A novel key exchange algorithm for security in internet of things

Koduru Suresh[1], PVGD Prasad Reddy[2], Padala Preethi[3]
[1,2]Department of CSSE, Andhra University, Visakhapatnam, India
[3]Department of Information Technology, NIT, Surathkal, India

Article Info

Article history:

Received Mar 2, 2019
Revised Jul 5, 2019
Accepted Jul 22, 2019

Keywords:

Cryptography
Internet of things
Public key exchange
Security

ABSTRACT

Today Internet of things (IoT) interconnects any object possessing sensing and computing capabilities to the internet. In this era, increasing number of electronic devices and applications in Internet of Things (IoT) requires secured communication with low power consumption capabilities. As security is a major challenge in internet of things, it is important to design a key management solution that considers resource constrained nodes and hence key management in public key cryptography is a crucial issue. In this paper, a novel key exchange algorithm was developed and implemented on a low powered "Raspberry pi machine" to realize the overall impact it creates on the device. The performance of the proposed algorithm had shown a great improvement over the popular Diffie Hellman key exchange algorithm and a two-level security for data exchange between the parties is implemented.

Corresponding Author:

Koduru Suresh,
Department of CSSE,
Andhra University, Visakhapatnam, India.
Email: koduru112@gmail.com

1. INTRODUCTION

From past few decades, working with and working for Internet of things (IoT) has become an interesting area in computer science. The term internet of things (IoT) refers to the connectivity of uniquely identifiable objects in internal or external environment through internet. Usually, IoT consists of components including sensing, heterogeneous access, information processing, applications and services.

In IoT, the devices will be connected to the internet and these devices will communicate with each other. It is expected that the growth of the connected devices will increase exponentially over jnext several years reaching a revenue of $19 trillion by end of 2020 [1]. Due to this, a new outbreak is opened for cyber-attacks in various applications such as automotive, industrial, smart homes, medical services, health care and intelligent transportation. Hence it is vital to address various challenges in information security and the networks should be equipped with various properties such as identification, confidentiality and integrality. To address the security problems of various applications, one of the important aspects that need to be considered is the authentication and key agreement for privacy protection and confidentiality. So far there is a well-known and widely trusted suite of cryptographic algorithms applied to internet security protocols as shown in Table 1 [2].

Table 1. A Suite of Cryptographic Algorithms

Algorithm	Purpose
Advanced encryption standard (AES)	Confidentiality
Rivest shamir adelman (RSA)/Elliptic curve cryptography (ECC)	Digital signatures key transport
Diffie-hellman (DH)	Key agreement
SHA-1/SHA-256	Integrality

Usually encryption is used to transfer the data using various algorithms to ensure that information is read by people possessing special knowledge and not everyone, which is usually referred as key and decryption is used for vice-versa process. Key encryption algorithms mainly include symmetric key algorithms and asymmetric key algorithms. Usually the symmetric encryption algorithm is used to encrypt data for confidentiality such as the advanced encryption standard (AES) block cipher. The asymmetric algorithms often used are Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC), Diffie-Hellman (DH) asymmetric key agreement, the SHA-1 and SHA-256 secure hash algorithms. As key management is one of the important aspects in most of the security mechanisms it always remains as an important topic for research. Hence it is important to design a key management solution that considers resources constrained nodes. Therefore, Key management in public key cryptography is a crucial issue and an attempt is made in this paper to improve the security with effective key management between the sender and receiver by defining a novel algorithm. The novel algorithm has better performance and security features when compared to Diffie Hellman algorithm.

The remainder of the paper is organized as follows. Section 2 presents the Literature Survey and section 3 provides the hardware and software components that are used to derive the test results. Methodology of novel algorithm is explained in section 4. Section 5 presents the results of the algorithm and conclusion is drawn in section 6.

