SN Computer Science (2021) 2:53
https://doi.org/10.1007/s42979-020-00429-z

ORIGINAL RESEARCH

Preserving Data Confidentiality in Internet of Things

Poornima M. Chanal[1] · **Mahabaleshwar S. Kakkasageri**[1]

Received: 17 July 2020 / Accepted: 12 December 2020

Abstract
The Internet of Things (IoT) is a network of linked physical objects worldwide, communicating via the Internet to one another. IoT expects the interconnection between a few trillions of intelligent things and the collected information offers a lot of private information needs to be analyzed and transmitted. So the provision of security to the information is a major challenge for many current and future applications of IoT. Basically, the main components of IoTs are Smartphone, Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), etc. The design and implementation of security and privacy management system for these things are driven by considerations such as good performance, information tampering, low power consumption, threat robustness and an end to end security. Security systems in IoT offer unauthorized access to information or other things by providing protection against modification or damage. In this paper, we propose a hybrid algorithm designed to preserve data confidentiality in IoT. Proposed algorithm design is a combination of Message Digest algorithm (MD5), Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) algorithms. The hybrid algorithm uses the concept of sharing geotag by destination IoT node to source node. Encryption involves three phases: Generation of fixed-length hash value i.e., hash function, encryption, and key generation. MD5 hash algorithm accepts plain text at the source IoT node as input and returns output a fixed length digest value. This value is encrypted using AES algorithm. Then ECC algorithm is applied to generate the encryption key. ECC offers a small key size and secured as compared to conventional cryptographic algorithms. We have simulated and analyzed the performance metrics of the proposed hybrid algorithm in terms of encryption time, memory utilization, end to end delay and decryption time w.r.t. varying file sizes as compared to AES encryption algorithm.

Keywords Internet of Things (IoT) · Message-Digest Algorithm · Confidentiality · Elliptic Curve Cryptography · Advanced Encryption Standard

Introduction

Internet of Things is a network of different devices, for example, sensors and actuators that can detect, connect, and respond to changes in unique condition. IoT assurances to enable an abundance of smart technologies in almost every area of our daily interactions and enhance the overall quality of life. The range of IoT application is outsized including smart office, smart homes, smart cities, e-health, etc. The scalability issue of IoT is unpredictable as tens and even hundreds of billions of devices will be associated. All devices in the network have keen abilities to gather, analyze and decide without any human communication. Hence privacy and security is an utmost constraint in such conditions. To allow several current and future applications, security and privacy in IoT need to be addressed at utmost care. The resource-constrained devices such as cell phones, WSNs and Radio Frequency Identifications (RFIDs), are part of IoT. Development of secure management systems for these devices are guided by different parameters such as good performance, tampering of the information, low power utilization, robustness to attacks and end to end security [1–5].

IoT main goal is to create smart systems and self-conscious independent devices used in the construction of smart cities, smart hospitals, intelligent transportation system etc., [6, 7]. In business, IoT provides good vision for various

✉ Poornima M. Chanal
pmcec@becbgk.edu

Mahabaleshwar S. Kakkasageri
mskec@beck.edu

[1] Department of Electronics and Communication Engineering, Basaveshwar Engineering College (Autonomous), Bagalkot, Karnataka 587102, India

Published online: 23 January 2021

organizations including IoT developers, various service providers, IoT integrators, network operators and software vendors [8, 9]. Scalability parameters and other restrictions on IoT device capabilities conclude that traditional cryptography protocols, protection algorithms, and security schemes are insufficient [10–12].

The security and privacy platform must be robust and the security architecture designed should be of good life span. When dealing with a large number of devices, some of the devices will be comprised of security and privacy aspects. Therefore, new design and development methodologies should be adapted to meet IoT requirements in terms of security and protection challenges are discussed in [13–17]. Security and protection are essentially liable for confidentiality, authentication, validation, non-repudiation and integration. So for efficient communication in IoT, all IoT objects should have powerful security intelligence mechanisms for cryptography to preserve confidentiality of data.

The data should not be available or disclosed to unauthorized peoples, entities, or processes is called as confidentiality. Confidentiality is one premier test of security and it shields information from unapproved individuals. Confidentiality in IoT, technologies can handle highly versatile prerequisites, heterogeneity of the structure in addition to resources scarcity of the embedded devices such as energy and computational constraints.

In this work, we addressed data confidentiality preservation using three algorithms such as Message-Digest (MD5), Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) algorithms. Next part of our work is given as: "Related Work" presents related works. "Proposed Work" presents the proposed work. Simulation and result analysis are mentioned in "Simulation". Conclusion part is given in "Conclusion".

Related Work

IoT enables interaction between entities and things, i.e., anything, anyone, anywhere and wherever. The Internet has evolved into more traditional than some other recent invention in a very small period [18, 19]. It has transfigured the system for human correspondence. This will be achieved by using a special Internet protocol that allows things to communicate with each other without human interaction. The advancement and eminence of IoT in everyday life and its design, conventions, a few potential applications are mentioned [20]. The author described different attacks on security and privacy. Various IoT layer structures, security issues of each layer and cross-layer hybrid integrations are examined [21, 22]. The system and security risks of IoT, and new multilayer security framework is presented in [23]. The latest IoT protection and Internet technology analysis, as well as new analyst methods and related security in certain IoT applications are discussed in [24]. IoT has gained more popularity and becoming more common in people lives, so prolonging the privacy and security in an intelligent manner is very crucial. Devices are restricted in size, battery life and computational techniques so they may not support the same of security and privacy as traditional Internet connected devices [25–27]. Total number of existing IoT devices and new devices connecting to the Internet will create new challenges and requires new approaches to solve the privacy and security issues.

The major challenges of security and privacy along with a new attack vector i.e., automated invasion attack is presented in [28]. Evolution of IoT, protocols, applications and security and privacy issues for real-world implementation of IoT are presented in [29]. IoT contains three layers: perception layer, transportation layer and application layer. Each layer security problems with solutions are mentioned in [30]. Cross-layer heterogeneous integration issues are also highlighted. IoT security risks, and a new multi-layer protection paradigm to strengthen IoT security methodology are explored in [31].

Some of the mature security technologies for protection, intrusion detection, authentication, and access control to enhance the safe, reliable and efficient operation in IoT is discussed in [32]. IoT presents unique challenges to the protection of individual privacy [33–35]. A description of a suitable query language is given in [36] to enable applications to extract the requested information from an information source. Information confidentiality is achieved for the desired information. Security structure with confidentiality and other issues of security and privacy are proposed in [37]. IoT challenging issues such as scalability, availability and stability are discussed in the work.

