Lightweight Security Architecture for Iot Device Communication

Vikas Reddy.S , Chandrashekara. SN

Abstract: Internet of Things (IoT) becomes part of our daily life. IoT has greatly uplifted the human life and has touched many aspect in our life style. IoT devices are sophisticated low-end device having limited computational and energy resources. Most of the cryptographic algorithms are based on complex mathematical calculation which is not feasible to be computed on IoT devices. Hence presently IoT devices lack strong security features. Security and privacy are becoming the real concern for IoT devices. In this paper we are exploring the various cryptographic algorithm which can be used for IoT device authentication and secure communication. The overall system is designed considering the light weight factor, scalability, time complexity and ease of implementation

Keywords :Public Key Infrastructure (PKI), Internet of Things (IoT), Elliptic Curve Diffie-Hellman (ECDH), Cryptography, Digital Certificate.

I. INTRODUCTION

The Internet of Things (IoT) is changing human life style in various ways. People are leveraging the benefit of IoT in almost all the fields. IoT is growing very rapidly and uplifting our daily life. The exponential growth of IoT has also increased the dimensions and complexity of the IoT connected network. As network security is already an important issue, IoT connected network poses many more challenges to be addressed with greater concern. IoT devices alone are not beneficial for any applications unless until it is connected with other devices or network. The traditional network and internet are well protected with security mechanism like Firewall, Intrusion Detection System etc. However, such mechanisms are designed, developed and implemented by keeping in view the architecture of network infrastructure and not suitable enough to secure the IoT networked system.

Conventional security system addresses many challenges of network infrastructure. However, there are many unique aspects associated with IoT, which require a different approach to secure IoT devices and infrastructure. Most of the IoT devices are directly interfacing and controlling the physical infrastructure. Any mishandling and exploitation in IoT devices and sensors will be devastating. Conventional security softwares, devices and techniques are resource incentive. Whereas the IoT devices do not have enough resources to perform heavy processing using conventional cryptographic algorithms[8][1][6].

II. IOT SECURITY AND PRIVACY ISSUES

As mentioned in introduction, IoT devices mostly interact with the physical world directly either to control the system or to collect the data for further process and analysis. Some of its security and privacy challenges are because of its intrinsic characteristics. Whereas some of its challenge are due to the integration of IoT and the Internet. Attackers may exploit the IoT system through its driver and embedded software or may exploit through the vulnerabilities in integrated network and Internet. Attack may occur through various ways from different points[4][5][6]. To design the security solution for IoT, it is important to understand the overall IoT system structure, information flow and various integration points which may be potential points of weakness.Below, we outline four security and privacy problems related to IoT systems:

A. Authentication

IoT devices are generally deployed in large distributed public infrastructure without any proper authentication. It is possible in large IoT enabled infrastructure that an IoT device or sensor may register itself claiming from specific location or it may be from different location. The demand for dynamic infrastructure makes authentication of IoT device challenging.

B. Integrity

Data integrity is one of the most important concern from security aspects. As mentioned, authentication of IoT device is challenging so the data integrity of IoT enabled network and system is also challenging. When the sensors are not authenticated, it is always possible that the data received is unreliable and tampered. It can be easily spoofed and forged. If the devices are of low quality the data can also be noisy.

C. Confidentiality

In general the IoT devices are interconnected using wireless networks. Because of low-end device, power and resource constraints, these wireless network connected with IoT devices lack many security features. Confidentiality measures ensures that the data cannot be accessed by unauthorized people. Unlike normal Wi-Fi network it is difficult for IoT device network to provide confidentiality.

Cryptography algorithms, encryption and key management can provide the confidentiality features, however implementing these security features need more power and resources.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

Vikas Reddy.S*, Assistant Professor, Department of Computer Science & Engineering , SJCIT, Chickballapur, India.

Dr. **S N Chandrashekara**, Professor, Head of the Department of Computer Science and Engineering at CBIT, Kolar, India.

