ELLIPTIC CURVE CRYPTOGRAPHY SECURITY IN THE CONTEXT OF INTERNET OF THINGS

[1]Shruti.P, [2]Chandraleka.R,
[1]Department of Computer Science and Engineering,
[2]Department of Information Technology,
Government College of Technology
Coimbatore, India
[1]shrutipadmakumar6@gmail.com, [2]chandraleka611@gmail.com

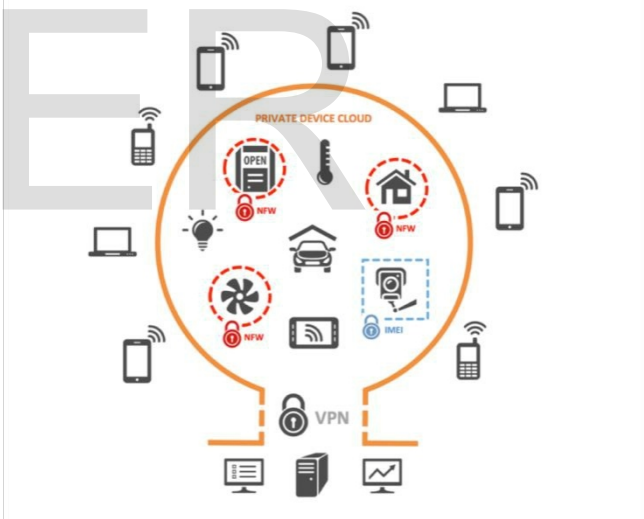
Abstract

One of the buzzwords in the Information Technology is Internet of Things (IoT). The future is Internet of Things, which will transform the real world objects into intelligent virtual objects. As many resources are being shared via internet, security becomes an essential entity in current trend..This paper describes in detail about the various security methods that can be applied to internet of things .Elliptic Curve Cryptography is one of the methods in access booting that can efficiently encrypt/decrypt the data by the use of digital signatures. Key generation serves as an important part in Elliptic Curve Cryptography, as both public and private key needs to be generated. This method ensures to provide an efficient privacy and security when compared with the other algorithms used in cryptography.

Keywords—IoT, Security, Access booting, Elliptic Curve Cryptography, Key.

I. INTRODUCTION

The Internet of Things (IoT) is the inter-networking of physical devices like vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. IoT security is the area of endeavour concerned with safeguarding connected devices and networks in the Internet of things (IoT).The Internet of Things[7] involves the increasing prevalence of objects as things provided with unique identifiers and the ability to automatically transfer data over a network. Much of the increase in IoT communication comes from computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home building automation, vehicle to vehicle communication and wearable computing devices. The main problem is that because the idea of networking appliances and other objects is relatively new, security has not always been considered in product design. IoT products [8] are often sold with old and unpatched embedded operating systems and software. Purchasers often fail to change the default passwords on smart devices or if they do change them, fail to select sufficiently passwords. This paper lists out some methods of security that could be applied to the future IoT products.



II. REVIEW OF LITERATURE

Elliptic curve cryptography is a newer a newer approach to public key cryptography based on algebraic structure of elliptic curves over finite fields and considered as a efficient technique with lower key size for the user and hard exponential time challenge for the attacker to break into the system. In ECC a 160 bit key provides the same security as RSA with 1024 bit key. It requires only lower computation

and less memory space. The advantage of the ECC is the absence of the sub exponential time algorithms and uses less key size and provides more security. ECC is widely used in many fields. It is used in devices which has less storage memory especially popularly employed in smart cards. Smart cards are being used as a bank cards, electronic tickets, personal identification cards, etc. Most of the manufacturing companies are producing smart card that makes use of elliptic curve digital signature algorithms. ECC is used in wireless communication and in devices with low computing power and resources such as mobile devices. For implement ECC, constrained devices have been considered to be the most suitable platform. Smaller key size results in faster execution which is beneficial to systems where real time performance is a critical factor. It is also not an easy task to choose appropriate elliptic curve [28]. ECC standardization is crucial for achieving practical and efficient implementation. National Institute of Standards and Technology (NIST) provides specification for ECC which are considered safe for the use in cryptographic application [29]

III. METHODS OF SECURITY IN IOT

Security methods deployed in IoT can be broadly classified into the following five types

- Secure booting
- Access control
- Device authentication
- Firewalling and IPS
- Updates and patches

A. Secure booting

When power is first introduced to the device, the authenticity and integrity of the software on the device is verified using cryptographically generated digital signatures. In much the same way that a person signs a cheque or a legal document, a digital signature attached to the software image and verified by the device ensures that only the software that has been authorized to run on that device, and signed by the entity that authorized it, will be loaded. The foundation of trust has been established, but the device still needs protection from various run-time threats and malicious intentions.

