IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 10 (October. 2018), ||V (IV) || PP 22-28

A Survey on Certificate-Less Public Key Encryption for Authentication in a Smart IoT-Based LoRaWAN

Srishti Tiwari[1], Dr. Hiren B. Patel[2],Dr. Bela Shrimali[3]
Computer Engineering Department, LDRP
Institute of Technology & Research, Gandhinagar, India
Corresponding Author: Srishti Tiwari

Abstract: Key management and authentication are the two key components to make sure that the entities involved in communication process in Internet of Things (IoT) operate securely. Due to architectural as well as operational differences between a conventional network and an IoT network, protocols and techniques used in a traditional key management are not well-suited for IoT. Mutual authentication is one of the critical task to achieve in an IoT network as the entities are spread across wide area with limited memory capacity and battery power. This can be achieved with the implementation of certificate-less public-key cryptography (CL-PKC) in IoT. Many recent researches have been carried out about Long Range (LoRa) and Long Range Wide Area Network (LoRaWAN) which are newly developed communication architectures focusing on communication over long-distance constrained with low-power factors and thus can be used in an IoT environment with utter efficiency and accuracy. Due to the nature of operations in Long Range Wide Area Network, the authentication method should be light-weight and easy to execute without adding much over-head to the network, which is why a certificate-less public key encryption for mutual authentication can be used. This survey aims to build a ground for research towards authentication algorithm with the certificate-less public-key cryptography (CL-PKC) technique in a smart IoT-based LoRaWAN.

Keywords: IoT, certificate, certificate-less, key, attacks, security, long, range, network, key-generator, battery

---

Date of Submission: 16-10-2018 Date of acceptance: 31-10-2018

I. INTRODUCTION

R. Minerva et.al. [1] definesIoT as- A network of devices which are embedded with sensors and are connected to the Internet for communicating with each other.

Internet of Things (IoT) is a new and swiftly budding technology that finds its applications in various field of wireless communications. IoT defines a plethora of connecting smart objects and devices that find the applications in the day-to-day life of an individual. With the introduction of IoT, the concept of smart world is an integral part of many wide ranges of applications, like wearable devices- smart watches, smart home, e-health applications- EHR, smart cities, etc. But, because of the nature of the IoT network raises the question of a secure communication in IoT – including authentication of heterogeneous nodes which are part of the network. It is one of the many open serious challenges which needs a serious attention and work to be done for deployment of such a large-scale as well as a commercial networks [2].

In any authentication method, key management plays a very critical role in achieving the security requirements in a given communication system. In an IoT network, authentication allows the system to communicate using the shared cryptographic keys securely between a node in an environment with limited resources and a remote environment operating on an internet-based network. Further, the use of mutual authentication between two communicating entities ensures to avoid any possibility of non-repudiation attack to be launched by any compromised or hacked nodes within or out of the network [2].

Another key criteria to be considered for IoT network is the battery power and coverage range – which brings a discussion out LPWANs and LoRaWANs. Low-Power Wide Area Networks (aka LPWANs) is one of the developing technologies in the IoT that supports long-distance wireless communication constrained with low-power supply. LPWANs are used to send and receive small packets of information at infrequent intervals. Its capacity to send small packets make it insufficient for large packets. As per LoRa Alliances documentation [4] - LoRa is a solution for physical layer, designed and developed by Semtech that fulfills the LPWAN requirements by using chirp spreading spectrum modulation technique. As per the LoRaWAN specification [5], it provides a coverage across 15 km area and a battery lifetime of ten years [6]. Because of high battery lifetime and wide coverage, LoRa and LoRaWAN are most suitable network environment for battery constrained communication in an IoT environment [3].

LoRaWAN architecture supports star network topology. It involves end node and network server communicating with each other, where the NS is acting like a hub connecting various small networks [4]. Mikhaylov et al. [7] propose a network-assisted D2D protocol which proves that a device-to-device (D2D) communication is applicable in a LoRaWAN environment by implementing the direct communication channel between two LoRaWAN end nodes with the help of the network server (NS) which assists the End-Devices (ED) to dynamically reconfigure its parameters before the transmission can be initiated [3].

Due to the nature of operations in LoRaWAN, the authentication method should be light-weighted and easy to execute without adding much over-head to the network, which is why a certificate-less public key encryption for mutual authentication can be used.

