Intelligent Security Framework for IoT Devices

Cryptography based End -To- End security Architecture

S. Sridhar
Research Scholar, Dept of IT,
Alpha College of Engineering,
Chennai, India.
sri_tag@yahoo.co.in

Dr. S. Smys
Dept.of ECE,
RVS Technical Campus,
Coimbatore, India.
smys375@gmail.com

***Abstract*— Internet of Thing (IoT) provide services by linking the different platform devices. They have the limitation in providing intelligent service. The IoT devices are heterogeneous which includes wireless sensors to less resource constrained devices. These devices are prone to hardware/software and network attacks. If not properly secured, it may lead to security issues like privacy and confidentiality. To resolve the above problem, an Intelligent Security Framework for IoT Devices is proposed in this paper. The proposed method is made up of (1) the light weight Asymmetric cryptography for securing the End-To-End devices which protects the IoT service gateway and the low power sensor nodes and (2) implements Lattice-based cryptography for securing the Broker devices/Gateway and the cloud services. The proposed architecture implements Asymmetric Key Encryption to share session key between the nodes and then uses this session key for message transfer This protects the system from Distributed Denial of Service Attacks, eavesdropping and Quantum algorithm attacks. The proposed protocol uses the unique Device ID of the sensors to generate key pair to establish mutual authentication between Devices and Services. Finally, the Mutual authentication mechanism is implemented in the gateway.**

Keywords—IoT Security; Internet of Thing; cryptography;quantum attack;authentication;Asymmetric Encryption;Symmetric Encryption; cryptography;DDOS.

I. INTRODUCTION

In [3] they proposed a secure IoT framework to ensure an End-To-End security from an IoT application to IoT devices. The combination of cloud computing and IoT enables ubiquitous sensing services and powerful processing of sensing data streams [13]. The IoT typically has a three-layer architecture consisting of Perception (sensing Device Domain), Network (networking Domain), and Application layers (Cloud Domain). Each IoT layer is susceptible to either active or passive threats and attacks, that can originate from external sources or internal network. The Internet of Things (IoT) is moving from a centralized structure to a complex network of decentralized smart devices. In [12], [14] IoT devices and services are susceptible to Denial of Service attacks (DoS). Eavesdropper collusion is a significant threat to wireless communication security. Security must be addressed throughout the device lifecycle, from the initial design to the operational environment. the tough challenges of the Internet of Things solutions face are how to get extra bit of battery life for the innovative IoT solutions and the power constraints in communication. First, we propose the Intelligent Security Framework for End -To- End security [16]. Second, the paper gives an overview of the cryptography method associated with.

A. Symmetric and Asymmetric Key Encryption

Asymmetric encryption systems have high overhead , they are not usable to provide full-time, real-world security.the public key is used for encryption and the private key for decryption during the initial handshake process, which allows the two parties to confidentially set up and exchange a newly-created “shared key”. The shared keys are used for secure communication and it is valid for its current session .This reduces the IoT nodes and Devices gateways key transfer overhead.

The rest of the paper is organized as follows. Section II reviewed the previous work in in literature. Section III specified the proposed protocol. Finally, Sect. IV presented the conclusion.

II. REVIEW OF PREVIOUS WORK

The interconnectivity of different types of IoT devices and heterogeneity lead to threat to data. In this survey, we explore the IoT security and the corresponding Authentication protocols in general with their vulnerabilities to attacks during routing.

B. The IoT Broker Registration Protocol [1]

In [1], they have proposed the intelligent IoT common service platform and IoT Broker registration.in this model The IoT Broker registers the new device using device model, location, IP address. After creating the device object, it is saved in the generic data model which is a database. The device management sends a request for device authorization to the authorization function in the security framework. The authorization function creates the device token and sends it to the device management and then registration gets completed.

C. Routing Protocol and its security features [2]

In this paper, they have classified the various routing protocols and the threat to them. The protocols are classified based on key management, cryptography and trust management secure IoT framework to ensure an End-To-End security.