Whereas the IoT devices has constraints on power and computational capabilities which puts barriers for security measures implementation.

D.Privacy

Privacy is major concern for IoT enabled networks and system. Privacy is, how the anonymity of individuals are preserved. It is a concern that how users information is used and shared or it has been used to trace the identity of user and its location.IoT devices and sensors collects large amount of dataand share it among peers. As discussed in the earlier section if authentication, integrity and confidentiality are not satisfied, Privacy issue will automatically emerge. If the device is exploitable and networks are vulnerable, there is always a risk of leaking data in global internet and exposing the anonymity of users.

III. SECURITY THREAT AND ATTACK TECHNIQUES IN IOT ENVIRONMENT

It may not be feasible to outline all the different types of security threats and attack techniques possible on IoT system as tactical combination may be many[4][3][7]. However some of the common attack techniques and scenario are as follows:

A.Eavesdropping

IoT devices are mostly connected through wireless channels. Since wireless medium are accessible by everyone, it is possible that some-one overhear the communication with wrong intention.

B.Impersonation

It is a kind of attack where adversary impersonate a trusted device. IoT systems are interconnected through various communication channels where many nodes join or leave the network randomly. It is possible that some of the malicious node pretend to be legitimate node.

C.Man in Middle Attack

When a malicious device intercept the communication between two systems or modify the traffic, it is called as Man-in-Middle Attack. Within the IoT network, we can imaging a scenario where a malicious device can feed the wrong temperature data to the monitoring device, so that overheat should potentially cause the physical and financial damage to the system.

D.Denial of Service Attack (DoS)

It is one of the most common and popular attack technique, where perpetrator incapacitate the device or network resource. Common approach to launch such attack is to overload the target device such that it will consume more computational resources, memory, bandwidth and power. The device will reach to its maximum working capacity and exhaust.

Some of the other sophisticated attacks on IoT devices are firmware attack, side channel attack, RAM attack etc.

Attack Scenario

In our proposed system we are addressing two primary security concerns.

-Prevention from malicious node from inside the IoT network:It is possible that some of the IoT devices within the network are compromised.

-Prevention from malicious node from outside the IoT network:As discussed in the section 2, IoT networks are dynamic in nature, where new IoT nodes can always join the network and leave the network dynamically. It is always possible that a new IoT sensor/device join the network claiming the genuine identity. It is also possible that some of the existing IoT devices are compromised and the data can be tampered.

In this paper authentication architecture is proposed to address the above issues.

IV. REQUIREMENTS FOR LIGHTWEIGHT CRYPTOGRAPHY ALGORITHM AND PROTOCOL

There are various issues related with the design and development of secure IoT based system. IoT devices are having limited capabilities[9][5]. It has limited amount of storage and processing capacities. IoT devices are designed to work on low power. It is important to consider following factors while designing algorithm for authentication and encryption.

- Processing Speed of Processor (Throughput)
- Power Consumption
- Circuit Size (ROM/RAM)

Size is important factor to be considered for implementation of algorithm in circuit board. Power is another major concern for a device based on battery driven energy resource. Power consumption is heavily dependent on the circuit size and processor speed. Throughput of the device is critical, as many of the IoT devices are used in real-time systems. Processing delay beyond certain acceptable values cannot be acceptable for the system. The system should also consider some of the quality factors which are as follows:

A.Scalability

It refers to the capability of a system to handle the growing amount of workload. In IoT system the growing size of IoT network with increased number of nodes, sensors, devices and demand for higher performance is important to consider. Many systemsare deployed over a large scale and hence it is important that system should support large number of nodes without any human intervention.

B.Consistency

IoT networks are built using various types of devices and protocols. The consistency among the protocols are important factor for the overall performance of the system.

C.Dynamic Mutual Trust

Dynamic movement of nodes are the inherent nature of IoT network. It is important that the each pair involved in communication should have a mutual trust agreement or authentication without any human intervention.