This paper is regularized as follows. Section II presents section an overview of overview of LoRaWAN in IoT. III presents advantages of the LoRaWAN network. Section IV presents related works for CL-PKC and LoRaWAN which form the basis of this survey and aid the decision of incorporating the CL-PKC into IoT in a LoRaWAN based system. Section V presents certificate-less public key cryptography and it's functioning in detail, followed by the advantages in section VI. Finally, section VII present conclusion and future works.

II. AN OVERVIEW OF LoRaWAN

LoRaWAN [4] defines a communication protocol and network system architecture while LoRa at the physical layer, enables the link to communication over a long-range. The battery life of a node, the network capacity, the QoS parameters, the security status, and the variety of applications supported by the network are identified based on the protocol and network architecture [4].

LoRaWAN operates at the media access control (MAC) layer of the WAN. It allows low-powered devices to communicate efficiently with internet applications over long range of wireless connections. Compared to the OSI model, LoRaWAN maps to the second and third layer of the model. In the industrial, scientific and medical (ISM) radio bands, LoRaWAN is implemented on the FSK modulation. [8].

I. Network Architecture

Mesh network is the most common network topology used by almost all existing deployed networks. Mesh topology connects each node in the system with every other node to increase the communication range and the coverage area of the network. It clearly increases the communication range but it also adds some degree of complexity within the network - as the network is wide spread and there are numerous nodes communicating simultaneously -, reduces network ability to handle load and battery life of the nodes as they are receiving and forwarding the packets across the network over a long-range to achieve maximum coverage [4].

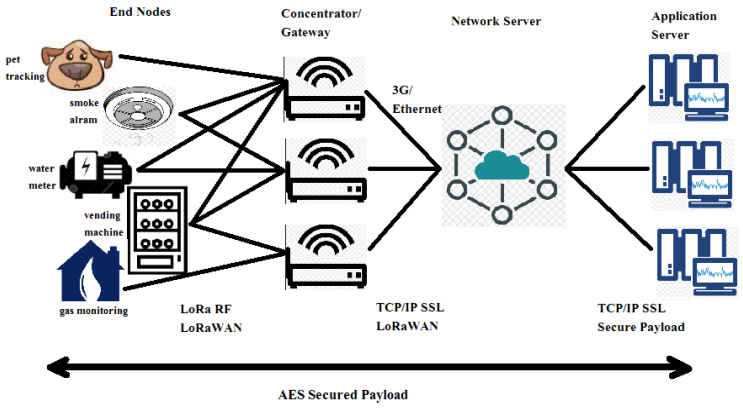

Figure 1: LoRa System [4]

In a LoRaWAN network, internal nodes don't have association with a particular gateway but the transmitted information is received by multiple gateways. Each of these gateways then forward the received packet to the cloud network via the backbone network (cellular network, Wi-Fi, etc). The increased network load is managed by the intelligence and complexity that helps to filter the redundant packets received, perform reuired security checks, send acknowledgments for the received packets through the gateways, and twick the data transmission rate as required, etc. If a node is mobile or moving there is no handover needed from gateway to gateway, which can be considered as a criteria to enable asset tracking applications–a major target application vertical for IoT [4].

I. Battery Life

Nodes in the LoRaWAN are asynchronous as they communicate only when there is any data to send depending on the event trigger or the scheduled time. This is same as the Aloha Method where communication takes place on the availability of the data packet with the node. In such a network, the node has to 'wake up' periodically from its sleep state to check for the data availability and synchronize with the network. To perform this synchronization, node has to loose significant power and battery life. Based on the comparison study done by the GSMA, it's concluded that LoRaWAN is 3 to 5 times better when compared with all other available technologies. [4].

I. Network Capacity

To increase the feasibility of the long range network implemented with a star topology like LoRaWAN, the gateway -which collects all the data and enables the communication, must have very high capability to handle the overhead of the high volume of data flowing in the network. One way to achieve high capability in the network is by implementing of the adaptive data rate - to modulate the data transmission rate and multiple channel- multi-modem transceiver for the gateway so that simultaneous data can be sent or received. [4].

Few of the factors that affect the network capacity are the number of simultaneous data links to synchronize, data transmission rate, payload size, and the transmission method. Signals in LoRa are orthogonal - since it uses spread-spectrum based modulation, which allows the utilization of the different spreading factors. This spreading factor controls the data transmission rate. This further enables the gateway to use different data rate to handle data packets on the same channel at the same time. The nodes near to the gateway will get high data rate so the communication can be completed as fast as possible. [4].