B. Access control

Mandatory or role-based access controls built into the operating system limit the privileges of device components and applications so they access only the resources they need to do their jobs. If any component is compromised, access control ensures that the intruder has as minimal access to other parts of the system as possible. Device-based access control mechanisms are analogous to network-based access control systems such as Microsoft Active Directory, even if someone managed to steal corporate credentials to gain access to a network, compromised information would be limited to only those areas of the network authorized by those particular credentials. The principle of least privilege dictates that only the minimal access required to perform a function should be authorized in order to minimize the effectiveness of any breach of security.

C. Device authentication

When the device is plugged into the network, it should authenticate itself prior to receiving or transmitting data. Deeply embedded devices often do not have users sitting behind keyboards, waiting to input the credentials required to access the network. How, then, can we ensure that those devices are identified correctly prior to authorization? Just as user authentication allows a user to access a corporate network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials stored in a secure storage area .

D. Firewalling and IPS

The device also needs a firewall or deep packet inspection capability to control traffic that is destined to terminate at the device. Why a host-based firewall or IPS is required if network-based appliances are in place? Deeply embedded devices have unique protocols, distinct from enterprise IT protocols. For instance, the smart energy grid has its own set of protocols governing how devices talk to each other. That is why industry-specific protocol filtering and deep packet inspection capabilities are needed to identify malicious payloads hiding in non-IT protocols. The device needn't concern itself with filtering higher-level, common Internet traffic—the network appliances should take care of that—but it does need to filter the specific data

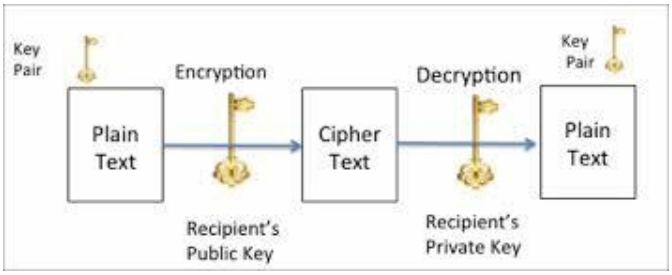
destined to terminate on that device in a way that makes optimal use of the limited computational resources available .

E. Updates and patches

Once the device is in operation, it will start receiving hot patches and software updates. Operators need to roll out patches, and devices need to authenticate them, in a way that does not consume bandwidth or impair the functional safety of the device. It's one thing when Microsoft sends updates to Windows users and ties up their laptops for 15 minutes. It's quite another when thousands of devices in the field are performing critical functions or services and are dependent on security patches to protect against the inevitable vulnerability that escapes into the wild . Software updates and security patches must be delivered in a way that conserves the limited bandwidth and intermittent connectivity of an embedded device and absolutely eliminates the possibility of compromising functional safety.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Cryptography is an electronic technique that is used to protect valuable data over transmission. Mainly cryptography is science to provide security to information. To protect our data by using different authentication scheme is the main objective of cryptography. When authentication of data is main consider that should be less cost than the value of original information. Elliptic curve cryptography is a public key cryptosystem developed by Neil Kobiltz and Victor Miller in 19th century [1] [2]. It is like RSA public key cryptography. The security strength of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP) [3]. ECC adopts scalar multiplication, which includes point doubling and adding operation which is computationally more efficient than RSA exponentiation. The complexity of ECC puts the attacker in difficulty to understand the ECC and to break the security key. The security level given by RSA with 1024 bit key can be achieved with 160 bit key by ECC. Hence it is well suited for resource constraint devices like smart cards, mobile devices, etc. [4]. It is also not an easy task to choose appropriate elliptic curve [5]. ECC standardization is crucial for achieving practical and efficient implementation. National Institute of Standards and Technology (NIST) provides specification for ECC which are considered safe for the use in cryptographic application [6]. Two main terms that is used for the cryptography technique are Encryption and Decryption. Encryption technique is used to send confidential data over communication .The process of encryption require two things (1) an encryption algorithm and (2) key.



