on estimation, calculations and computations. IoT has made the world smart by making the ordinary devices as smart devices [3, 4]. A large number of smart applications have been built using these smart devices [5]. Radio frequency identification, Cloud Computing, wireless sensor networks (WSNs) are the basis and aspects of IoT [6]. IoT consists of scenarios where the smart things are designed and composed of unique identifiers where the data is sent through insecure network to the destination host. These smarts devices can be smart sensors, appliances, people, wearable devices etc. IoT not only senses the environment but it also has the capability of making decisions, calculations and computations. In healthcare domain the patients heartbeat, BP and other minute details can be analyzed by doctor if the patient is wearing smart healthcare device [7]. Thus if the doctors cannot reach the patient immediately then they can analyze the condition of the patient through this device and can give necessary instructions for the patient. The security of IoT devices and their data is at utmost priority and is also the main challenge because of scalability and heterogeneity of this wireless interaction [8, 9, 10]. Various researchers have worked on the security of IoT data by implying various encryption algorithms. This paper will focus on the various encryption algorithms used by various researchers in the IoT data security and will define the comparison between these algorithms.

A. Signcryption

Signcryption is an encryption technique which has the capability and functionality of performing mutually digital signature as well encryption in single consistent step [11]. As a result of this combined step, Signcryption technique works at a tremendously low cost than the traditional method in which the procedure is executed in two sequential steps. In first step digital signature of the data is created and in second step the data along with the digital signature is encrypted by utilizing some encryption technique [12, 13, 14]. Both digital signature and encryption achieves legitimacy, privacy and reliability and confidentiality [15]. This scheme is a resource-efficient scheme that accomplish lesser computational and communication cost then the existing conventional schemes. It also achieves non-repudiation, reliability, validation and confidentiality at a minimal cost [16, 17]. In public key encryption scheme, the authenticity of the public key can be validated by existing techniques: identity-based cryptosystem (IBC), public key infrastructure (PKI) and certificateless cryptosystem (CLC) [18,19]. Based on these authentication schemes signcryption has three further classifications which are described as follows:

- Public Key Infrastructure (PKI): In this technique, a certificate authority (CA) provides a certificate that holds a public key and the customer individuality which is analyzed by the CA's signature. The PKI has its high demand in the field of security in internet. Due to heavy load of certificates that are generated and stored, PKI is not recommended.
- Identity based signcryption (IBSC): In this there is no requirement of generating certificates. The identity of the user (Like email, IP address) is utilized for generating the Public key. A public key generator (PKG) is utilized as trusted third party to engender public key. The PKG is responsible for generating all the secret keys to be utilized by users [20, 21]. IBC suffers from key escrow problem. In this problem PKG, which is totally responsible for the entire key generations is suspected to exploit its privileges [22, 23].

Certificateless signcryption (CLSC): CLSC has both the qualities of PKI and IBSC. From IBSC it takes over the solution to certificate management issues and also eradicates the requirement of trusted authority in between [24]. This methodology does not utilize certificates while signcrypting messages and further the stress of management, revocation and storage of the certificates is also not incurred. CLSC uses Key generation centre which is responsible for generating partial private keys only. This partial key is then amalgamated with confidential information generated during encryption process to generate secret keys. Thus here third party key generator centre does not have any knowledge of user's private keys. So the key escrow problem is also solved in this scheme as key generation centre does not have complete access to user's secret keys. The scheme achieves various security requirements including confidentiality and non-repudiation.

B. *Difference between Signcryption and Sign-Then-Encryption*

Security is the priority step when sending message from sender to receiver. There is traditional method 'sign-then-encryption in which data transfer occurs, in which there following steps:

- Digital signature algorithm is utilized for signing the meassage.
- Then the message along with this digital signature is encrypted using private key encryption algorithm under randomly nominated encryption key.
- Thereafter, using receiver's public key, the random encryption key is encrypted.
- Finaly the message is sent to the receiver.

This method has the disadvantage that digitally signing and then encrypting the message takes large time and a lot of computational power.

Yuliang Zheng in 1997 invented a novel cryptography known as 'Signcryption' in which digital signature and encryption takes place in a solitary step. This scheme overcomes the limitations of sign-then-encryption scheme by providing less computational cost [23].