If the higher data rate is used, the time spent by the packet on air is reduced so that the other nodes can use the free channel for data transmission. With the use of adaptive data rate, the battery lifetime is increased. For the adaptive data rate to work, sufficient capability is needed for both up and downlink channels. This feature make LoRaWAN to have higher capacity and increases the scalability of the network as well. [4].

Because of increased scalability, such a network can be implemented with minimal infrastructure and depending of the required capacity, the gateways can be added which will help to control the data rates, thus reduce the amount of the overlap between the other gateways in the network, and increasing the network capacity 6-8x times more. Compared to LoRaWAN, other LPWAN techniques limit downlink capacity or implement different rates for downlink and uplink channels thus resulting into a reduced scalability [4].

II. Device Classes

Depending on the different requirements, end-devices can be used for different applications. Based on the application used, LoRaWAN provides different devices to use- which are categorized in different classes. The devices classes are defined considering the network downlink communication versus the battery lifetime of the application it can be used for. Downlink communication delay is an important factor in a constrained application. [4].

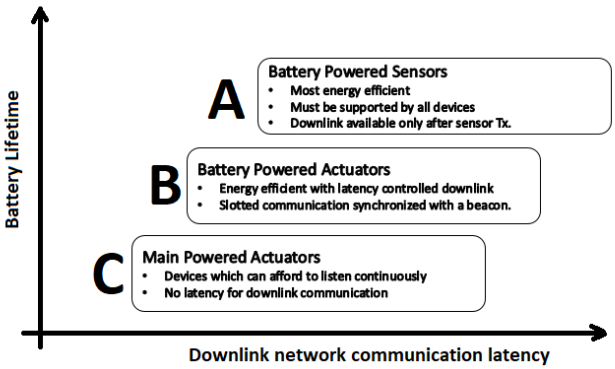

Figure 2: Device categories in LoRaWAN [4]

a. Class A devices (Bi-directional end-devices):

Class A devices are idle for two-way communication where after each node's uplink transmission window there is are two short receive windows for downlink communication. Depending on the communication requirements, the transmission slot can be scheduled by the node at random times- same as in ALOHA transmission [4].

Class A devices operations are used for low power systems and applications where downlink communication need to be scheduled soon as after the node completes the uplink transmission. Since the downlink communication is followed by uplink communication, the node has to spend some time waiting for the downlink window to start before it can start communicating. [4].

b. Class B devices (Bi-directional end-devices with scheduled receive slots):

Class B devices also supports the random receive windows, same as class A devices, however along with this it also has an extra receive window at each scheduled time. Before the initiation of the each receive window, the node receives a time-synchronized token from the gateway. The receiving of the beacon makes the node to be ready to listen when the receive window starts [4].

c. Class C (Bi-directional end-devices with maximal receive slots):

Devices in this class have closed transmission windows like other devices but it they have open receive windows- i.e., it is ready to receive data anytime the other node or gateway has some data for the node [4].

III. Security

Like all other architectures, security is needed in LPWAN as well. LoRaWAN implements security at two different layers: network layer and application layer. Security implementation at the network layer ensures that only authentic node is part of the network. Application security ensures that the network entities or nodes don't have access to the end-user applications or the data until properly authenticated. To achieve this security, AES encryption is used for key exchange [4].

III. ADVANTAGES OF LoRaWAN

With the advantages of supporting low battery and longer active lifetime- LoRaWAN has following advantages [4]:

IV. **Long Range**:

a. Greater than cellular
b. Deep indoor coverage
c. Star topology

V. Maximum Lifetime:

a. Low power optimized
b. 10-20yr lifetime
c. >10x vs cellular M2M

VI. Multi-usage:

a. High capacity
b. Multi-tenant
c. Public network

VII. Low Cost:

a. Minimal infrastructure
b. Low cost end node
c. Open SW

IV. RELATED WORK

Authentication plays a key role in initiating the connection setup process for setting up a communication channel in aIoT environment where the end nodes are always on the move and storage and power are limited. The related work presented here focus on the problems identified in the traditional approaches which directed towards the introduction of a certificate-less public key authentication. The research works specific to IoTauthentication in a LoRaWAN infrastructure are also studied and summarized in this section.

D. Q. Bala et.al. [2] focuses on the problem of mutual authentication for a node in a resource constrained smart environment and its challenges in the communication with the remote end-user for authentication.

