IJRSET APRIL 2019 Volume 6, Issue 4 Pages: 31-36
ISSN 2394-739X
International Journal for Research in Science Engineering and Technology

ROBUST AND SECURE DATA DISSEMINATION BASED ON CRYPTOGRAPHIC SCHEME FOR INTERNET OF THINGS

[1] S. Sunanda Jency, [2] P. Nisha Priya
[1] PG Scholar, CSI College of Engineering, Ketti.
[2] Dept of Computer Science & Engineering, CSI College of Engineering, Ketti.

ABSTRACT: Io T integrated smart applications are growing rapidly to make everything smart.Researchers all over the world contribute enormously for the realm of smartness with the maxim of anytime anywhere paradigm. This growing technology is at the risk of security requirements such as authentication, confidentiality, integrity and non-repudiation.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.

Key terms: [Internet of Things, Cryptographic key generation.]

1. INTRODUCTION

The Internet of Things (IoT) is the internetworking 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 Thingsinvolves 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 buildingautomation, 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 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.

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

In this techniques, we present 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.And, we used Cryptographic key generation from fused features, here a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Finally, utilize encryption Scheme. This encryption provides image data security using cryptographic technique and Confidentiality of data is ensured by use of strong encryption.

2. LITERATURE REVIEW

This section provides the basic significance of security in IoT. It also provides thenumerous methodology to secure Transmissiontechniques.

A Survey on Security and Privacy Issues in Internet-of-Things Internet of Things (IoT) are everywhere in our daily life. They are used in our homes, in hospitals, deployed outside to control and report the changes in environment, prevent fires, and many more beneficial functionality. The survey consists of four segments. The first segment will explore the most relevant limitations of IoT devices and their solutions. The second one will present the classification of IoT attacks.

Mutual Authentication in IoT Systems using Physical Unclonable Functions-.IoT devices are usually small, low cost and have limited resources, which makes them vulnerable to physical, side channel, and cloning attacks. To address this issue, we present light-weight mutual authentication protocols for IoT systems based on Physical Unclonable Functions (PUFs). Protocols for two scenarios are presented, one when an IoT device and server wish to communicate and the other when two IoT devices want to establish a session. A security and performance analysis of the protocols shows that they are not only robust against different types of attacks.

A PUF-Based Paradigm for IoT Security- The security of different PUFs designs against these modelling attacks have been evaluated in multiple research efforts. To perform this evaluation, we implemented several strong delay based PUFs. The results showed that when factoring in the PUFs implementation area costs, these PUFs compare differently as some enhanced PUF designs turned out to have inferior efficiency compared to their simpler counterpart. We recognized the most effective design elements in the implemented PUFs. Based on the efficiency figures obtained, we recommended the optimal PUF design for the different security schemes used in constrained IoT devices.

Security Requirements Analysis for the IoT. -IoT is a very useful ecosystem that provides various services (e.g., amazon echo); however, at the same time, risk can be huge too. Collecting information to help people could lead serious information leakage, and if IoT is combined with critical control system security attackwould cause loss of lives. First, we propose basic security requirements of IoT by analyzing three basiccharacteristics (i.e., heterogeneity, resource constraint, dynamic environment). Then, we suggest six key elements of IoT and analyse their security issues for overall security requirements. Inaddition, we evaluate several IoT security requirement researches

Achieving Trust in Cloud Computing Using Secure Data Provenance- This paper presents the provenance description and challenges in providing security assurances in the Cloud. The paper also proposes a novel trust model for data provenance in cloud computing. The model will be used for securing the transaction process of storing and accessing the data provenance. The paper describes in detail the flow process of the model to achieve a high level of trust in cloud services.

3. METHODOLOGIES

In this techniques, we present 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. And, we used Cryptographic key generation from fused features, here a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Finally, utilize encryption Scheme. This encryption provides image data security using cryptographic technique and Confidentiality of data is ensured by use of strong encryption.

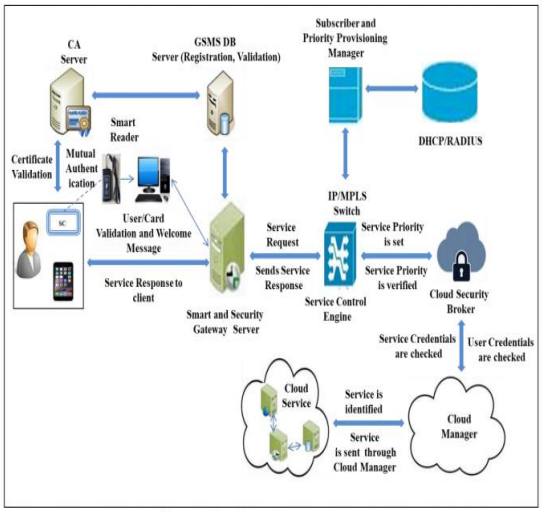


Figure 1.1 Block Diagram of Proposed work

3.1 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.