2. LITERATURE SURVEY

With the advancement of technology and increased usage on Internet of Things, the key research areas with its problems are discussed by explaining how IoT can bring a distinct future [3]. Today the demand for offering effective security services such as confidentiality, integrity, authentication, availability and privacy is increasing exponentially for various applications. With this in view, a roadmap for security challenges in internet of things is derived in [4]. Here the roadmap for IoT security is presented based on cognitive and systematic approach. Later a case study based on smart manufacturing is considered to highlight the components and interactions based on defined cognitive and systematic approach [4]. Integration of internet of things with wireless sensor networks is discussed in [5] with existing methods such as basic sensor node architecture, stack-based approach, topology-based approach, WSN based approach, independent network and hybrid network by covering various security challenges such as node compromise, unauthorized data access and data privacy.

A top down survey for security in internet of things is elucidated in [6] covering the IoT applications and its security requirements with their impacts. Later a brief comparison of the available security solutions with its challenges were discussed, as internet of things has become internet of everything in day to day life. Similarly, Kai Zhao and Lina Ge [7] mentioned that the development of security capabilities as an important part of IoT. They have explored the security concerns in a three-layer system structure and proposed solutions to address the issues. In [8] performance analysis of various security algorithms for internet of things is derived by using cryptographic libraries such as FLECC_IN_C and Crypto++. The time taken for each operation is derived in milliseconds for various security algorithms that are considered. It is concluded that in a defined constraint environment there is an optimal performance with RSA1024 and LUCDIF per security routine. Light weight security algorithms such as Deffie-Hellman, Elliptic Curve Diffie-Hellman (ECDH) key agreement algorithms for low power devices were discussed in [9] where ECDH algorithm has achieved a significance in terms of low power and robustness. Authors in [10] discussed embedded security for internet of things requirements and the solutions that can be adopted for the devices that are vulnerable for security attacks. Here they have attempted to address the issues of security for data at rest. Similarly, today Internet of things is playing a major role in healthcare industry. But as mentioned in [11] there are many open challenges in this industry and security is one aspect of it where managing credentials, access to patient data, confidential information exchange should be handled effectively.

In [12] a review of communication security in internet of things is examined considering the standard security protocols that need to be used in conjunction with constrained application protocol (CoAP) that is used to adapt to the constraints of IoT devices. Here Datagram Transport Layer Security (DTLS) is used as a channel for CoAP and standardization efforts to enhance the DTLS for IoT applications is discussed in detail. IoT key management protocols were studied in [13] to understand the advantages and disadvantages of each protocol. The centralized and decentralized methods for two party key establishment protocols and key management protocols for group communication were discussed to perform security and key management evaluation. It is concluded that there is no unique solution to address all the security requirements for different IoT applications and hence it is important to understand the IoT application requirements in detail before defining an appropriate security solution. In [14] it is addressed that Smart home energy management systems form part of the smart grid program and smart home applications is one of the fast-developing areas. Today Inadequate security is a big issue in smart home energy management systems. They considered the major issue of security in smart home energy management systems to establish the initial session key between the wireless nodes and control center. To have improved security, a novel image encryption scheme using Gray code-based permutation approach is illustrated in [15]. The defined approach takes full advantage of Gray-code achievements and the proposed scheme have demonstrated good operational efficiency with high security. In [16] RF communication analysis of a low consumption asymmetric encryption is discussed where AA-Beta especially on encryption is feasible to preserve data integrity based on internet of things devices. Several researches were done based on IoT applications [17], [18, 19] to automate, reduce manual intervention and to use the applications in smarter way. But all these applications can still be extended with security aspects. Security aspects with respect to internet of things and data transmission over network are covered in several research studies. Advanced encryption scheme (AES) and compression using Huffman coding are used and later concealed in using DWT [20]. Advancement of watermarking using dual-layer fragile technique is used in [21] that guarantees integrity, authenticity and authenticity of user data. This technique has shown higher level of security in medical image data. Security attacks that are vulnerable over web were discussed and later the prevention methods are addressed in [22]. Honey encryption scheme (HE) is modified to support the encoding of natural language processing techniques. This resulted in producing syntactically correct messages that will help to deceive the attacker trying to decrypt a cipher text with incorrect keys [23]. N-tier modelling of robust key management and a cost-effective security paradigm with 2-tier model to safeguard cloud data with effective authentication are discussed in [24, 25].