J. Kim et.al. [3] discusses communication between devices with reduced battery consumption. It points out that the in-built security within the LoRaWAN is not effective which means there is a need for a better alternative for a D2D communication.

S. Sciancalepore et.al. [9] addresses the problem of computational complexity involved ina Public Key Cryptography for a sensor that needs to communicate with the other nodes and reduce the airtime consumption required for message and certificate exchange needed for authentication purpose.

M. Wazid et.al. [10] explains that a Hierarchical IoT Network (HIoTNs) needs an authentication method where a user can directly use the real-time data transmitted by the other nodes to fulfill a generic application in IoT networking environment.

Z. Mahmood et.al. [11] puts talks about the mobile devices and the universal connectivity used by the devices in the IoT environment. Hence, the availability of a secure key management method is obligatory to have confidentiality of the information interchange taking place.

S. Al-Riyami et.al. [12] talks about the drawbacks of the traditional public key authentication methods which compromise the overall performance and security of the network- the overall of overhead on the network for maintaining a Certificate Authority (CA) and the high risk of key-escrow problem. It also sheds light on how certificate-less public key cryptography (CL-PKC) is an alternative for the aforementioned limitations.

IV. DISCUSSION ON CERTICATE-LESS PUBLIC KEY CRYPTOGRAPHY TECHNIQUE

The basic functioning of the Certificate-less Public key Encryption can be summarized as:

A CL-PKC system uses a Trusted-Third Party (TTP) called the key generating center (KGC). In contrast to ID-PKC, the KGC used here doesn't have access to the private keys of the nodes communicating. Instead, in this process, KGC uses the identity IDA and master shared key A to calculate the partial private key (DA) for the given node A. The KGC transfers the partial private key confidentially and authentically to the node A. Once the node A gets the partial private key, it combines it with the secret information to get the private key SA. Since A is generating its own private key, it's not known to KGC. [12].

After the private key is calculated, node A combines the secret information with the global parameters of the KGC to calculate the public key PA. Both SA and PA are independently on each other which means the order of calculation doesn't matter here and only the secret information with node A is needed to calculate both keys. Since the key calculation is not dependent on the identity, it makes the system no more ID-based. [12].

Once A's public key is calculated, it is shared with the other nodes in the network by sending it as a part of the transmitted message or by making it available in a public directory. Once the public key is shared, there is no need for any additional security needed- no need to maintain certificate for A's keys. To send a message to A or for verifying signatures, node B can use the PA and IDA. [12].

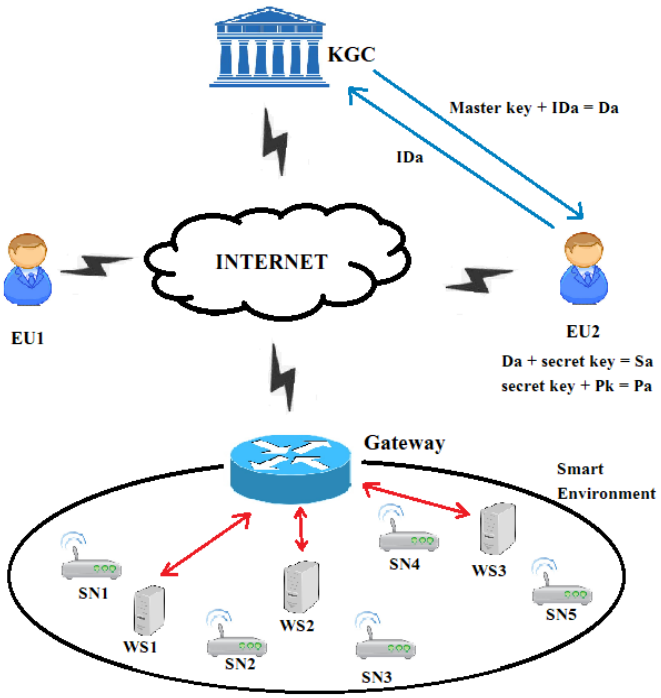

Figure 3: Certificate-less Authentication [2]

As the CL-PKC architecture allows the network to function in an efficient way without having to manage a dedicated CA, instead KGC are assigned dynamically. Further since there is not dedicated node to manage and maintain the keys, the key-escrow problem doesn't exist.