- **Traditional Method**
  - Encryption scheme
  - Signature-Then-Encryption Scheme
  - Encryption-Then -Signature Scheme

  Disadvantage:
  - Low efficiency
  - High computational cost and high computational overheads [27,28]
  - Time consuming

- **Signcryption**
  - Performs encryption and signing in a logical solitary step

  Advantage:
  - A solitary step that perform encryption and signature resulting in resource-efficiency.
  - Better and real-time data security [24].
  - Less computational overheads and less communication expenses [25].
  - Better overall performance and efficiency[25]

II. Related Work

Authors in [1] have given the overview of IoT and FIoT with the emphasis on implementing datamining to FIoT. A framework based on swarm optimization for intelligent data management was also defined in the research. In [2] a smart city scenario was defined that is capable of identifying the various aspects of IoT including resources and energy management, security, privacy and session management. A survey was implemented on IoT, its visions in different directions and related technologies were reviewed [3]. A wireless surveillance system based on IoT was designed that resulted in best minimum range of bandwidth and minimal video distortion [4]. In [5] authors worked on sending data securely from sensor to the internet host for efficient working of IoT. For this author designed a novel heterogeneous online/offline signcryption scheme that achieved privacy, reliability and substantiation in one single step. This scheme utilizes less computational cost in the overall interaction path and is effective and extensible in IoT environment. In [6] the author focused his research on issues and encounters in contrast to reliability and privacy in distributed IoTs'. Authors in [7] designed a secure and privacy based framework having multiple cloud servers for protecting the privacy of the patient's data. In [8] IoT and cloud computing were combined together and then analysis was made on their integration. The results showed that cloud computing improve the IoT devices functionalities and performance. In [9, 10] the IoT architecture, protocols, security issues and applications of IoT were discussed. Study was conducted on signcryption and a comparison between signcryption and sign-then-encryption approach was carried out to know the benefits of signcryption [11, 12]. Certificate signcryption was discussed in detail and a security model was designed to show its correctness in random oracle model [13, 14]. In [15] work was done on security of smart cameras as cameras captures various sensitive information and has open infrastructure thus are prone to high security risk. The author implemented a security technique using signcryption algorithm using Elliptic curve cryptography. By using signcryption resource efficiency was achieved as digital signature and generating ciphertext are implemented in one logical step. This architecture provides security against various threats and facilitates the authenticity of encrypted images. The experimental result demonstrates that this ECC based signcryption provides confidentiality and resource efficiency. In [16] author analyzed the security issues and challenges in previous signcryption schemes and designed an efficient and improved signcryption scheme that was based on ECC. In [17] author proposed a signcryption scheme that was heterogenous in nature and it was able to provide a secured communication from WSNs to a server. An efficient certificateless signcryption scheme was implemented in [18, 19]. An identity based signcryption scheme that satisfies various security conditions was implemented in [20, 21, 22]. Various authors have worked on signcryption techniques by to study the depth and the techniques used in this encryption scheme and how to get a secure system [23, 24, 25]. In [26] the researcher implemented a generalized certificateless signcryption scheme that focuses on providing security to the data being transmitted from IoT devices. Performance evaluation of the scheme showed that this scheme is applicable on resource-constrained devices and ensures confidentiality and authentication. In [27] an authentication protocol was developed to ensure security between data transmitted from IoT devices and cloud. This scheme was based on ECC encryption algorithm. This algorithm shows better results as compared to other asymmetric key algorithms .The research implementation outcome demonstrated that the protocol is secure and competent and also ensures low computational cost. The protocol is applicable on any HTTP enabled device and it results in reliable and the defined scheme ensures secure communication and mutual authentication. Authors in [28] designed a secure signcryption scheme that utilizes RSA as security algorithm for providing data security. The author concludes that his scheme offers security as it produces compact cyphertext but with high computational cost. In [29] the author proposes an efficient signcryption scheme based on RSA algorithm. Firstly message cyphertext is generated using RSA algorithm and thereafter signcryption key is developed which is of 126 bit. The scheme when experimented shows security and integrity and takes large file size. Improved signcryption scheme is designed in [30, 31, 32] to achieve high level of data security. Authors in [33] designed an elliptic curve based signcryption scheme that provides an improved signcryption scheme with the help of ECDLP that has high scalability and takes less storage space. A Certificateless multi-reciever aggregate signcryption based scheme was designed in [34] that provide integrity, authenticity and confidentiality of images and videos in multi-receiver environment. Figure 1 show the analysis which has been made by reviewing the literature survey.