The evaluation of information and lightweight execution of the ECC algorithms is discussed in [38]. A survey on some security issues and some crypto-system solutions to address key confidentiality issues are described in [39]. Light weight 64-bit block cipher encryption algorithm used to encrypt secure IoT system information is discussed in [40]. The author presented the concept of geo encryption (location-based encryption) and modern geo-encryption in [41]. Security and privacy mechanisms of the IoT network are discussed in [42].

Cryptography techniques encourage in accomplishing security and privacy issues such as confidentiality, integrity, authentication etc. for powerful and popular security algorithms. Advanced Encryption Standard (AES) is a symmetric block cipher algorithm can encrypt or decrypt data. Compared with triple-DES, AES algorithm is faster and stronger. The AES algorithm has three key lengths which are 128, 192, or 256 bits. The AES encryption process consists of 10 rounds, 12 rounds and 14 processes in rounds for

128-bit keys, 192-bit keys, and 256-bit keys respectively. Except for the last round in each case, other rounds are identical [43, 44].

ECC is an important algorithm for public-key cryptography focused on the algebraic form of the elliptic curve over finite fields. This algorithm allows smaller keys than non ECC to provide equivalent security [45]. ECC algorithm refers to key agreements, pseudo-random generators, digital signatures and other functions. Indirectly, the key agreement can be paired with a symmetric encryption scheme to use them for encryption. The ECC algorithm is a public key crypto-system class which offers very strong security with lower bits key, offering faster performance and less computational complexity. A 160 bit key in the ECC algorithm offers the same level of security as 1024 bit key in the protocol Rivest Shamir Adleman (RSA). In key generation, both private and public key are generated [46, 47].

MD5 algorithm is widely used hash function producing a 128-bit hash value. Initially, MD5 was designed to be used as a cryptographic hash function, it has been found that it is more prone to significant vulnerabilities. It is still used as a checksum for verifying data integrity. Divides the input into 512-bit blocks each, and add 64-bit at the end of the last block to record the initial input length in the MD-5 algorithm. If the last block is less than 512 bits, some additional bits will be padded to the end [48, 49].

Time and energy usage of the AES can be performed with various key and buffer size in both hardware and software is discussed in [50]. Data transmission of secure framework using AES algorithm to provide security to data and analysis of different performance parameters like execution time and throughput are presented in [51].

Long Range Wide Area Network (LoRaWAN) and the Secure Low Power Communication (SeLPC) system is used to minimize the data encryption power of end devices using AES encryption cycles [52]. The SeLPC method presents the encryption key to improve safety level and simplifies the AES encryption process to minimize power consumption. Comparing with traditional AES, SeLPC method minimizes the encryption power.

ECC algorithm is an attractive and effective public-key crypto system algorithm based on the Secure Mobile Agent Protocol (BROSMAP) defined in [53] to provide confidentiality, authentication, authorization, transparency, accountability and non- repudiation. The ECC encoded hybrid DNA scheme [54] provides security at various levels. Selected DNA sequence is a sorting process, and a specific set of nucleotide groups is called allocated. These are translated directly to binary sequence and the encrypted using ECC. That provides security double-fold.

To store information in the cloud, a hybrid and stable algorithm is described in [55]. The algorithm helps to encrypt the data generated by AES before it is sent to the cloud by the edge device. Using the RSA cryptosystem the AES key is encrypted. The encoded RSA key is exchanged via electronic mail with the correct person. Cryptographic is an essential tool for information storage within a health care management system. An effective security on medicinal information in the IoT health care management system is discussed in [56]. Compared to other cryptographic algorithms, hybrid algorithms deal effectively with security challenges. Hybrid algorithm of encryption and decryption techniques to protect the data in the IoT network is discussed in [57].

A lightweight hybrid encryption scheme that uses the Elliptic Curve Diffie Hellman (ECDH) key exchange mechanism to produce keys and connect digital authentication signature is described in [58]. Three ways secured data encryption mechanism interprets three protection schemes of authentication, information security and verification. Low cost of computation and rapid speed make it easy for attackers to crack the security system while securing transmission information.

A hybrid model to ensure security, integrity and validity of information during the transmission is discussed in [59]. The model is a mixer of two cryptographic algorithms Secure Hash Algorithm (SHA-1) and hash generation algorithm. AES algorithm is used to encrypt and decrypt data. Hybrid cryptography is a combination of the two algorithms such as message digest and symmetric key cryptography [60]. The algorithm provides extra protection as well as confidentiality, authentication and integrity.

Hybrid Data Confidentiality (HDC) algorithm provides more security in IoT [61]. Initially, the data are encrypted with the mixture of AES-ECC algorithms is combined with the digest text document. The results are also based on the geolocation of the sender and receiver. It shows the great variance in keyspace and provides a high level of data confidentiality. A brief summarization of the existing privacy and security algorithms are depicted in Table 1.

Some of the problems that need to be addressed in preserving the data confidentiality for IoT are as follows: more robust encryption and decryption policies, minimization of encryption and decryption delay, optimized key size, etc. Hence in this paper, we propose a hybrid algorithm to preserve data confidentiality in IoT. Our proposed work is a grouping of Message-Digest algorithm (MD5), Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) algorithms.

Proposed Work

Our proposed work is a grouping of Message-Digest algorithm (MD5), Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) algorithms. The hybrid algorithm uses the concept of sharing geotag by destination

Table 1 Privacy and Security Algorithms

Sl. no.	Algorithm	Issue addressed	Mechanism used	Encryption delay	Decryption delay
1	Light weight encryption [38, 39]	Confidentiality	Geo-encryption	208–662 s	165–516 s
2	AES [49]	Integrity and confidentiality	SeLPC	140 s	96 s
3	RSA [52]	Authentication	–	220 s	190 s
4	Hybrid AES [55]	Authentication and confidentiality	ECDH	–	–
5	Hybrid SHA1, AES [56]	Integrity and validity	–	–	–
6	Hybrid RSA, AES [57]	Authentication, integrity and confidentiality	–	906 ms	890 ms
7	ECE [50]	Confidentiality, authorization, accountability, non-repudiation	BRoSMAP	–	–
8	DNA based ECC Scheme [51]	Security	DNA	–	–

IoT node to source node. Encryption involves three phases: Generation of fixed-length hash value i.e., hash function, encryption, and key generation. MD5 hash algorithm accepts plain text at the source IoT node as input and returns output a fixed-length digest value. This value is encrypted using AES algorithm. Then ECC algorithm is used to generate the encryption key. Ciphertext is added with geo-tags i.e., location information of the receiver. Receiver matches the identity of geo-tag. If identity matched, the ciphertext is decrypted as plain text otherwise, the ciphertext is discarded.