The above-mentioned research efforts majorly focused on survey of internet of things and its applications for identifying the research problems and its solutions. Researchers have also tried to provide enhanced solutions using encryption mechanisms to have confidentiality, integrity and appropriate authentication in Internet of Things. Customizations are also done to have low powered devices where the existing security algorithms were evaluated to understand the performance under a constrained environment. In in paper we have customized the standard build files that suits to the low powered PI machine and we have proposed a novel key exchange algorithm that has shown greater improvement than Deffie-Hellman algorithm in a constrained environment.

3. SOFTWARE AND HARDWARE COMPONENTS

A customized environment has been setup up on a low powered PI machine to execute the defined libraries and algorithm by randomly passing test data sets. Crypto++® 8.1 libraries [26] are installed and compiled in local environment. The libraries suit to both 64-bit and 32-bit architectures which support major compiler and operation systems. Here the libraries were customized to fit the novel algorithm. The platform used is Raspberry Pi 3 and the system is prepared for compiling the libraries and to execute the sample code [27]. Here GCC compiler and Raspbian Jessie operation system is used to compare the execution time of novel algorithm and Diffie Hellman algorithm.

4. METHODOLOGY

It is hard to calculate modulus of integers that act as a tool in providing security to the applications during communication. Here a two-party key exchange algorithm is considered where both parties consider a large number common to them. The individual entities randomly generate a number and consider it as a private key. Then public keys are computed based on their private keys and gray code. The public keys are exchanged to generate the shared key. The below is the defined novel algorithm.

```
Algorithm
Step 1: Consider a large number - P (Large Prime number)
Step 2: Generate private keys, 'a' for Alice and 'b' for Bob
            (a and b should be greater than P)
            a = rand () // Any large number greater than P
            b = rand () // Any large number greater than P
Step 3: Compute $P_a$ and $P_b$ for Alice and Bob
            $P_a$ = a mod P // Public key of Alice
            $P_b$ = b mod P // Public key of Bob
Step 4: Convert $P_a$ and $P_b$ into binary & gray coded decimal
Step 5: Exchange of keys of both the parties
Step 6: Convert the exchanged public keys back to binary Code
```

Step 7: Calculate shared keys (S_a and S_b)
S_a = Shared key of Alice
S_b = Shared key of Bob

Shared key calculated by Alice:
S_a = [(Public key of Bob) * a]mod P // S_a = [P_b * a] mod P

Shared key calculated by Bob:
S_b = [(Public key of Alice) * b]mod P // S_b = [P_a * b] mod P

Step 8: Common shared key/ secret $S_a = S_b$
Step 9: End of program

Figure 1 explains the key exchange representation between Alice and Bob based on the defined novel key exchange algorithm.

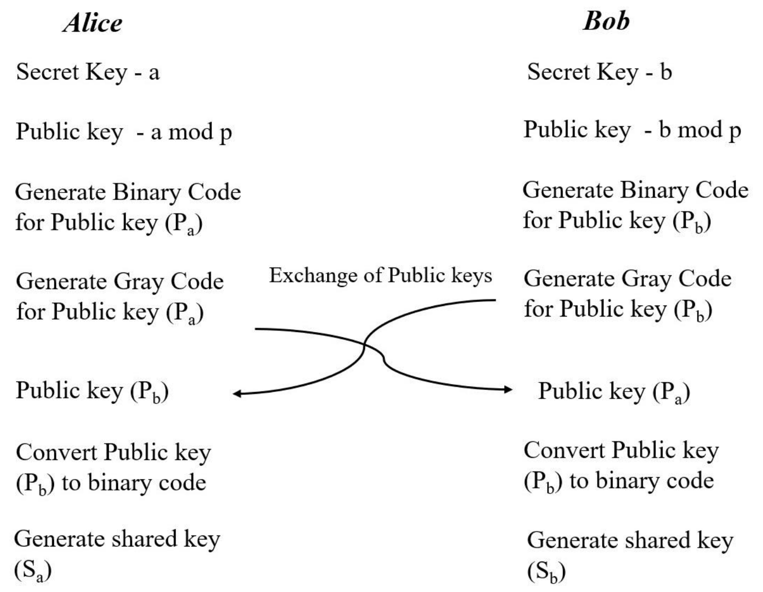
Alice
Bob
Secret Key - a
Secret Key - b
Public key - a mod p
Public key - b mod p
Generate Binary Code for Public key (P_a)
Generate Binary Code for Public key (P_b)
Generate Gray Code for Public key (P_a)
Exchange of Public keys
Generate Gray Code for Public key (P_b)
Public key (P_b)
Public key (P_a)
Convert Public key (P_b) to binary code
Convert Public key (P_b) to binary code
Generate shared key (S_a)
Generate shared key (S_b)