III. Comparison Table

Different researchers have worked on the security of IoT data by implying various encryption algorithms. Table.1 shows the comparison that focus on the various encryption algorithms used by various researchers in the IoT data security. The comparison has been made on the basis of the technologies used, motive of the research, strength and the limitations of work done.

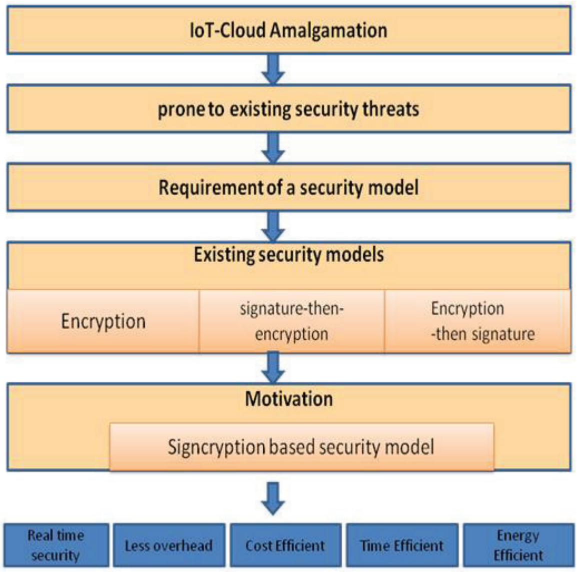
IoT-Cloud Amalgamation
prone to existing security threats
Requirement of a security model
Existing security models
Encryption
signature-then-encryption
Encryption -then signature
Motivation
Signcryption based security model
Real time security
Less overhead
Cost Efficient
Time Efficient
Energy Efficient

Fig. 1. Signcryption Based Security Model

TABLE I. Comparative analysis of various encryption algorithms

Paper	Technology Used	Motive	Strength	Limitations
Ting, P.Y et. al. [7]	Heterogeneous online/ offline signcryption scheme	To securely send data from sensor nodes to Internet Host	• Confidentiality • Integrity • Authentication • Non-repudiation • Less Computational Time	Only low power IoT devices is suitable under this scheme.
Ullah et. al. [17]	Signcryption based on ECC	The motive of the paper was to guard the data being retrieved from smart device like cameras.	• Authenticity, • Confidentiality, • Resource proficient • Short key size of ECC • Implementation of both signing and encryption in one step • Less Computational Time	It requires considerable calculations for more complex events detection which defy for sensing objects.
Karati et. al. [28]	A novel gCLSC	Message confidentiality in between two parties.	• Authenticity • Confidentiality when the IoT devices are resource-constrained.	Unforgeability makes this scheme less secure.
Kalra, S et. al.[29]	A mutual authentication protocol that utilizes ECC for key generation	The motive of this paper was to establish an authentic interaction using HTTP cookies between smart devices and cloud	• Low computational cost • Proposed model can be implemented on any embedded device that is HTTP enabled. • Better than any asymmetric key algorithms as ECC has less key size and thus takes less computational time.	Scheme lacks mutual authentication, forward secrecy, and a workable key Agreement. Suspected to the replay Attacks Suspected to the impersonation attacks.
Malone-Lee et. al. [30]	A signcryption scheme grounded on the technique based on RSA	The motive of this paper is to ensure privacy by providing proof of security.	• Non-repudiation • Privacy • Authenticity • Produces compact ciphertexts	This scheme offers high computational cost. Also Large key size of RSA takes more computation and encryption time.
Namdev et. al. [31]	RSA based signcryption scheme	To overview Signcryption Security Schemes	• Better execution time • File size is large • Security • Integrity	The scheme does not support different file format as it supports text file only.
Ahirwal et. al.[32]	Signcryption and ECC based framework	To specify signcryption scheme based on elliptic curves	• Less computational cost • Less computational overheads	Scheme is less efficient as there are more number of ECPM operations
Bala, S et. al. [33]	Signcryption scheme that works on Ellptic curves	To provide an improved signcryption scheme with the help of ECDLP	• Forward secrecy • Less storage requirement • Scalable	Lacks Message authentication in encryption model and has high computational cost.
Ullah, S. et. al. [34]	Certificateless multi-reciever aggregate signcryption based scheme	A light weight security approach for smart camera	• Integrity, authenticity and confidentiality of images and videos in multi-receiver environment	Scheme cannot be implemented on embedded smart cameras