Our Contributions

More specifically our contributions are as follows: (1) AES, ECC, and MD5 based hybrid algorithm for preserving effective data confidentiality for IoT devices, (2) use of geo-tag in between source and destination as an additional feature, and (3) optimized key sizes for the usage of the hybrid algorithm to encrypt and decrypt information.

Proposed Hybrid Algorithm for Data Confidentiality

In this section network architecture and proposed confidentiality algorithm for IoT discussed.

IoT Network Architecture

In the proposed work, we have considered three layer architecture as shown in Fig. 1. Architecture has three layers: Layer 1 is perception layer, layer 2 is network layer and third layer is application layer. In IoT network, the perception layer identifies all devices. The different devices of layer 1 are sensors, actuators, cameras and RFID tags etc. At the first layer, sensor devices are used to sense and collect data about each thing in the IoT network. Network layer is the main and it establishes the connection between the devices and servers and transmits the collected information from layer 1. The application layer provides IoT application services to the user and it supports various applications such as smart cities, smart home and office, e-health; smart transport system etc.

Proposed Preserving Data Confidentiality Algorithm

Proposed algorithm uses geotag technique shared by destination node to source node before encryption process. Encryption involves three phases: Generation of fixed length hash value i.e., hash function, encryption, and key generation. MD5 hash algorithm accepts plain text and converts plain text as the hash value. This value is encrypted using AES algorithm. Then ECC algorithm is applied to generate the encryption key.

The operational sequence of the proposed hybrid algorithm is depicted in Fig. 2. Proposed data confidentiality preserving algorithm operates in the following sequence: MD5 hash algorithm accepts plain text at the source IoT node as input and returns output as fixed-length digest value. This value is encrypted using AES algorithm. Then ECC algorithm is applied to generate the encryption key. Then public key and a geo-tag (initially shared by the destination to source node) is added with ciphertext.

In the proposed work, we have considered up to 40 kbytes length of message size and 64 bytes of key size. First receiver will send request message for data to the sender along with location information called geo-tag (as shown in Fig. 2). At sender, for the plain text message of length L, MD5 hash algorithm is applied and output of the hash algorithm is encrypted using AES. The same plain text message of length L is encrypted using ECC algorithm. ECC algorithm output is also encrypted by AES. Ciphertext with public key and geotags (to assure guaranteed geolocations) is transmitted to the receiver. At the receiver side, decryption of cipher files is done using AES and ECC. Conversion of hash function using MD5 algorithm is carried out. In the final step, receiver collects data using a secret key if decrypted data hash function is compared with original hash function. Algorithms for encryption and decryption

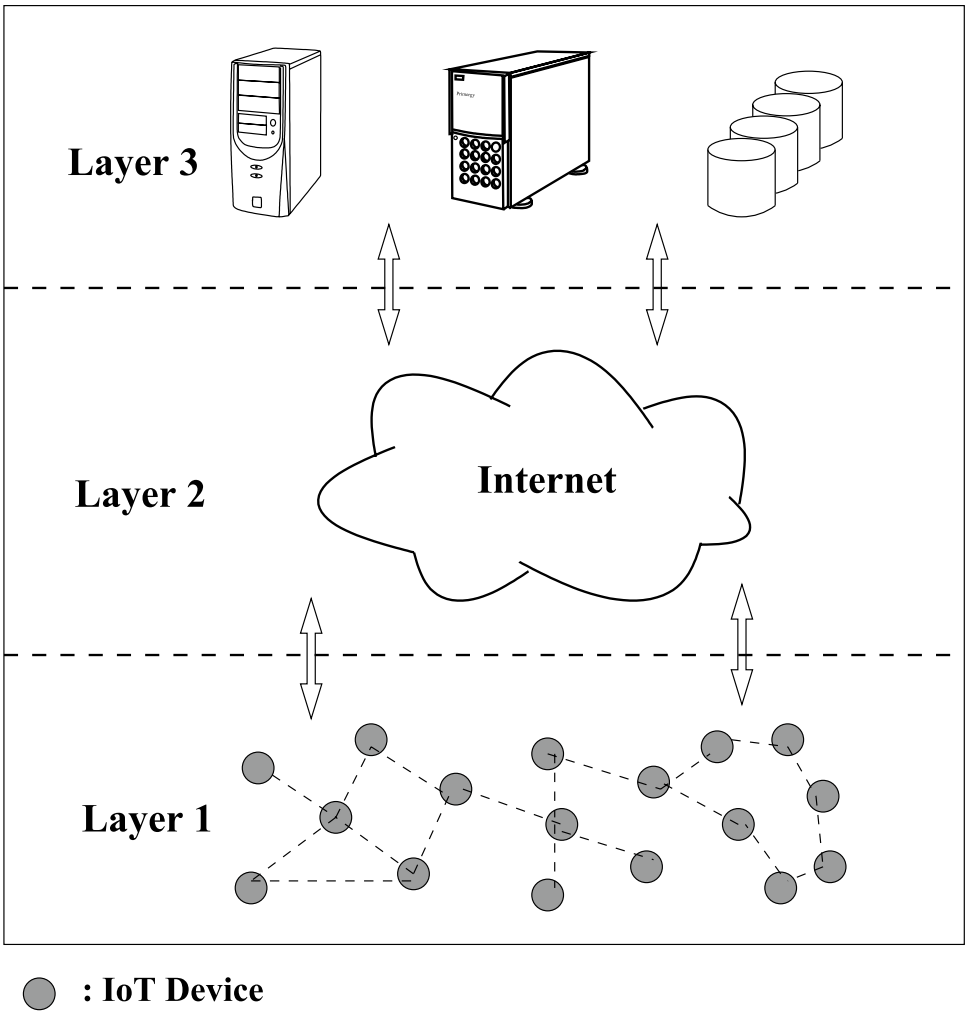

Fig. 1 Three layer IoT architecture

at the abstract level are presented in algorithms 1 and 2, respectively.

