ARO_VID: A UNIFIED FRAMEWORK FOR DATA SECURITY IN INTERNET OF THINGS

[1]A. Vithya Vijayalakshmi, [2]Dr. L. Arockiam
[1]Ph.D. Scholar, [2]Associate Professor,
[1,2]Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India

Abstract : The Internet of Things visualizes a real world in which every object is connected to the Internet. Things used in our day-to-day life form a part of the virtual world, whereby they can be controlled and remotely accessed in a spontaneous way. However, the interaction and data exchange may be performed by different communication channels and can be direct. Hence, the communication between the devices must be secured and the data transmitted between the devices or the local gateway should also be protected. Therefore, this paper proposes a data security framework for internet of things to secure the data in all the IoT communication models such as device-to-device communication, device-to-gateway communication and back-end data-sharing model.

Key words: Internet of Things, Data Security, Communication Models, Framework

---

1. INTRODUCTION

The aim of Internet of things is to communicate among pervasive devices such as RFID, sensors etc. through heterogeneous networks. IoT can be defined as "a network of uniquely identifiable, accessible, and manageable smart things that are capable of performing communication, computation and ultimate decision making" [1]. IoT completely transforms connectivity from "anytime", "anywhere" for "anyone" into "anytime", anywhere" for "anything" [8]. IoT holds many applications such as smart cities, smart homes, healthcare etc. Wireless Sensor Networks are an important part of the IoT that are responsible of collecting data. However, the sensor nodes should send data to the server in a secure way. This communication should satisfy confidentiality, authentication, integrity, non-repudiation and anonymity etc. [2]. Providing data security to the streaming or sensed data is a major issue in IoT. To use device communication effectively, we need to secure the data in the communication models of Internet of Things.

2. INTERNET OF THINGS COMMUNICATION MODELS

2.1. Device-to-Device Communication

In device-to-device communication model, two or more devices connects and communicate directly between each other. Protocols used to communicate these devices are Bluetooth, Z-Wave, ZigBee etc. Communicate between devices occurs at different types of networks such as IP networks and Internet. Figure 1 shows the device-to-device communication model.

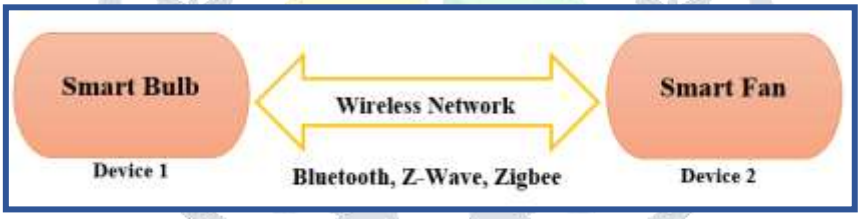

Figure 1: Device-to-Device Communication

2.2. Device-to-Cloud Communication

In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic [7]. This model uses communication mechanisms such as wired Ethernet or Wi-Fi connections to create a connection between the device and the IP network which directly connects to the cloud server. Figure 2 shows the device-to-cloud communication model.

Figure 2: Device-to-Cloud Communication

2.3. Device-to-Gateway Communication Model

Device-to-gateway model is like device-to-application-layer gateway (ALG) model. To reach a cloud service, the IoT device connects through an application-layer gateway service. This ALG in a local gateway acts as an intermediate between the cloud server and the device to provide security, protocol or data translation. Here, the local gateway can be a smartphone, where the application is running. This application communicates with the device and sends data to the cloud server. Figure 3 shows the device-to-gateway communication model.

Figure 3: Device-to-Gateway Communication

2.4. Back-End Data-Sharing Model

Back-End Data-Sharing model is the extended version of the single device-to-cloud communication model. This model denotes the communication that enables users to export and analyze smart object data from a cloud service in combination with data from other sources [7]. It allows the data collected from the IoT device data streams to be aggregated and analysed. Figure 4 shows the Back-End Data-Sharing Model.