3.2 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.

3.3 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.

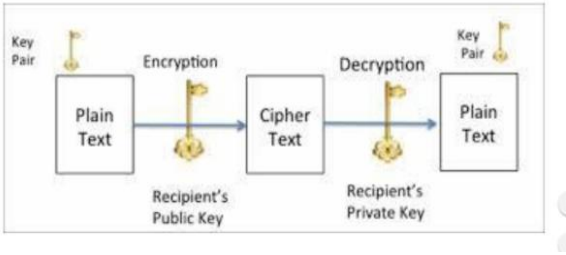
4. ELLIPTIC CURVE CRYPTOGRAPHY

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. It is like RSA public key cryptography.

The security strength of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP). 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. It is also not an easy task to choose appropriate elliptic curve. 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. Two main terms that is used for the cryptography technique are Encryption and Decryption. Encryption technique is used to send confidential data over communication.



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.

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.

Decryption

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

M = C2 – d * C1

M is the original message that we have send.

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)

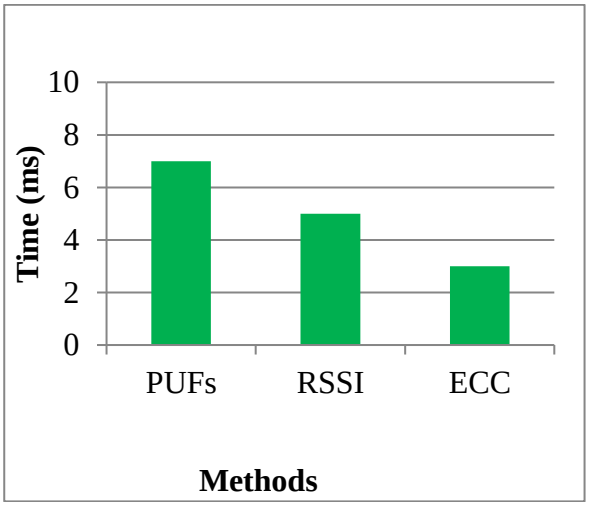
= M (Original Message)

Thus the original message is regained.

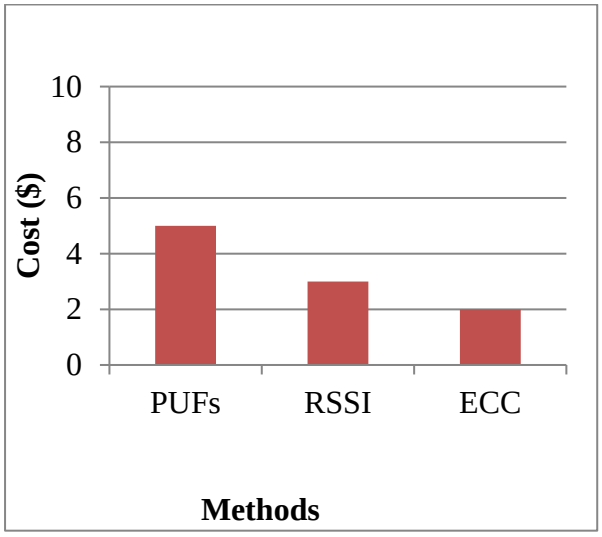
5. RESULTS

In this section, the overall setup of our experiment and the results obtained from it is described to validate the proposed ECC. In our experiment, RSSI, PUFs are chosen as test cases.

5.1 Communication Time



5.2 Communication Cost



CONCLUSION

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.

The results prove, with all the security mechanisms incorporated at card level in the proposed architecture, the response time for varied applications is less and highly secured. The future work is to develop the architectural level security mechanism for IoT Cloud integrated smart application architecture.

REFERENCES

[1]. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, ‘‘A survey on security and privacy issues in Internet-of-Things,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1250–1258, Oct. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7902207/

[2]. S. Satpathy, S. Mathew, V. Suresh, and R. Krishnamurthy, ‘‘Ultra-low energy security circuits for iot applications,’’ in Proc. IEEE 34th Int. Conf. Comput. Design (ICCD), Oct. 2016, pp. 682–685.

[3]. M. N. Aman, K. C. Chua, and B. Sikdar, ‘‘Mutual authentication in IoT systems using physical unclonable functions,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1327–1340, Oct. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7924368/

[4]. T. Idriss, H. Idriss, and M. Bayoumi, ‘‘A puf-based paradigm for IoT security,’’ in Proc. IEEE 3rd World Forum Internet Things (WF-IoT), Dec. 2016, pp. 700–705.