Algorithm 1 Algorithm for Encryption

1: **Begin**
2: Input data (Plain text)
3: Conversion of data into hexadecimal number
4: Perform shift rows operation to transform hexadecimal number into rows and column
5: Perform mix column transformation to transform each column into a new column
6: Add round key to each column to perform addition of matrix
7: XOR the output of the addition of matrix with key
8: Generation of encrypted message
9: **End**

Algorithm 2 Algorithm for Decryption

1: **Begin**
2: Input data (Cipher file)
3: Transform into hexadecimal number
4: Perform shift rows operation to transform hexadecimal number into rows and column
5: Perform mix column transformation to transform each column into a new column
6: Add round key to each column to perform addition of matrix
7: XOR the output of the addition of matrix with key
8: Generate original text message
9: **End**

Simulation

In this section, we discussed simulation inputs, performance parameters, and result analysis of our proposed work.

Simulation Inputs

In this proposed work, different simulation parameters considered are as follows: Number of nodes, N = up to 50, Communication range of nodes, R = up to 10 kms., Message size, Ms = 1 KByte to 40 KBytes, Key size, K = 64 Bytes.

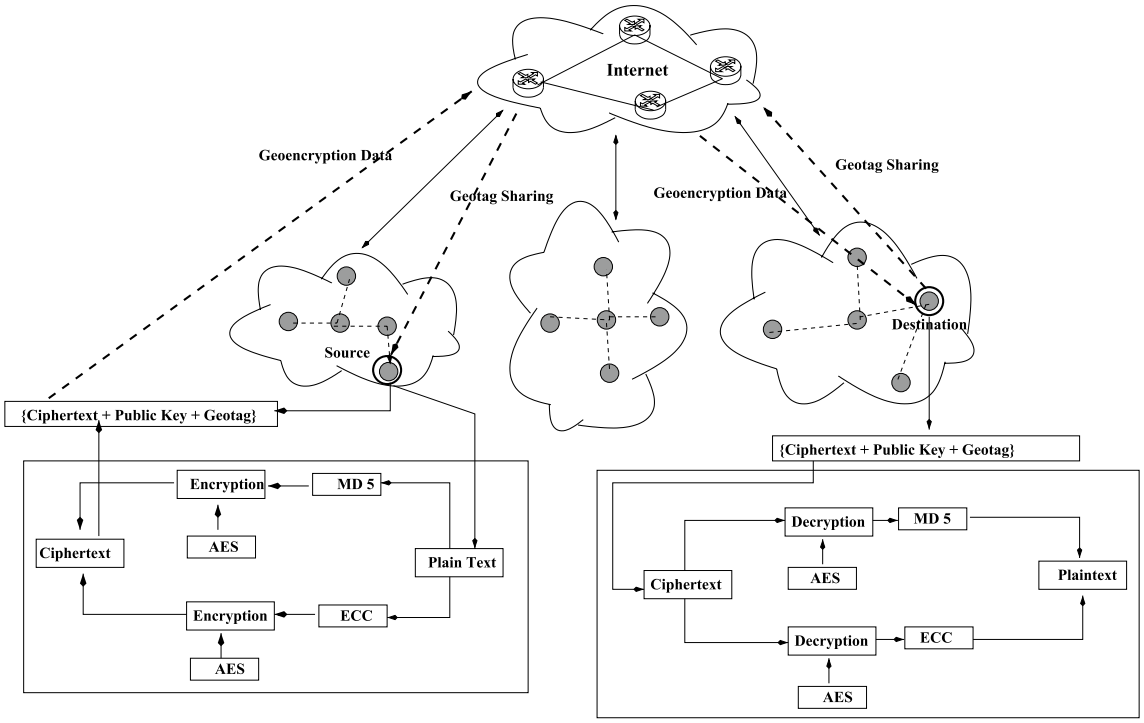

Fig. 2 Proposed hybrid algorithm operational sequence

Performance Parameters

To evaluate the efficiency of the proposed hybrid confidentiality algorithm, the following output parameters are considered and compared with the AES algorithm.

- Encryption time It is the time which is taken by the algorithms to produce ciphertext from plain text. It is expressed in milliseconds.
- Decryption time It is the time which is taken by the algorithms to produce plain text from ciphertext. It is also expressed in milliseconds.
- Key size It is the total length of key size, represented in terms of bytes.
- End-to-end delay It is the total time taken for encryption and decryption. It is represented in terms of milliseconds.
- Memory utilization Memory utilization is the amount of memory consumption at sender and receiver for encryption and decryption process. It is represented in terms of MBytes.
- Throughput at encryption It is the average of total plain text (message in kbytes) to the ratio of average encryption time. It is represented in terms of %.
- Throughput at decryption It is the average of total ciphertext to the ratio of average decryption time. It is represented in terms of %.

Result Analysis

Encryption time versus different message sizes of both AES and hybrid algorithm is shown in Fig. 3. Encryption time increases of both hybrid and AES algorithms as message size increases. The proposed hybrid algorithm displays less time for encryption than the AES algorithm. Decryption time of both AES and hybrid algorithm with message sizes is given in Fig. 4. As message size increases decryption time of both hybrid and AES algorithm also increases. Our proposed algorithm took less decryption time compared to AES.

Decryption time increases as message size increases, but the decryption time is less as compared to the AES algorithm. Different key size versus message sizes is shown in Fig. 5. Key size increases as message size increases for both hybrid and AES algorithms gradually. Figure 6 shows a total end to end delay for both hybrid and existing algorithm. As message size increases the total end to end delay is also increases. Figure 7 illustrates both hybrid and AES algorithms for the Message size w.r.t memory. When message size increases the memory consumption for both algorithms also increases. Figure 8 illustrates the number of attempts versus number of key bits. If the length of the key bit is 1 then the key is recovered after the 10 attempts. If the length of the key is increased to 5 then 10000 attempts are required which takes a lot of time to recover the key. This means that