D. Q. Bala et.al [2] proposes theCL-PKC protocol which eliminates the need of a certificate authority by using the CL-PKC technique. It uses the idea of bilinear Pairing to define Certificate-less Public-Key Encryption (CL-PKE) and Certificate-less Public-Key Signature (CL-PKS) that focusses on tackling the problem of authentication. The author also suggest to enhance the proposed work for wide network creation/clustering based on neural network.

J. Kim et.al. [3] provides a secure link establishment scheme for authentication and protection in the LoRaWAN D2D communication. The solution proposed is focused on LoRaWAN Network with Security implementation in a cellular network.

S. Sciancalepore et.al. [9] proposes a Key Management Protocol which makes uses of the pre-defined certificates with Elliptic Curve Diffie-Hellman for key exchange to carry out the authentication and key derivation which is using the concept of CA to manage the authentication process. The proposed work is implemented on OpenWSN protocol stack (openwsn.atlassian.net) which is installed on the OpenMote-CC2538 constrained platform (Cooja) for simulation testing. It also suggests future work to be done on implementation using Certificate-less public key and increase the airtime saving.

M. Wazid et.al. [10] proposes the design for a new secure as well as lightweight scheme using three-factor remote user authentication for HIoTNs called the User Authenticated Key Management Protocol (UAKMP). It's a generic authentication key management protocol which uses the concepts of user authenticated key management protocol, sensing node registration, user as well as sensing node secrecy implemented on AVISPA tool for simulation.

Z. Mahmood et.al. [11] tackles the problem of key management for multi-key by proposing a Distributed Multiparty Keying (DMK) scheme which uses chaotic maps to provide one-way hashing and Chebyshev polynomial (CP) for establishing a common multi-party key. The proposed system is tested on NS 2.35 with 3-4 nodes and can be enhanced for N-ary node implementation for an IoT network.

V. ADVANTAGES OF CL-PKC

In a traditional Public Key Infrastructure (PKI), authentication is achieved by the use of certificates managed by a Certification Authority (CA) [13]. Gutmann et.al. [14] lists down the problems of PKI technology are the issues, among which are the issues due to management in the certificates, including assignment, revocation, storage and distribution cost incurred due to certificate verification. [15].

In ID-PKC, the node's identity is used to calculate its public key, for example, an IP address or an e-mail address associated to the node. Private Key Generator (PKG) gets the private keys by a trusted third party (TTP) [16].

The origin of public keys in ID-PKC removes the necessity of managing the certificates and overcomes various other problem caused due to it. On the other hand, with the dependency on a PKG to calculate the private keys certainly presents key escrow within an ID-PKC systems. Equally concerning is that the PKG could fake as any other entity in an ID-PKC scheme, by using its signatures, so ID-PKC cannot conceal non-repudiation same as the traditional PKI can offer [16].

Key escrow (also known as a "fair" cryptosystem) is an scenario in which the keys that are needed to decrypt encrypted data are stored in a central location -'escrow'- to be used at the time of need, when in any particular situation, an authorized third party may gain access to those keys [17]. Since all the keys are stored at a common location, the only step in breaching the security is getting access to the CA- hence this scenario is called *key escrow problem*.

The use of multiple PKGs and threshold techniques helps to overcome the key escrow problem up to certain extent, but it adds the need of an extra communication and stronger infrastructure. Moreover, in a situation if the PKG's master key is compromised, it can be much more of a concern in the ID-PKC system, and similarly the negotiation of a CA's validation key in a traditional PKI can compromise security [12].

As compared to ID-PKC, the CL-PKC infrastructure is lightweight. This is because there is no need to have additional resources for the assignment or management of the certificates, which is there in ID-PKC. This is the key feature that makes CL-PKC as an idle option for a low-data rate and low-battery applications, for example, mobile security applications, which cannot have long battery life and managing certificates in such circumstances in a huge limitation. [15].

Based on the recent studies, there have been new certificate system which takes short signatures in to use [18] which can be used in ID-PKC to overcome to limitations of the certificate management thus resulting into a lightweight PKI but because private key is in sole possession of the node to which it belongs, CL-PKC can truly be a better solution to the problem of non-repudiation faced in ID-PKC. [15].

Previous work helps us conclude that CL-PKC can overcome the two major drawbacks of the traditional PKI as well as the ID-PKC techniques- Managing CA or PKG and key escrow problem. This advantage makes it a light weight protocol for a complicated network like a LoRaWAN. Along with this, it also

allows less overhead and supports non-repudiation as well which is why it is a good option for a LoRaWAN architecture.