D.Minimal Human Intervention

The protocol should require minimal human intervention.

It should be self-configurable and should support dynamic node configuration.

V. CLASSIFICATION OF CRYPTOGRAPHY ALGORITHMS

Generally, cryptography algorithms are classified as asymmetric and symmetric cryptography. Asymmetric cryptography also known as public key cryptography uses pair of keys called as public key and private key. Public key is used for encryption of the message whereas private key is used for decryption. Paired key approach is the best feasible solution for providing the security architecture to IoT networked systems. It allows two devices to establish secure communication without the need of any pre-agreed shared key. However, public key algorithms are demanding in terms of computational resources and hence not feasible to be implemented in the IoT device directly. We need to design a mixed approach by using the asymmetric and symmetric algorithm. There are many symmetric and asymmetric key protocols available, however all these protocols are very resource intensive. We need to first analyze the time complexity of some well-known algorithms which can be suitable for our requirements. Based on literature we have identified the algorithms which are as follows:

A.RSA

RSA is a public key algorithm. It has both advantages and disadvantages. RSA is safe and secure because of its complex mathematical factorization which is not so easy to break. However the algorithm can be slow for large volume of data and has higher time complexity. Because of complex mathematical calculation it requires more computational effort and power consumption.

B. Diffie-Hellman

The Diffie-Hellman key exchange protocol is one of the well-known protocol used for secure key exchange. The security of Diffie-Hellman protocol is based on the discrete logarithm problem. Diffie-Hellman protocol is only used for key-exchange and does not support encryption or decryption directly. The advantage of algorithm is that both the sender and receiver need not have prior knowledge about each other and communication can take place through insecure channel. The disadvantageis, it cannot be used for asymmetric key exchange.

C.Elliptic Curve Diffie-Hellman

Elliptic Curve Diffie-Hellman protocol is used for key generation and sharing between two parties. It is getting popularity because it requires less computational resources and it is fast. It provides feasible solution for small devices where security is important but simultaneously power and computational resources are also a concern.

- *Curve25519:* It is one of the variation of Elliptic Curve Diffie-Hellman protocol which provides the security up-to 128-bit key length. The performance of the Curve25519 is significantly better than the NIST standard elliptic curve and hence widely used in various popular applications.

VI. PERFORMANCE ANALYSIS

We analyzed the performance of the selected public-key algorithm for generating a key pair and time taken for secret key exchange. The evaluation has been done on Intel Core i5 Processor with 16 GB RAM on Ubuntu 16.04.2 LTS. Fig 1 shows the time complexity of algorithms for generating the key whereas Fig 2 shows the time complexity for key exchange.