D. End -To- End security based Protocol [3]

In this paper, they have proposed the secure environment using IoT device, IoTbroker, and IoT application. The Constrained Application Protocol (CoAP) and Message Queue Telemetry Transport (MQTT) Protocols are used to communicate between the IoT broker and the IoT devices. The Advanced Encryption Standard (AES) and Attribute-Based Encryption (ABE) are used to create cipher text.

E. Data management and deduplication in cloud computing [4]

In this paper, they have proposed Attribute-Based Encryption (ABE) to deduplicate encrypted data stored and support secure data access control. the Data users (IDs) are used to create public key. The generated key is used to authenticate device to the IoT broker.

F. VM-replication-based Protocol [5]

In this paper, they have proposed the use of VM replication to improve the survivability of mission-critical applications in cloud systems through a new multi-level VM replication approach

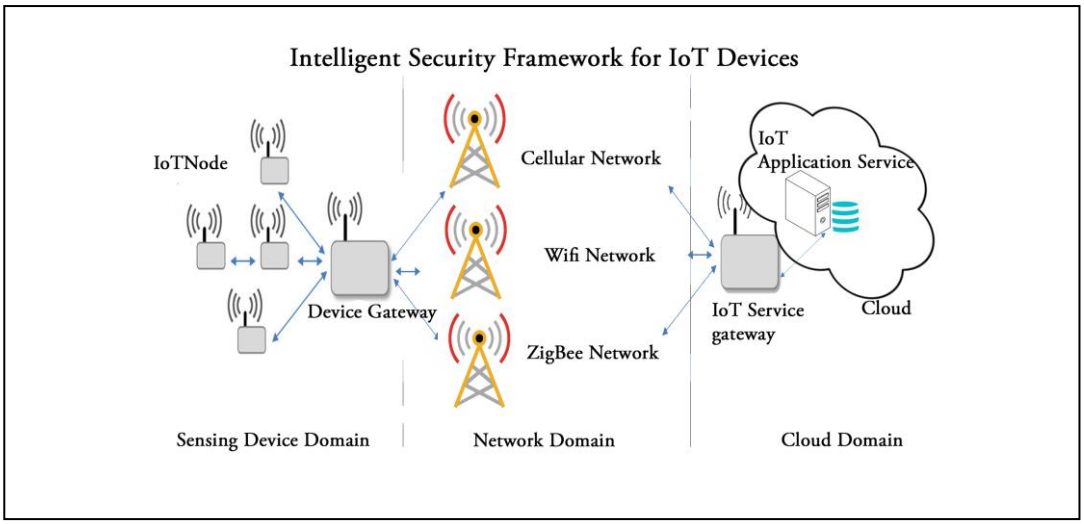

Fig 1: Intelligent Security Framework for IoT Devices

G. Trusted-third-party-based key exchange protocol [6]

In this paper, they have proposed the use of trusted third party to generate key.it generates 40 session keys simultaneously .it resists the known-key, impersonation, replay, eavesdropping and forgery attacks.

H. Machine-to-Machine (M2M) key exchange protocol [7]

In this paper, they have surveyed Machine-to-Machine research and more the threats that Machine-to-Machine communications have to face.

I. A Tutorial Introduction [8]

In this paper, they have We provided a tutorial introduction to the IoT ecosystem. They have deep dive into two specific research challenges in IoT, security and energy efficiency.

J. Trusted-third-party-based key exchange protocol [10]

In this paper, they have performed a set of uniform tests across all always-on consumer IoT devices and organized the results into 4 domains: user-facing cloud services, mobile application interface, back-end cloud services, and device debugging interfaces.

K. Trusted-third-party-based key exchange protocol [11]

In this paper, they have focus on security considerations for IoT from the perspectives of end-users, cloud tenants, and cloud providers, working across the range of IoT technologies.

L. Attacks on IoT Systems [15]

In this paper, they have focus on security considerations, Attacks and their countermeasures. Physical Attacks, Side

Channel Attacks, Environmental Attacks, Cryptanalysis Attacks, Software Attacks, Network Attacks are subcategorized.