IV. Conclusion

In this paper work implemented by various researchers has been analyzed to the depth in the domain of security of IoT data. Through this we focused upon encryption algorithms being implemented by these researchers. This paper aims at recognizing the strength and weakness of various algorithms that are utilized in IoT security. We found that most of the work has been done on signcryption algorithm, ECC and RSA algorithm. Signcryption is an encryption technique which has the capability and functionality of performing mutually digital signature as well encryption in single consistent step. As a result of this combined step, Signcryption technique works at a tremendously low cost than the traditional method in which the procedure is executed in two sequential steps of signing-then-encryption. Also signcryption which is based on elliptic curves is suitable for devices having low computing power and confined memory. ECC is better than any asymmetric key algorithms as it has less key size and thus takes less computational time. This makes ECC work more efficiently than RSA. ECC when used with signcryption for data security is more secure and ensures best result in terms of authenticity, confidentiality, integrity, non-repudiation, less computational cost and non-repudiation.

References

[1] Chhabra, R., Verma, S. and Krishna, C.R, A survey on driver behavior detection techniques for intelligent transportation systems. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence, pp. 36-41, 2017, January.

[2] Kakkar, L., Gupta, D., Saxena, S. and Tanwar, S., IoT Architectures and Its Security: A Review. In Proceedings of the Second International Conference on Information Management and Machine Intelligence (pp. 87-94). Springer,2021, Singapore.

[3] Tsai, C. W., Lai, C. F., & Vasilakos, A. V., Future Internet of Things: Open issues and challenges. Wireless Networks, 20(8), 2201–2217, 2014.

[4] Ning, H. S., & Liu, H., Cyber-physical-social-thinking space based science and technology framework for the Internet of Things. Science China Information Sciences, 58(3), 031102(19), 2015.

[5] Atzori, L., Iera, A. and Morabito, G., "The internet of things: A survey", Computer Networks, vol. 54(15), pp. 2787-2805,2010.

[6] Alsmirat, M.A., Jararweh, Y., Obaidat, I. and Gupta, B.B., "Internet of surveillance: a cloud supported large-scale wireless surveillance system", The Journal of Supercomputing, vol. 73(3), pp. 973-992, 2017.

[7] Ting, P.Y., Tsai, J.L. and Wu, T.S., Signcryption method suitable for low-power IoT devices in a wireless sensor network. IEEE Systems Journal, 12(3), pp.2385-2394, 2017.

[8] Roman, R., Zhou, J., & Lopez, J. , On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266–2279,2013.

[9] Kakkar, L., Gupta, D., Saxena, S. and Tanwar, S., An Analysis of Integration of Internet of Things and Cloud Computing. Journal of Computational and Theoretical Nanoscience,16(10), pp.4345-4349, 2019.

[10] Chhabra, R., Verma, S. and Krishna, C.R., A survey on driver behavior detection techniques for intelligent transportation systems. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 36-41). IEEE, 2017, January.

[11] Luo, E., Bhuiyan, M.Z.A., Wang, G., Rahman, M.A., Wu, J. and Atiquzzaman, M., Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. IEEE Communications Magazine, 56(2), pp.163-168, 2018.

[12] Stergiou, C., Psannis, K.E., Kim, B.G. and Gupta, B., 2018, "Secure integration of IoT and cloud computing", Future Generation Computer Systems, vol. 78, pp. 964-975.

[13] Zheng, Y., Signcryption and its applications in efficient public key solutions. In International Workshop on Information Security (pp. 291-312). Springer, 1997, September, Berlin, Heidelberg.

[14] Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption) _ cost (signature) ? cost(encryption). In Advances in Cryptology-CRYPTO'97, LNCS 1294 (pp. 165–179). Springer, 1997.