[5]. S.-R. Oh and Y.-G. Kim, ‘‘Security requirements analysis for the IoT,’’ in Proc. Int. Conf. Platform Technol. Service (PlatCon), Feb. 2017, pp. 1–6.

[6]. M. I. M. Saad, K. A. Jalil, and M. Manaf, ‘‘Achieving trust in cloud computing using secure data provenance,’’ in Proc. IEEE Conf. Open Syst. (ICOS), Oct. 2014, pp. 84–88.

[7]. S. T. Ali, V. Sivaraman, D. Ostry, G. Tsudik, and S. Jha, ‘‘Securing first-hop data provenance for bodyworn devices using wireless link fingerprints,’’ IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2193–2204, Dec. 2014.

[8]. K. Zhang, X. Liang, R. Lu, and X. Shen, ‘‘Sybil attacks and their defenses in the Internet of Things,’’ IEEE Internet Things J., vol. 1,no. 5, pp. 372–383, Oct. 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6868197/

[9]. G. Kecskemeti, G. Casale, D. N. Jha, J. Lyon, and R. Ranjan, ‘‘Modelling and simulation challenges in Internet of Things,’’ IEEE Cloud Comput., vol. 4, no. 1, pp. 62–69, Jan./Feb. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7879128/

[10]. J. Pacheco and S. Hariri, ‘‘IoT security framework for smart Cyber infrastructures,’’ in Proc. IEEE Int. Workshops Found. Appl. Self Syst., Sep. 2016, pp. 242–247.

[11]. Z. Bohan, W. Xu, Z. Kaili, and Z. Xueyuan, ‘‘Encryption node design in Internet of Things based on fingerprint features and cc2530,’’ in Proc. IEEE Int. Conf. Green Comput. Commun., Internet

Things, IEEE Cyber, Phys. Soc. Comput., Aug. 2013, pp. 1454–1457.
[12]. J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, ‘‘A lightweight authentication protocol for Internet of Things,’’ in Proc. Int. Symp. Next-Gener. Electron. (ISNE), May 2014, pp. 1–2.
[13]. M. N. Aman, K. C. Chua, and B. Sikdar, ‘‘Secure data provenance for the Internet of Things,’’ in Proc. 3rd ACM Int. Workshop IoT Privacy, Trust, Secur., 2017, pp. 11–14. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3055245.3055255
[14]. J. Qian, H. Xu, and P. Li, ‘‘A novel secure architecture for the Internet of Things,’’ in Proc. Int. Conf. Intell. Netw. Collaborative Syst. (INCoS), Sep. 2016, pp. 398–401. [Online]. Available: http://ieeexplore.ieee.org/document/7695208/
[15]. Y. Xie and D. Wang, ‘‘An item-level access control framework for intersystem security in the Internet of Things,’’ Appl. Mech. Mater., vols. 548– 549, pp. 1430–1432, Apr. 2014. [Online]. Available: https://www.scientific.net/AMM.548-549.1430
[16]. Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, ‘‘LACS: A lightweight label-based access control scheme in IoT-based 5G caching context,’’ IEEE Access, vol. 5, pp. 4018–4027, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7872420/
[17]. Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, ‘‘Social big-data-based content dissemination in Internet of vehicles,’’ IEEE Trans. Ind. Inform., vol. 14, no. 2, pp. 768–777, Feb. 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7995077/
[18]. Z. Zhou, K. Ota, M. Dong, and C. Xu, ‘‘Energy-efficient matching for resource allocation in D2D enabled cellular networks,’’ IEEE Trans. Veh. Technol., vol. 66, no. 6, pp. 5256–5268, Jun. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7585029/
[19]. Z. Zhou, H. Yu, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, ‘‘Dependable content distribution in D2D-based cooperative vehicular networks: A big data-integrated coalition game approach,’’ IEEE Trans. Intell. Transp. Syst., vol. 19, no. 3, pp. 953–964, Mar. 2018. [Online]. Available: http://ieeexplore.ieee.org/document/8264740/
[20]. Micaz-Wireless Measurement System, Crossbow Technol., Milpitas, CA, USA, Apr. 2007.
[21]. C.-L. Wu and C.-H. Hu, ‘‘Computational complexity theoretical analyses on cryptographic algorithms for computer security application,’’ in Proc. IEEE 3rd Int. Conf. Innov. Bio-Inspired Comput. Appl. (IBICA), Sep. 2012, pp. 307–311.