A.Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, we have to select a number'd' within the range of 'n'. Using the following equation we can generate the public key

$$Q = d * P$$

d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve. 'Q' is the public key and'd' is the private key**.**

B.Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 – (n-1)]. Two cipher texts will be generated let it be **C1** and **C2**.

$$C1 = k*P$$

$$C2 = M + k*Q$$

C1 and C2 will be sent.

C.Decryption

To get back the message 'm' that was sent,

$$M = C2 – d * C1$$

M is the original message that we have send.

D.Proof

How do we get back the message?

$$M = C2 – d * C1$$

'M' can be represented as 'C2 – d * C1'

$$C2 – d * C1 = (M + k * Q) – d * (k * P)$$

(C2 = M + k * Q and C1 = k * P)

$$= M + k * d * P – d * k *P$$

(cancelling out k * d * P)

$$= M \text{ (Original Message)}$$

Thus the original message is regained.

V. SECURITY IMPLEMENTATION THROUGH ELLIPTIC CURVE

In IoT Elliptic curve cryptography were discovered by Neal Koblitz and Victor Miller in 1985. ECC is the most efficient public key encryption method based on the concept of elliptic curve which is used for enhanced cryptographic key. Generally, ECC is used to compare with the public key encryption methods like RSA and diffie-hellman key exchange problem. ECC helps to provide greatest security with low power computing devices. Some public key encryption methods like RSA, D-H key exchange and Digital Signature Algorithm (DSA) are very suitable for high power computation but when we go for IoT or cloud computing then there is a possibility that low power computing devices will not support such types of devices. Table 1 shows the comparison between various encryption algorithms.

Table 1: Comparison among different algorithm

Algorithm	**Key Exchange**	**Encryption /decryption**	**Digital signature**
Diffie Hellmen	Yes	Yes	No
DSA	No	No	Yes
RSA	Yes	Yes	Yes
ECC	yes	yes	Yes

From the above table, ECC proves to have a better performance when compared to all the other cryptographic techniques.

VI. CONCLUSION

In conclusion, the Internet of Things is closer to being implemented than the average person would think. Most of the necessary technological advances needed for it have already been made, and some manufacturers and agencies have already begun implementing a small-scale version of it. The main reasons why it has not truly been implemented is the impact it will have on the legal, ethical, security and social fields. Workers could potentially abuse it, hackers could potentially access it, corporations may not want to share their data, and individual people may not like the complete absence of privacy. For these reasons, the Internet of Things may very well be pushed back longer than it truly needs to be. By implementing Elliptic Curve Cryptography, the security of resources via internet can be improved. The privacy and the secured access of data can be maintained.

REFERENCES

[1] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, Vol.49, pp. 203-209, 1987. V.S. Miller, Use of Elliptic Curves in Cryptography, Advances in Cryptology

[2] Moncef Amara and Amar Siad, Elliptic Curve Cryptography and its Applications, 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), IEEE, 2011, pp. 47-250.

[3] Sandeep S. Kumar, Elliptc Curve Cryptography for Constrained Devices, PhD Thesis, Ruhur University Bochum, 2006.

[4] Ankita Soni and Nisheeth Saxena, Elliptic Curve Cryptography; An Efficient Approach for Encryption and Decryption of a Data Sequence, International Journal of Science and Research, Vol.2, No.5, 2013

[5] Mohsen Bafandehkar, Sharifah Md Yasin, Ramlan Mahmod, Zurina Mohd Hanapi, Comparison of ECC and RSA Algorithm in Resource Constraint Devices, Proceedings of the International Conference on IT Convergence and Security (ICITCS), IEEE, 2013, pp. 1-3.

[6] Butler, D. (2020) Computing: Everything, Everywhere. Nature, 440, 402-405. http://dx.doi.org/10.1038/440402a.

[7] Dodson, S. (2008) The Net Shapes upto Get Physical.Guardian. Gershenfeld, N., Krikorian, R. and Cohen, D. (2004) The Internet of Things. ScientificAmerican,291,7681.