[15] Li, F., Han, Y. and Jin, C., Certificateless online/offline signcryption for the Internet of Things. Wireless Networks, 23(1), pp.145-158, 2017.

[16] Shi, W., Kumar, N., Gong, P., Chilamkurti, N. and Chang, H., On the security of a certificateless online/offline signcryption for Internet of Things. Peer-to-Peer Networking and Applications, 8(5), pp.881-885, 2015.

[17] Ullah, S., Rinner, B. and Marcenaro, L., Smart cameras with onboard signcryption for securing IoT applications. In 2017 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE, 2017, June.

[18] X. Zhou, "Improved signcryption scheme with public verifiability," in Proc. KESE Pacific-Asia Conference on Knowledge Engineering and Software Engineering, , pp. 178– 181, Dec 2009.

[19] F. Li, Y. Han, and C. Jin, "Practical signcryption for secure communication of wireless sensor networks," Wireless Personal Communications, vol. 89, no. 4, pp. 1391–1412, 2016.

[20] Ahene, E., Dai, J., Feng, H. and Li, F., A certificateless signcryption with proxy re-encryption for practical access control in cloud-based reliable smart grid. Telecommunication Systems, 70(4), pp.491-510, 2019.

[21] Li, F., Han, Y. and Jin, C., Certificateless online/offline signcryption for the Internet of Things. Wireless Networks, 23(1), pp.145-158, 2017.

[22] Chen L., & Malone-Lee, J. Improved identity-based signcryption. In Public Key Cryptography-PKC 2005, LNCS 3386 (pp. 362–379). Springer, 2005.

[23] Jo, H. J., Paik, J. H., & Lee, D. H. , Efficient privacy preserving authentication in wireless mobile networks. IEEE Transactions on Mobile Computing, 13(7), 1469–1481, 2014.

[24] Barbosa, M. and Farshim, P., Cetificateless signcryption. In Proceedings of the 2008 ACM symposium on Information, computer and communications security, pp. 369-372, 2008, March.

[25] Ullah, S., Russo, F., Marcenaro, L. and Rinner, B., "Aggregate-Signcryption for Securing Smart Camera IoT Applications", Global Internet of Things Summit, vol. 3(3) , pp. 1-6, 2018.

[26] Nishanth, R.B., Ramakrishnan, B. and Selvi, M., "Improved signcryption algorithm for information security in networks", International Journal of Computer Networks and Applications, vol. 2(3), pp. 151-157, 2015.

[27] Li, F., Shirase, M. and Takagi, T., Certificateless hybrid signcryption. In International Conference on Information Security Practice and Experience (pp. 112-123). Springer, 2009, April, Berlin, Heidelberg.

[28] Karati, A., Fan, C.I. and Hsu, R.H., Provably Secure and Generalized Signcryption With Public Verifiability for Secure Data Transmission Between Resource-Constrained IoT Devices. IEEE Internet of Things Journal, 6(6), pp.10431-10440, 2019.

[29] Kalra, S. and Sood, S.K., Secure authentication scheme for IoT and cloud servers. Pervasive and Mobile Computing, 24, pp.210-223, 2015.

[30] Malone-Lee, J. and Mao, W., Two birds one stone: signcryption using RSA. In Cryptographers' Track at the RSA Conference (pp. 211-226). Springer, 2003, April, Berlin, Heidelberg.

[31] Namdev, S. and Singh, P., An efficient FIS and RSA based Signcryption Security Scheme. International Journal on Recent and Innovation Trends in Computing and Communication, 2(9), pp.2612-2617, 2014.

[32] Ahirwal, R., Jain, A. and Jain, Y.K., Signcryption scheme that utilizes elliptic curve for both encryption and signature generation. International Journal of Computer Applications, 62(9), 2013.

[33] Bala, S., Sharma, G. and Verma, A.K., An improved forward secure elliptic curve signcryption key management scheme for wireless sensor networks. In IT Convergence and Security, pp. 141-149, 2013.

[34] Ullah, S., Marcenaro, L. and Rinner, B., Secure smart cameras by aggregate-signcryption with decryption fairness for multi-receiver IoT applications. Sensors, 19(2), p.327, 2019.