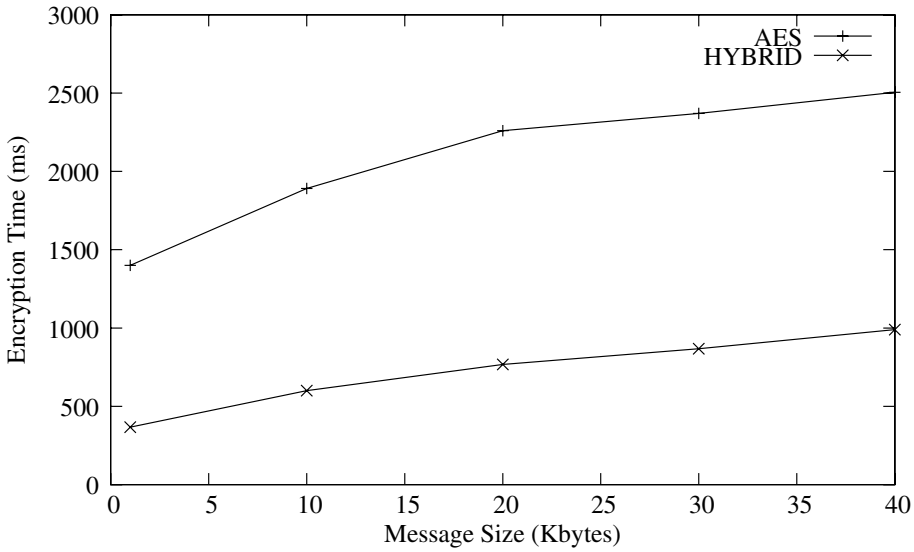

Fig. 3 Message size vs. encryption time

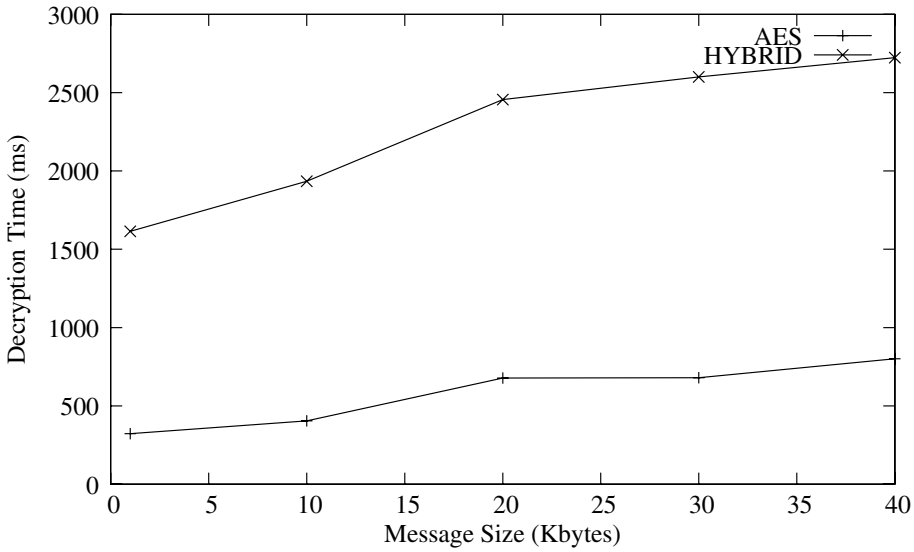

Fig. 4 Message size vs. decryption time

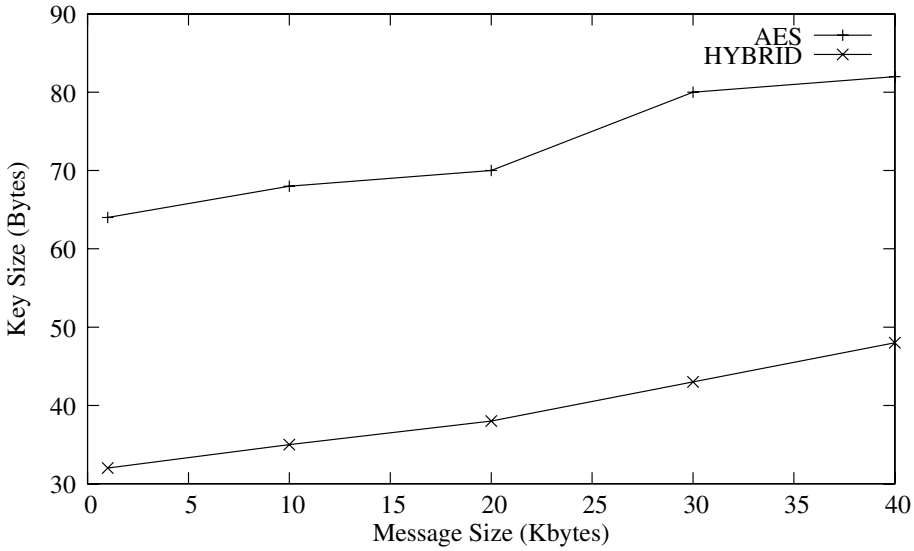

Fig. 5 Key size vs. message size

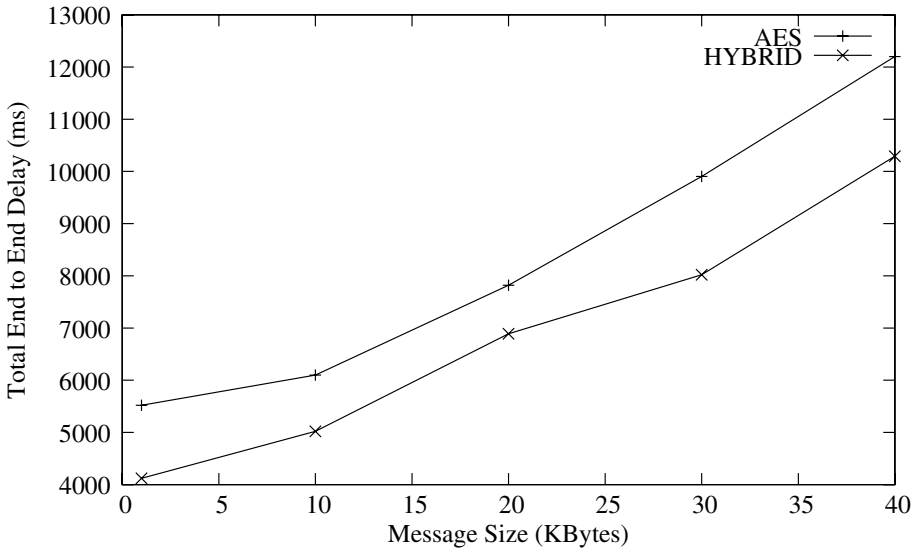

Fig. 6 Message size vs. end to end delay

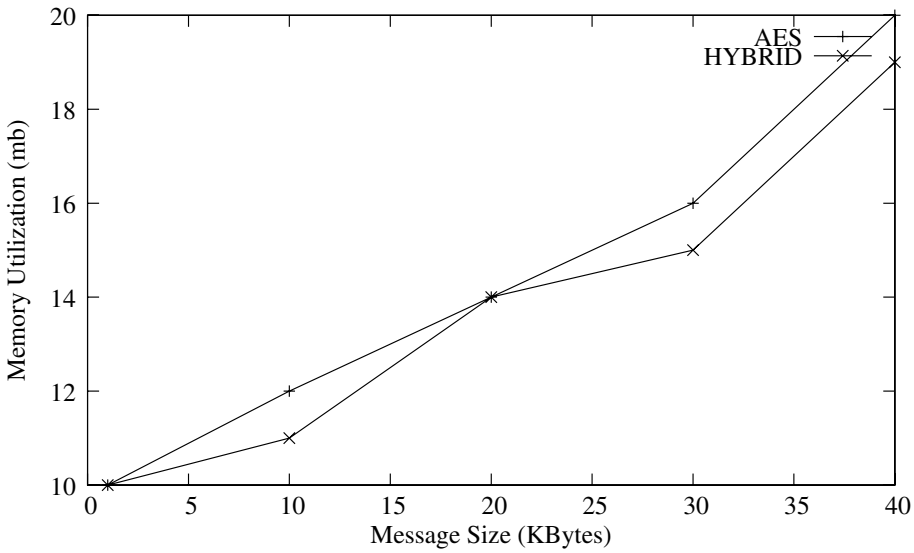

Fig. 7 Message size vs. memory utilization

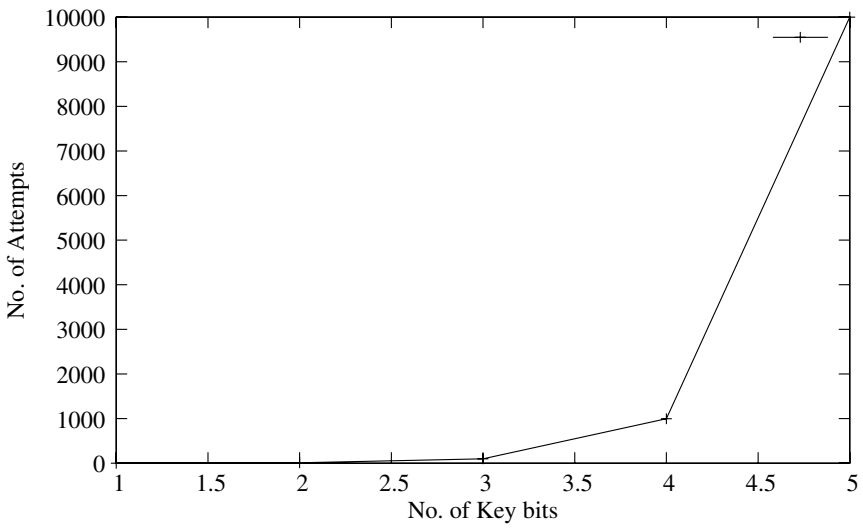

Fig. 8 No. of attempts vs. no. of bits

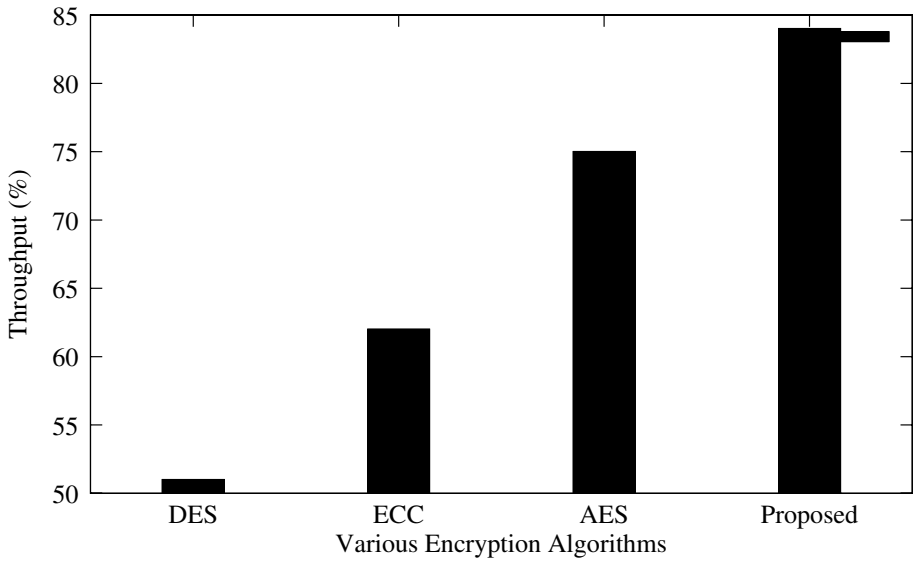

Fig. 9 Throughput of various encryption algorithms

security keeps on increasing as the key size increases but the control overheads of the system is also increased. Figure 9 shows throughput of various encryption algorithms. From the graph it is clear that the proposed algorithm provides more throughput than the other encryption algorithms. The proposed algorithms provide more throughput comparing with other decryption algorithms as shown in Fig. 10.

Table 2 shows the performance analysis of existing standard algorithms with a proposed hybrid algorithm, where proposed algorithm overall performance is best in terms of encryption delay, decryption delay, and end to end delay.

Conclusion

The secure transmission of data in IoT is a very difficult task. We proposed hybrid algorithm to provide confidentiality to every device. Hybrid confidentiality algorithm is a grouping of Message-Digest algorithm (MD5), Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) algorithms. The proposed algorithms provide strong confidentiality on the information transmission for IoT network. From the simulation and result analysis, we achieve that our proposed hybrid algorithm shows improved performance in terms of encryption time, decryption time, key size, memory utilization, end-to-end delay, and throughput as compared to the pure usage of AES algorithm for encryption. Further,