M. Security, privacy and trust [16]

In this paper, they have focus on the satisfaction of security and privacy requirements which includes data confidentiality and authentication, access control, IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies.

III. Intelligent Security Framework

Cryptography is the use of codes and ciphers to protect private communication and it keep them private from everyone except the intended recipients., it is complex to implement sufficient cryptographic functions on constrained devices due to the resources limitation. This proposed system implements Dual Mutual Authentication.

First Light Weight Asymmetric Key cryptography is used to provide authentication between sensor node and Device Gateway. The Sensor Node's Unique Id and Device Gateway's unique Id is used to create a secret key/Digital certificate using AES Algorithm. Second the Device Gateway and the Cloud Service is mutually authenticated using public Key Encryption-Digital Signature.

A. ASymmetric Key Cryptography

Lightweight cryptography is a cryptographic algorithm implemented in constrained environments including RFID tags, sensors, contactless smart cards, and so on.

It is possible to prevent leakage of personal information and harmful actuating tasks by means of peer authentication and secure data transmission. we introduce a novel delegation architecture for one-way certificate-based authentication.

One time hand shake between sensor nodes and Device Gateway was carried using the Devices unique Id.

The sensor nodes message is encrypted using Digital certificate and the Device gateway decrypts the message and verifies the owner's id if there is violation that message will be discarded.

An Effective Algorithm is implemented in the Gateway to restrict the Unwanted traffic over the network and the cloud devices.

B. Lattice-based cryptography

A public key is generated using the random number and Gateways unique id.This key is used to transfer the message between cloud and Gateway.

The sensor devices unique id is shared using the initial Handshake, on arrival of new /fake devices the Device Gateway verifies the unique id and authenticated nodes information is updated to the cloud service.

The Device gateway encrypts the message using cloud service's public key. On receiving the message the cloud service decrypts the message using its private key and checks for the unique id in its repository. if there is any miss match the messages will be discarded.

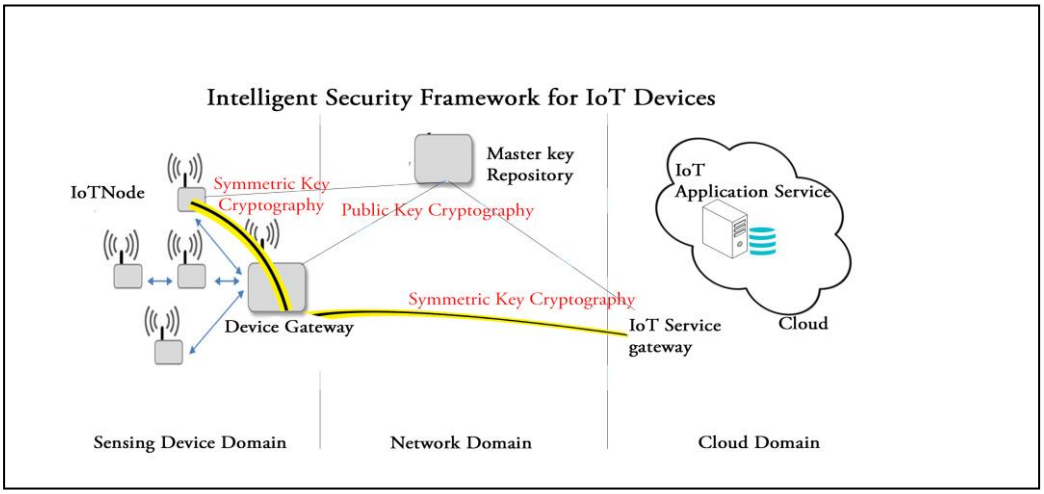

Fig 2: Cryptography- Symmetric & Public key Encryption

C. Intelligent Security Framework a Proposed Algorithm

Step 1: Pre-requisites

1.1: Master key repository maintains the details of the unique id of IoT nodes, Device gateway, IoT Service gateway & Cloud services and it generates the Key pair using Learning with errors encryption.

$$\text{Secret key } sk=s \xleftarrow{} Z^{n}_{q}$$

1.2: Master key repository's public key is made available to the connected entities via one time handshake and all the communications between them are carried by encrypting the message with Master key repository's public key that is acquired/generated (by Master key repository's)

Step 2: IoT nodes Key pair generation

2.1: IoT node communicates the Master key repository by offline/online mode and acquires Master key repository's public key.