VI. CONCLUSION

Authentication is the key role to play in the connection setup process for the initiating a communication channel in an IoT environment where the end nodes are always on the move and storage and power are limited. In this paper, we have analyzed the working of the CL-PKC algorithm and its advantages. We also studied how implementing CL-PKC can be beneficial in a LoRaWAN architecture. The study of previous papers have highlighted that a mutual authentication algorithm is needed for a LoRaWAN in an IoT network which can be simulated in NS2 or Cooja simulators. In addition, future work can involve enhancing the efficiency further by incorporating the hierarchical CL-PKC and proxy decryption functionality to reduce the overall time in key exchange and authentication.

REFERENCES

[1] Roberto Minerva, Abyi Biru and Domenico Rotondi, "Towards a definition of the Internet of Things (IoT)", IEEE Internet Initiative, pp.10, 27 May, 2015.

[2] D. Q. Bala, S. Maity and S. K. Jena, "Mutual authentication for IoT smart environment using certificate-less public key cryptography," 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS), Chennai, 2017, pp. 29-34.

[3] J. Kim and J. Song, "A Secure Device-to-Device Link Establishment Scheme for LoRaWAN," in IEEE Sensors Journal, vol. 18, no. 5, pp. 2153-2160, 1 March, 2018.

[4] "A technical overview of LoRa and LoRaWAN," LoRa Alliance, San Ramon, CA, USA, Tech. Rep., Nov. 2015. [Online]. Available: https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

[5] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "LoRaWAN specification," LoRa Alliance, San Ramon, CA, USA, Tech. Rep. Version 1.0.2, Jul. 2016.

[6] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," IEEE Commun. Surveys Tuts., vol. 9, no. 2, pp. 855–873, 2nd Quart., 2017

[7] K. Mikhaylov, J. Petäjäjärvi, J. Haapola, and A. Pouttu, "D2D communications in LoRaWAN low power wide area network: From idea to empirical validation," in Proc. IEEE Int. Conf. Commun. Workshops, Paris, France, May 2017, pp. 737–742.

[8] [Online] *https://www.thethingsnetwork.org/docs/lorawan/*-"LoRaWAN"

[9] S. Sciancalepore, G. Piro, G. Boggia and G. Bianchi, "Public Key Authentication and Key Agreement in IoT Devices With Minimal Airtime Consumption," in IEEE Embedded Systems Letters, vol. 9, no. 1, pp. 1-4, March 2017.

[10] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 269-282, Feb. 2018.

[11] Z. Mahmood, A. Ullah and H. Ning, "Distributed Multiparty Key Management for Efficient Authentication in the Internet of Things," in IEEE Access, vol. 6, pp. 29460-29473, 2018.

[12] Al-Riyami S.S., Paterson K.G. (2003) Certificateless Public Key Cryptography. In: Laih CS. (eds) Advances in Cryptology - ASIACRYPT 2003. ASIACRYPT 2003. Lecture Notes in Computer Science, vol 2894. Springer, Berlin, Heidelberg.

[13] C. Adams and S. Lloyd. Understanding Public-Key Infrastructure { Concepts, Standards, and Deployment Considerations. Macmillan Technical Publishing, Indianapolis, USA, 1999.

[14] P. Gutmann. PKI: It's not dead, just resting. IEEE Computer, 35(8):41{49, 2002.

[15] J. Dankers, T. Garefalakis, R. Schaelhofer, and T. Wright. Public key infrastructure in mobile systems. IEE Electronics and Commucation Engineering Journal, 14(5):180{190,2002.

[16] A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology { CRYPTO'84, volume 196 of LNCS, pages 47{53. Springer-Verlag, 1984.

[17] [Online]*https://www.cia.gov/library/readingroom/docs/DOC_0000239468/DOC_0000239468.pdf* "Encryption Policy: Memo for the Vice President"

[18] D. Boneh, H. Shacham, and B. Lynn. Short signatures from the Weil pairing. In C. Boyd, editor, Advances in Cryptology { ASIACRYPT 2001, volume 2248 of LNCS, pages 514{ 532. Springer-Verlag, 2001.

Srishti Tiwari. " A Survey on Certificate-Less Public Key Encryption for Authentication in a Smart IoT-Based LoRaWAN." IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 10, 2018, pp. 22-28.