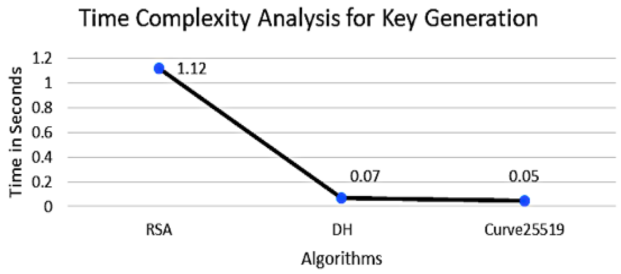

Fig 1:- Time Complexity Analysis for Key Generation

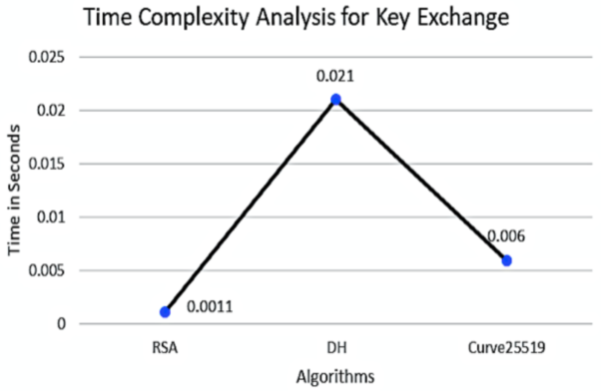

Fig 2:- Time Complexity Analysis for Key Exchange

One of our objective is to exchange key between the IoT device and gateway for authentication and secure communication. There are many key exchange protocols available based on asymmetric key algorithm but these algorithms are vulnerable to Man-In-The-Middle (MITM) attacks. An alternate approach to prevent from MITM attack is to implement the device Certification Authorities (CA) and Public Key Infrastructure (PKI). Our proposed system architecture is developed on the PKI which is based on Elliptic Curve Digital Signature with the Curve25519 algorithm because of better performance.

VII. PROPOSED SYSTEM ARCHITECTURE

In this section we are proposing the overall system architecture. The objective of the proposed system is to solve some of the basic security requirements mentioned in the section III. The proposed system will serve the purpose of device authentication and trusted communication. The proposed system is implemented based on the consideration of various design factors i.e. light weight algorithm, efficiency, time complexity, scalability etc. as discussed in section IV. The overall system architecture is shown in Fig 3. The major components of the system are as follows:

Certificate Authority (CA):- Certificate Authority (CA) is a device responsible for issuing and revoking the digital certificates. It can be implemented using OpenSSL and an open source certificate toolkit. Certificate toolkit helps the administrator to configure various parameters for the certificate and the criteria which device or users must fulfill to enroll for a digital certificates.

Authenticated Device: - All the IoT devices in the network must have a public key for communication. The device must be registered through Registration Authority and should have a valid certificate.

Registration Authority (RA):- It is an important component of PKI. RA takes care of user request for digital certificate. Any device which needs a Digital Certificate has to request RA, which verifies the user request and ask the CA to issue the Digital Certificate for the requested device.

The security architecture of overall system is based on PKI as shown in fig 3. Any new IoT device which wants to communicate with other IoT devices in network need to first register itself and acquire a digital signature. The IoT device can initiate the registration process throughRA. Once the device is successfully registered and acquired the digital signature, it can use the recipients/receiving IoT device public key for encrypting the message for secure communication. Since all the IoT devices in the network must have a valid digital signature it protects the network from forged, spoofed or malicious devices. The authentication among the devices are performed using Elliptic Curve Digital Signature with the Curve25519 algorithm. The authenticated devices can securely communicate data using a session key that is shared via EDCH based on Curve25519 algorithm.

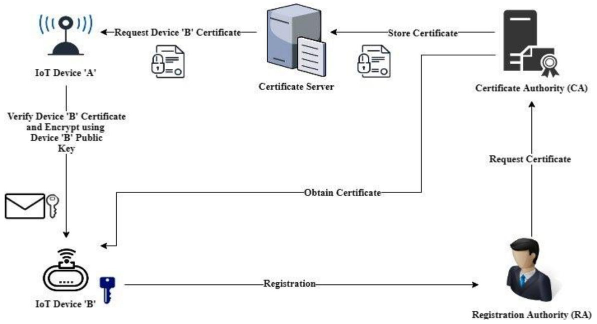
Request Device 'B' Certificate
Store Certificate
IoT Device 'A'
Certificate Server
Certificate Authority (CA)
Verify Device 'B' Certificate and Encrypt using Device 'B' Public Key
Request Certificate
Obtain Certificate
Registration
IoT Device 'B'
Registration Authority (RA)

Fig 3:- IoT Device Public Key Infrastructure

VIII. RESULT ANALYSIS AND CONCLUSION

Computational resource, memory and power consumptions are the major concerns for designing security architecture for IoT system. Most of the cryptographic algorithmsare based on complex mathematical computations which are not feasible to be computed on IoT devices because of severely resource constraints. We have explored various cryptography algorithms which are best in performance and light weight. In our time complexity analysis, we found that Elliptic Curve Digital Signature with the Curve25519 algorithm is one feasible solution because of its performance. The overall system was implemented using PKI and Elliptic Curve Digital Signature with the Curve25519 algorithm. The system was tested with six IoT devices in a wireless network in close range of 100-meter open space without any obstacle. Based on device capacity each device took different time duration for registration, authentication and secure communication. In experimental analysis it was found that on average IoT device took 15-20 seconds for authentication and establishing the secure communication. The result varies based on the network speed, distance between the devices, key size and computational speed of the devices.