Figure 1. Key Exchange between Alice and Bob

5. RESULTS AND DISCUSSIONS

The novel algorithm that is developed on a low powered PI machine and Diffie-Hellman algorithm are evaluated based on various P values that randomly selected under a defined constrained environment. For Diffie- Hellman algorithm G values are also considered. Table 2 and Figure 2 illustrates the execution time in milliseconds for novel key exchange algorithm and existing Diffie-Hellman algorithm. Additionally, there is a two level security implemented with binary and gray code conversion as explained in section 4 that enables secure data exchange between two parties.

Table 2. Comparison of Novel Algorithm Vs Diffie Hellman Algorithm in (ms)

S. No	P	A	B	Novel algorithm	Diffie Hellman (G – P)
1	2873113	5440673	3899807	0.145	0.149
2	5858581	1186110	1144979	0.096	0.1237
3	6082007	5023326	3224938	0.0881	0.1308
4	6860989	5857950	8606894	0.112	0.1171
5	1014061	9531106	4600250	0.068	0.09176

As shown in Figure 2, the novel algorithm has greater improvement than Diffie-Hellman for the given sample data sets under the defined constrained environment.

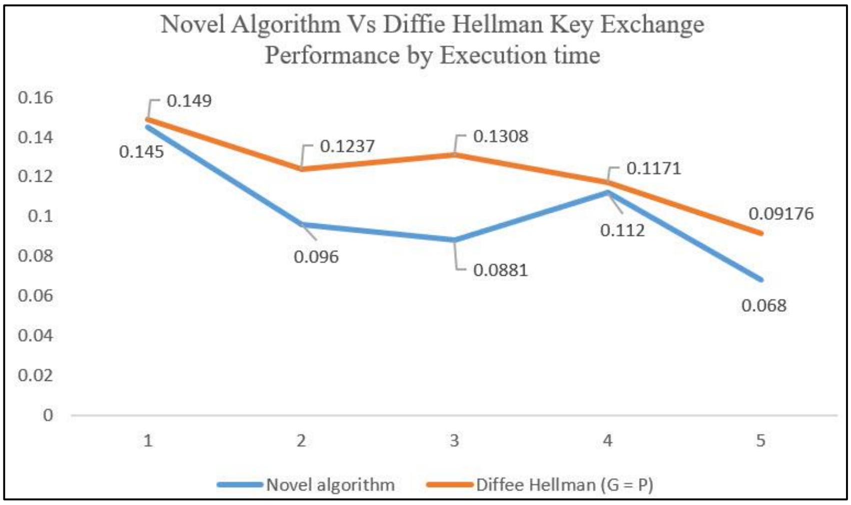

Figure 2. Comparison of Novel Algorithm Vs Diffie Hellman Algorithm

6. CONCLUSION

Though there are lot of researches on security aspects of Internet of Thigs, key management in IoT systems is still a challenging issue. In this paper the build files are customized to suit the low powered Raspberry PI machine. The proposed novel algorithm is simple and implemented on this machine. It has shown a greater improvement with respect to execution time and security over Diffie Hellman algorithm. The customized libraries and the proposed algorithm can be used to check if the overall carbon emissions can be reduced to achieve a green IoT solution.