2.2: IoT Node encrypts its unique id and the Timestamp(T) with Master key repository's public key (Pub).

$$\text{Pub}_{\text{Master key repository}} (\text{nodes unique id} + T)$$

2.3:the Master key repository verifies the unique id and Timestamps. the Master key repository generates a key pair and encrypt with its private key and send it to IoT node and sends the public key of Device gateway to IoT node.

$$\text{Pub}_{\text{Master key repository}} (\text{nodes Key pair})$$

Step 3: Secret Device Session Key generation

3.1: IoT nodes encrypts its unique id and the Timestamp with its private key(Pri) and double encrypts with Master key repository's public key and send to Master key repository.

$$\text{Pub}_{\text{Master key repository}} (\text{Pri}_{\text{IoT nodes}} (\text{unique id} + T))$$

3.2: The Master key repository decrypts with its private key and with IoT nodes public key. A secret Device Session Key (sdsk)is generated for this particular unique id and timestamp.

$$\text{sdsk} \leftarrow (\text{unique id} + T)$$

3.3: Master key repository encrypts the sdsk and Device gateways public key with its private key and sends it to IoT node.

$$\text{Pri}_{\text{Master key repository}} (\text{sdsk} + \text{Pub}_{\text{device gateway}})$$

3.4: Master key repository encrypts the sdsk and IoT nodes public key with its private key and sends it to device gateways.

$$\text{Pri}_{\text{Master key repository}} (\text{sdsk} + \text{Pub}_{\text{IoT node}})$$

Note :

The secret device session key is acquired for each session.

Step 4: Secret Service Session Key generation

4.1: Device gateway encrypts its unique id and the Timestamp with its private key(Pri) and double encrypts with Master key repository's public key and send to Master key repository.

$$\text{Pub}_{\text{Master key repository}} (\text{Pri Device gateway (unique id} + T))$$

4.2: The Master key repository decrypts with its private key and with Device gateways public key. A Secret Service Session Key (sdsk)is generated for this particular unique id and timestamp.

$$\text{sssk} \leftarrow (\text{unique id} + T)$$

4.3: Master key repository encrypts the sssk and IoT Service gateways public key with its private key and sends it to Device gateway.

$$\text{Pri}_{\text{Master key repository}} (\text{sssk} + \text{Pub}_{\text{IoT Service gateway}})$$

4.4: Master key repository encrypts the sssk and Device gateways public key with its private key and sends it to IoT Service gateway.

$$\text{Pri}_{\text{Master key repository}} (\text{sssk} + \text{Pub}_{\text{Device gateway}})$$

Note :

The secret service session key is acquired for each session.

Step 5: Data transfer from IoT nodes and Device gateway after acquiring Secret Device Session Key.

5.1: The node encrypts the message (m) & Timestamp using secret device session key(sdsk)

$$\text{secret device session key } (T + m)$$

5.2: The nodes gateway decrypts the message using secret device session key and then checks the Timestamp.

5.3: The message is retrieved after session key verification and local instructions are updated.

Note:

If the secret device session key is not present (after receiving multiple request from the same node) in Device gateway, it establish a session with Master key repository and sends public key of node. The Master key repository verifies again to check the unique id, if its updated then the public key and sdsk of node is updated to Device gateway else the discard message indication is conveyed and the packet is dropped.

Step 6: Data transfer from Device gateway and IoT Service gateway after Secret Service Session Key.

6.1: The Device gateway the message (m) & Timestamp using secret service session key(sssk)

secret service session key (T +m)

6.2: The IoT Service gateway decrypts the message using secret service session key and then checks the Timestamp.