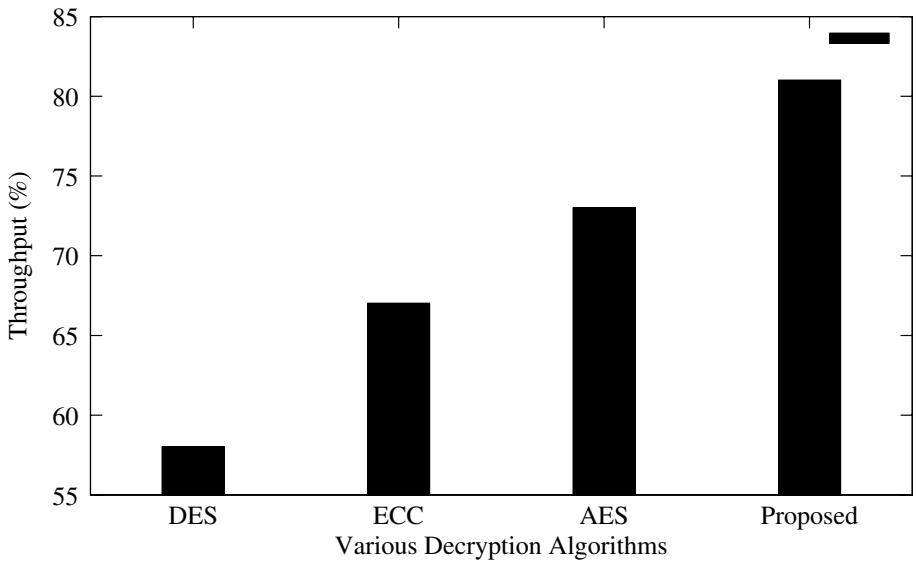

Fig. 10 Throughput of various decryption algorithms

Table 2 Performance Analysis of Existing Algorithms with Proposed Algorithm

Sl. no.	Algorithm	Issue addressed	Mechanism used	Encryption delay	Decryption delay	Total end to end delay
1	Light weight encryption [38, 39]	Confidentiality	Geo-encryption	208–662 s	165–516 s	16 s
2	AES [49]	Integrity and confidentiality	SeLPC	140 s	96 s	9 s
3	RSA [52]	Authentication, confidentiality	–	220 s	190 s	–
4	Hybrid AES [55]	Authentication and confidentiality	ECDH	–	–	–
5	Hybrid SHA1, AES [56]	Integrity and validity	–	–	–	–
6	Hybrid RSA, AES [57]	Authentication, integrity and confidentiality	—	906 ms	890 ms	21 ms
7	ECE [50]	Confidentiality, authorization, accountability, non-repudiation	BRoSMAP	–	–	–
8	DNA based ECC Scheme [51]	Security	DNA	–	–	–
9	Proposed Algorithm [AES, ECC, MD5]	Confidentiality	–	780 ms	823 ms	19 ms

the work may be extended by considering more number of nodes participating in the network activity, variable plain text size and key sizes.

Compliance with Ethical Standards

Conflict of interest Author Mrs. Poornima M. Chanal declares that she has no conflict of interest. Author Dr. Mahabaleshwar S. Kakkasageri declares that he has no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. J Future Gener Comput Syst. 2013;29(7):1645–60.
2. Covington M, Carskadden R. Threat implications of the Internet of Things. In: Proceedings of the 5th international conference on cyber conflict, Estonia; 2013, pp. 1–12.
3. Roman R, Najera P, Lopez J. Securing the Internet of Things. Int J Comput Netw. 2011;44(9):51–8.
4. Atzori L, Iera A, Morabito G. The Internet of Things: a survey. Int J Comput Netw. 2010;54(15):2787–805.
5. Bandyopadhyay D, Sen J. Internet of Things: applications and challenges in technology and standardization. Int J Wirel Pers Commun. 2011;58(1):49–69.
6. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of Things: vision, applications and research challenges. Int J Ad Hoc Netw. 2012;10(7):1497–516.
7. Yang D, Liu F, Liang Y. A survey of Internet of Things. In: Proceedings of the international conference on e-business intelligence (ICEBI'10), vol. 978, China; 2010, pp. 78–99.
8. Gérald S. The Internet of Things. In: Sylvie W, editor. Harald S, Patrick G, Peter F. Cluster of European research projects on the Internet of Things, European Commission Information Society and Media, Belgium: Vision and Challenges for Realising the Internet of Things; 2010. pp. 9–27.
9. Nicolaie LF, Till R, Jochen S, Wittenstein AG, Stefan F. IoT Applications - Value Creation for Industry. In: Ovidiu V, Peter F, editors. Internet of Things - Converging Technologies for Smart Environments and Integrated Ecosystems. Aalborg Denmark: River Publishers Series in Communications; 2013. pp. 153–204.
10. Suo H, Wan J, Zou C, Liu J. Security in the Internet of Things: a review. In: Proceedings of the IEEE international conference on computer science and electronics engineering, vol. 3. China; 2012, pp. 648–651.
11. Yang G, Xu J, Chen W, Qi ZH, Wang HY. Security characteristics and technology in the Internet of Things. Int J Nanjing Univ Posts Telecommun. 2010;30(4):20–29.
12. Internet of Things Strategic Research Road map. http://www.internet-of-thingsresearch.eu/pdf...pdf. Accessed 10 Feb 2020.
13. Yuqiang, Jianlan G, Xuanzi H. The research of Internet of Things supporting technologies which face the logistics industry. In: Proceedings of the international conference computational intelligence and security, Spain; 2010, pp. 659–663.
14. Pan J, Paul S, Jain R. A survey of the research on future internet architectures. IEEE Commun Mag. 2011;49(7):26–36.
15. Atzori L, Lera A, AMorabito G. The Internet of Things: a survey. Int J Comput Netw. 2010;54(15):2787–805.
16. Al-Fuqaha J, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor. 2015;17(4):2347–76.
17. Mahmoud E, Seyed S, Hon C. The Internet of Things: new interoperability, management and security challenges. Int J Netw Secur Appl. 2016;8(2):85–102.
18. Inayat A, Sonia S, Zahid U. Internet of Things security, device authentication and access control: a review. Int J Comput Sci Inf Secur. 2016;14(8):456–66.
19. Yinghui H, Guanyu L. Descriptive models for Internet of Things. In: Proceedings of the IEEE international conference