REFERENCES

1. A. K. Sahu, S. Sharma, D. Puthal, A. Pandey and R. Shit, "Secure Authentication Protocol for IoT Architecture," 2017 International Conference on Information Technology (ICIT), Bhubaneswar, 2017, pp. 220-224.
2. F. Ye and Y. Qian, "A Security Architecture for Networked Internet of Things Devices," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6.
3. Flauzac Olivier, Gonzalez Carlos, Nolot Florent, New Security Architecture for IoT Network, Procedia Computer Science, Volume 52, 2015, Pages 1028-1033, ISSN 1877-0509.
4. Job Noorman, Jo Van Bulck, Jan Tobias Mühlberg, Frank Piessens, Pieter Maene, Bart Preneel, Ingrid Verbauwhede, Johannes Götzfried, Tilo Müller, and Felix Freiling. 2017. Sancus 2.0: A Low-Cost Security Architecture for IoT Devices. ACM Trans. Priv. Secur. 20, 3, Article 7 (July 2017), 33 pages.
5. M. Radovan and B. Golub, "Trends in IoT security," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2017, pp. 1302-1308.
6. O. Salman, I. Elhajj, A. Chehab and A. Kayssi, "Software Defined IoT security framework," 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, 2017, pp. 75-80.
7. R. Román-Castro, J. López and S. Gritzalis, "Evolution and Trends in IoT Security," in Computer, vol. 51, no. 7, pp. 16-25, July 2018.
8. Rafael Alvarez, Cándido Caballero-Gil, Juan Santonja, and Antonio Zamora. Algorithms for Lightweight Key Exchange. Sensors 2017, 17(7), 1517.
9. S. Kulkarni, S. Durg and N. Iyer, "Internet of Things (IoT) security," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 821-824.
10. Sibin Mohan, Mikael Asplund, Gedare Bloom, Ahmad-Reza Sadeghi, Ahmad Ibrahim, Negin Salajageh, Paul Griffioen, and Bruno Sinopoli. 2018. The future of IoT security: special session. In Proceedings of the International Conference on Embedded Software (EMSOFT '18). IEEE Press, Piscataway, NJ, USA, Article 16, 7 pages.
11. T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan and Q. Jin, "A Secure IoT Service Architecture With an Efficient Balance Dynamics Based on Cloud and Edge Computing," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4831-4843, June 2019.

AUTHORS PROFILE

Vikas Reddy.S completed MS from University of Texas at Dallas, USA, currently pursuing Ph.D on Internet of Things (IoT) domain in VTU Belgaum,he is author of a book titled “Fundamentals of Computer Networks”. He is currently working as Assistant Professor in department of Computer Science & Engineering , SJCIT, Chickballapur, India. He is a member of CSI and IEI.

Dr. S N Chandrashekara, is currently working as Professor and Head of the Department of Computer Science and Engineering at CBIT, Kolar, India. He received his Bachelor of Engineering from Bangalore University and Masters of Technology in Computer Science and Engineering from NITK, Suratkal. He was awarded Ph.D in Network and Devices from IISc, Bangalore. His area of research includes Computer Networks, Cloud Computing, Cyber Security and IOT Medical Image Processing. He is a Life Member of Indian Society for Technical Education, Computer Society of India. He is a Fellow of Institute of Engineers and Life member of ISSE.