6.3: The message is retrieved after session key verification and local instructions are updated.

Note:

If the secret service session key is not present (after receiving multiple request from the same node) in IoT Service gateway, it establish a session with Master key repository and sends public key of Device gateway. The Master key repository verifies again to check the unique id, if its updated then the public key and sssk of Device gateway is updated to IoT Service gateway else the discard message intication is conveyed and the packet is droped.

Step 7: End-To-End secure transaction.

7.1: The node sends the message (m) + secret device session key(sdsk) and double encrypt it using its private key and Device gateways public key.

$$\text{Pub}_{\text{Device gateway}}(\text{Pri}_{\text{Iot node}}(\text{sdsk} + m))$$

7.2: The Device gateway decrypts the message using its private key and then decrypts with nodes public key and verifies the sdsk.

7.3: The Device gateway removes the sdsk and embed the message with sssk and encrypts with its private key and double encrypts with the public key of node IoT Service gateway.

$$\text{Pub}_{\text{IoT Service gateway}}(\text{Pri}_{\text{Device gateway}}(\text{sssk} + m))$$

7.4: The IoT Service gateway decrypts the message using its private key and then decrypts with Device gateways public key and verifies the sssk and reads the original message.

Note:

If there is any mismatch in the timestamp the packets get discarded.

Fig 1 and Fig 2 represents the key architecture and cryptosystems.This scheme eliminates the Eavesdropping attack, Man in the Middle attack and Distributed Denial of Service Attacks [9]. The lattice key cryptography provide security and eliminates Quantum algorithm attacks.

IV. CONCLUSION

In this paper, we have proposed the Mutual and double authentication schemes, which reduces the traffic by eliminating the fault and fake packets. This system provide security against the Quantum Attacks, improves the performance and reduces the bandwidth consumption

References

[1] Jihyun Kim , Yonghun Jeon, Howon Kim, “The intelligent IoT common service platform architecture and service implementation,” J Supercomput DOI 10.1007/s11227-016-1845-1, © Springer Science+Business Media New York ,20-Aug- 2016 .

[2] David Airehrour , Jairo Gutierrez , Sayan Kumar Ray,” Secure routing for internet of things: A survey”,Elsevier Ltd 2016.pp.198-213.10-Mar-2016.

[3] Jongseok Choi, Youngjin In,Changjun Park,Seonhee Seok,Hwajeong Seo, Howon Kim,” Secure IoT framework and 2D architecture for End-To-End security”, DOI 10.1007/s11227-016-1684-0 © Springer Science+Business Media New York ,02-Mar-2016.

[4] Zheng Yan, Mingjun Wang, and Yuxiang Li,Athanasios V. Vasilakos, ” encrypted Data Management with Deduplication in Cloud Computing” 2325-6095/16/©2016 IEEE,Mar-2016.

[5] I.S. Jacobs and C.P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[6] Kun-Lin Tsai, , Yi-Li Huang, Fang-Yie Leu,” TTP based High-efficient Multi-Key Exchange Protocol” unpublished.

[7] Amira Barki1, Abdelmadjid Bouabdallah, Sa¨ıd Gharout and Jacques Traor´e “M2M Security: Challenges and Solutions”, unpublished.

[8] Sandip Ray,Yier Jin,and Arijit Raychowdhury,” The Changing Computing Paradigm with Internet of Things:A Tutorial Introduction”, unpublished.

[9] Nirmala Singh , Sachchidanand Singh “Internet of Things(IoT): Security Challenges,Business Opportunities & Reference Architecture for E-commerce” 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).Nov-2016.

[10] “The Internet of Things:Security Research Study” Veracode White Paper ,2014

[11] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers,” Twenty security considerations for cloud-supported Internet of Things”, INTERNET OF THINGS JOURNAL, IEEE,23-Nov-2016.

[12] Rolf H. Weber,” Internet of Things – New security and privacy challenges”, comp u t e r law & s e c u r i t y r e v i e w 2 6 (2 0 1 0) 2 3 – 3 0,22-Nov-2016.