REFERENCES

[1] Datafloq. Available: https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948.

[2] H. Suo, et al., "Security in the internet of things: a review," *2012 international conference on computer science and electronics engineering*, IEEE, vol. 3, 2012.

[3] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, pp. 3-9, 2014.

[4] A. R. Sfar, et al., "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, pp. 118-137, 2018.

[5] V. Reddy and Gayathri P., "Integration of Internet of Things with wireless sensor networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, pp. 439-444, 2019.

[6] D. E. Kouicem, et al., "Internet of things security: a top-down survey," *Computer Networks*, 2018.

[7] K. Zhao and L. Ge, "A survey on the internet of things security," *2013 Ninth international conference on computational intelligence and security*, IEEE, 2013.

[8] N. Khan, et al., "Performance analysis of security algorithms for IoT devices," *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, IEEE, 2017.

[9] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices," *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, IEEE, 2016.

[10] A. Ukil, et al., "Embedded security for Internet of Things," *2011 2nd National Conference on Emerging Trends and Applications in Computer Science*, IEEE, 2011.

[11] A. Rghioui and A. Oumnad, "Challenges and Opportunities of Internet of Things in Healthcare," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 2753-2761, 2018.

[12] S. L. Keoh, et al., "Securing the internet of things: A standardization perspective," *IEEE Internet of things Journal*, vol. 1, pp. 265-275, 2014.

[13] S. Naoui, et al., "Security analysis of existing IoT key management protocols," *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, IEEE, 2016.

[14] Y. Li, "Design of a key establishment protocol for smart home energy management system," *2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks*, IEEE, 2013.

[15] J. Chen, et al., "An efficient image encryption scheme using gray code-based permutation approach," *Optics and Lasers in Engineering*, vol. 67, pp. 191-204, 2015.

[16] S. F. S. Adnan, et al., "Testbed versus simulation approach on RF communication with AAβ asymmetric encryption scheme on internet of things devices," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, pp. 353-359, 2019.

[17] F. Kamaruddin, et al., "IoT-based intelligent irrigation management and monitoring system using Arduino," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, pp. 2378-2388, 2019.

[18] D. N. C. Loong, et al., “Machine vision based smart parking system using Internet of Things,” *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol. 17, pp. 2098-2106, 2019.

[19] S. A. W. Al-abassi, et al., “Smart prepaid traffic fines system using RFID, IoT and mobile app,” *TELCOMNIKA (Telecommunication Computing Electronics and Control*), vol. 17, pp. 1828-1837, 2019.

[20] C. A. Sari, et al., “An improved security and message capacity using AES and Huffman coding on image steganography,” *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol. 17, pp. 2400-2409, 2019.

[21] M. A. Ayu, et al., “Advanced watermarking technique to improve medical images’ security,” *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol. 17, pp. 2684-2696, 2019.

[22] M. Awad, et al., “Security vulnerabilities related to web-based data,” *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol. 17, pp. 852-856, 2019.

[23] A. E. Omolara and A. Jantan, “Modified honey encryption scheme for encoding natural language message,” *International Journal of Electrical and Computer Engineering (IJECE),* vol. 9, pp. 1871-1878, 2019.

[24] J. Metan and K. N. N. Murthy, “n-Tier Modelling of Robust Key management for Secure Data Aggregation in Wireless Sensor Network,” *International Journal of Electrical and Computer Engineering (IJECE),* vol. 9, pp. 2682-2690, 2019.

[25] Veena R. S., et al., “A cost-effective 2-tier security paradigm to safeguard cloud data with faster authentication,” *International Journal of Electrical and Computer Engineering (IJECE),* vol. 9, pp. 3833-3842, 2019.

[26] Raspberrypi. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/.

[27] Cryptopp. Available: https://www.cryptopp.com/.