on intelligent control and information processing, China; 2010, pp. 483–486.
20. Surpon K, Panwit T. A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. In: Proceedings of the 11th international conference on wireless communications, networking and mobile computing (WiCOM'15), China; 2015, pp. 1–6.
21. Mahmoud E, Seyed S, Hon C. The Internet of Things: vision and challenges. In: Proceedings of the IEEE conference of IEEE region 10 (TENCON'13), Sydney; 2013, pp. 218–222.
22. Jing Q, Vasilakos AV, Wan J, Jingwei L, Dechao Q. Security of the Internet of Things: perspectives and challenges. Int J Mob Commun Comput Inf. 2014;20(8):2481–501.
23. Yang X, Li Z, Geng Z. Multi-layer security model for Internet of Things. Int J Internet Things. 2012;312(7):388–93.
24. Qiang C, Quan G, Bai Y, Yang L. Research on security issues of the Internet of Things. Int J Future Gener Commun Netw. 2013;6(6):1–10.
25. Farooq U, Waseem M, Mazhar S, Khairi A, Kamal T. A review on Internet of Things (IoT). Int J Comput Appl. 2015;113(1):1–7.
26. Sonar K, Upadhyay H. A survey: DDOS attack on Internet of Things. Int J Eng Res Dev. 2014;10(11):58–63.
27. Borgohain T, Kumar U, Sanyal S. Survey of security and privacy issues of Internet of Things. Int J Netw Appl. 2015;6(4):2372–8.
28. Mahmoud E, Seyed S, Hon C. The Internet of Things: vision and challenges. In: Proceedings of the TENCON spring conference, 2013, pp. 218–222.
29. Surapon K, Panwit T. A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. In: Proceedings of the 11th international conference on wireless communications, networking and mobile computing (WiCOM'15), 2015; pp. 1–6.
30. Qi Jing, Vasilakos Athanasios V, Wan J, Lu J, Dechao Q. Security of the Internet of Things: perspectives and challenges. Int J Wirel Netw. 2014;20(8):2481–501.
31. Yang X, Li Z, Geng Z, Zhang H. A multi-layer security model for Internet of Things. Int J IOT Workshop. 2012;312:388–93.
32. Sun X, Wang C. The research of security technology in the Internet of Things. Int J CSISE. 2011;105:113–9.
33. Weber RH. Internet of Things: privacy issues revisited. Int J Comput Law Secur. 2015;31(5):618–27.
34. Borgohain T, Kumar U, Sanyal S. Survey of security and privacy issues of Internet of Things. Int J Adv Netw Appl. 2015;6(4):2372–8.
35. Qiang C, Quan G, Bai Y, Yang L. Research on security issues of the Internet of Things. Int J Future Gener Commun Netw. 2013;6(6):1–10.
36. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of Things: vision, applications and research challenges. Int J Ad Hoc Netw. 2012;10(7):1497–516.
37. Farooq MU, Waseem M, Khairi A, Mazhar S. Critical analysis on the security concerns of Internet of Things (IoT). Int J Comput Appl. 2015;111(7):1–6.
38. Oriol P, Piol SR, Joakim E, Thiemo V. BSD based elliptic curve cryptography for the open Internet of Things. In: Proceedings of the 7th international conference on new technologies, mobility and security (NTMS'15), Paris; 2015, pp. 1–4.
39. Wang C. An IBE based security scheme on Internet of Things. In: Proceedings of the 2nd international conference on cloud computing and intelligence systems, China; 2012, pp. 32–37.
40. Rohollah K, Mohammad K. Enhancing security and confidentiality in location based data encryption algorithm. In: Proceedings of the 4th international conference on applications of digital informations and web technologies, USA; 2011, pp. 1–6.
41. Farooq MU, Waseem Muhammad, Khairi Anjum. Critical analysis on the security concerns of Internet of Things (IoT). Int J Comput Appl. 2015;111(7):1–8.
42. Shancang L. IoT node authentication. https://cdn.ttgtmedia.com/....ch4.pdf. Accessed 10 Apr 2020.
43. Mustafa EH, Masrullizam MI, Nurulfajar AM. Review on improvement of advanced encryption standard (AES) algorithm based on time execution, differential cryptanalysis and level of security. Int J Telecommun Electron Comput Eng. 2018;10(1):139–45.
44. Rayarapu A, Saxena A, Krishna NV, Mundhra D. Securing files using AES algorithm. Int J Comput Sci Inf Technol. 2013;4(3):433–5.
45. Vahdati Z, Ghasempour A, Salehi M. Comparison of ECC and RSA algorithms in IOT devices. Int J Theor Appl Inf Technol. 2016;97(16):4293–308.
46. Manvi SS, Kakkasageri MS. Message authentication in vehicular ad hoc networks (VANETs): ECDSA based approach. In: Proceedings of the international conference on future computer and communication, Malaysia, 2009.
47. Zargar AJ. Encryption and decryption using elliptical curve cryptography. Int J Adv Res Comput Sci. 2017;8(7):48–51.
48. Rivest R. The MD5 message-digest algorithm. RFC Editor; 1992.
49. Kasgar AK, Dhariwal MK, Tantubay N, Malviya H. A review paper of message digest 5 (MD5). Int J Mod Eng Manag Res. 2013;1(4):29–35.
50. Pedro SM, Nam T, Brandon C, Behnam D, Yuhong L. Analyzing the resource utilization of AES encryption on IoT devices. In: Asia Pacific signal and information processing association annual summit and conference, Hawaii, USA; 2018.
51. khambra D, Dabas P. Secure data transmission using AES in IoT. Int J Appl Innov Eng Manag. 2017;6(6):283–9.
52. Samiksha S, Vinay C. Analysis of AES encryption with ECC. In: Proceedings of the international conference on engineering science and management, Goa; 2016, pp. 195–201.
53. Haya H, Tasneem S, Dina S, Jamal Zemerly M, Chan YY, Mahmoud A-Q, Yousof AH. Secure lightweight ECC based protocol for multiagent IoT systems. In: Proceedings of the 13th international conference on wireless and mobile computing, networking and communications (WiMob'17), Rome, 2017.
54. Tiwari Harsh Durga, Kim Jae Hyung. Novel method for DNA based elliptic curve cryptography for IoT devices. Int J Electron Telecommun Res Inst. 2018;40(3):396–409.
55. Chandu Y, Rakesh Kumar KS, Khanolkar NV, Anish AN, Rawal S. Design and implementation of hybrid encryption for security of IOT data. In: Proceedings of the international conference on smart technologies for smart nation (SmartTechCon'17), Bangalore, August 2017.
56. Kavitha S, Alphonse PJA. A hybrid cryptosystem to enhance security in IoT health care system. Int J Wirel Microw Technol. 2019;1:1–10.
57. Trivedi DM, Raval TJ. Improving communication security in IoT using hybrid encryption decryption. Int J Adv Res Innov Ideas Educ. 2018;4(2):4175–82.
58. Tenzin Kunchok, Kirubanand VB. A light weight hybrid encryption technique to secure IoT data transmission. Int J Eng Technol. 2018;7(2):1–9.
59. Aruna Sankaralingam S, Usha G, Acharya Ankita. A hybrid cryptographic algorithm based on AES and SHA in RFID. Int J Pure Appl Math. 2018;118(11):835–40.
60. Jain Avinash, Kapoor V. Novel hybrid cryptography for confidentiality, integrity, authentication. Int J Comput Appl. 2017;171(8):35–40.
61. Chanal PM, Kakkasageri MS. Hybrid algorithm for data confidentiality in Internet of Things. In: Proceedings of the 11th

international conference on computing, communication and networking technologies (ICCCNT19), IIT, Kanpur, India, July 6–8, 2019.