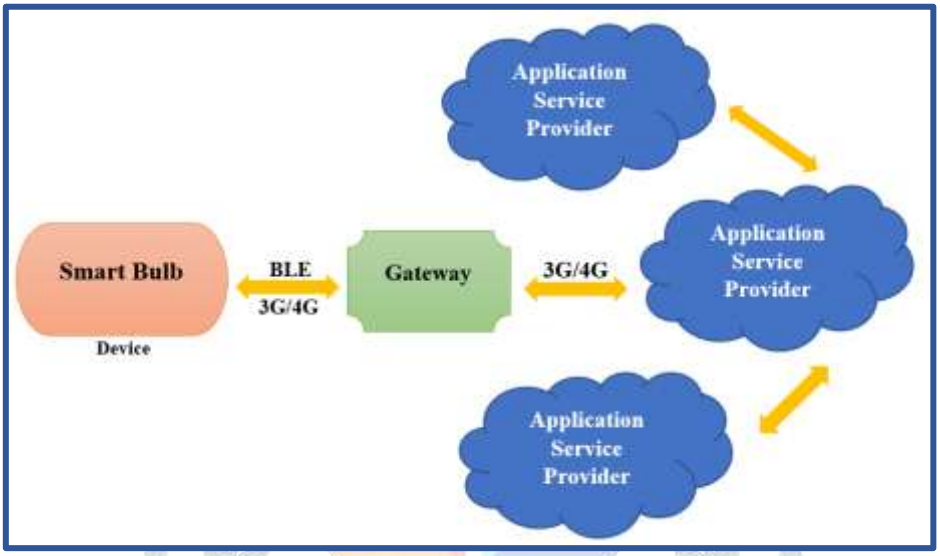

Figure 4: Back-End Data-Sharing Model

3. Related Works

Dharmendra Singh Rajput et al. [3] presented an architectural framework for secure health monitoring. They mainly concentrated on health-related issues such as diabetics, pulse rate measuring and heart monitoring system. The data collected from the healthcare sensor are processed and accessed through a smart phone. The simulation done by using the health issues collected from the people who are residing in the remote areas by using different sensors. This framework helps to secure the data collected from the sensors and stored in the cloud and accessing the data from different geographical locations.

Sukant K. Mohapatra et al. [4] discussed various IoT management issues and challenges such as privacy, security, scalability, availability etc. They proposed a solution framework for managing those issues. The proposed framework provides various innovative solutions for enriching IoT systems. They also provide the enablement solutions, operational solutions, Business solution and security solutions. In managing the IoT system, security issues face a major role. They elaborated various standard organizations focused on managing IoT systems.

Ebrahim AL Alkeem et al. [5] focused on the security issues and challenges on wearable devices and the advantages of using them in smart healthcare. They explained the need of security in patient's information and the solutions to secure that information. The proposed scheme focused on authentication and role base access control. A framework to overcome the security issues in authentication and role base access control is proposed. The proposed security service will enhance security levels of IoT Technologies. The simulation has done by the data collected from the Dubai Health Authority (DHA) to secure medical records.

Wolfgang Leister et al. [6] developed a framework for the assessment and validation of context - aware adaptive security solutions for IoT Smart Healthcare. The evaluation process used three scenario such as smart home, e-health and emergency. The scenario explained the detection of security threats and solutions to overcome those threats. They discussed two types of requirements namely security requirements and QoS requirements, the framework is based on these requirements. The working of the proposed framework was explained with the numerical values as an input.

4. The System Model for Internet of Things

The Figure 5 shows the system model for Internet of things. It includes Sensors, local processing, IoT gateway, cloud storage.

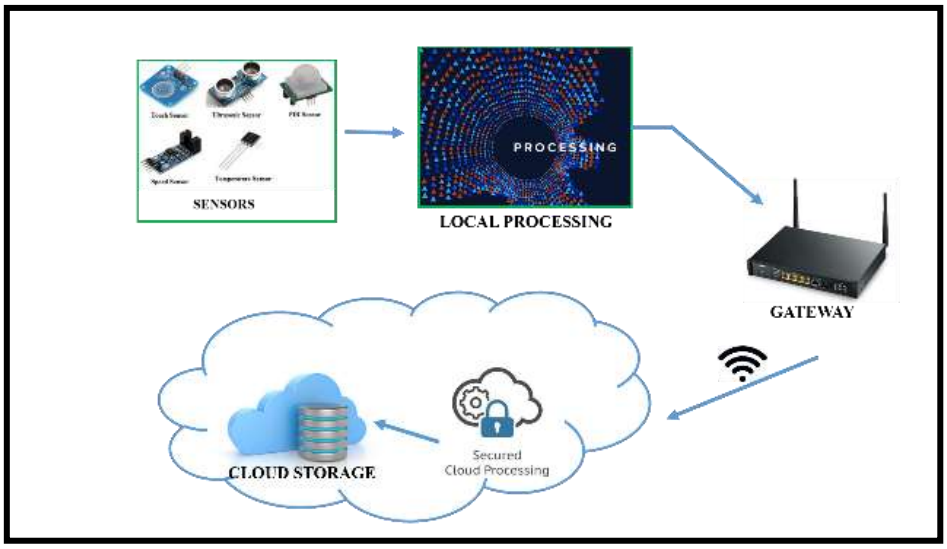

Figure 5. System model for Internet of Things

4.1. Sensors

Sensor is a device which detects the environment/events and sends the information to other electronic devices. For example, the data come from the various smart devices such as RFID, barcode labels, actuators and intelligent detection devices are processed and transferred to other devices or local/cloud server.

4.2. Local Processing

The data collected from the sensor are processed in such a way that the attacks or unauthorized users cannot find the source of the data while transferring it through the wireless network.

4.3. IoT Gateway

IoT is an application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation.

4.4. Cloud Storage

One of the characteristics of the IoT is the intelligent processing, which means using cloud computing and other intelligent computing technology to analysis and process vast amounts of data and information as to implement intelligent control for objects. The development of the IoT uses cloud calculation's strong processing and storage capacity.

5. Methodology

The objective of this research work is to propose a data security framework for Internet of Things communication models. To achieve the data security in three communication models such as device-to-device, device-to-gateway and back-end data-sharing model, the proposed ARO_VID framework includes three security techniques, namely ARO_EDGE (data security between device-to-device), ARO_GATE (data security between device-to-gateway) and ARO_CLOUD (data security in back-end data-sharing). The proposed framework is shown in the below figure.

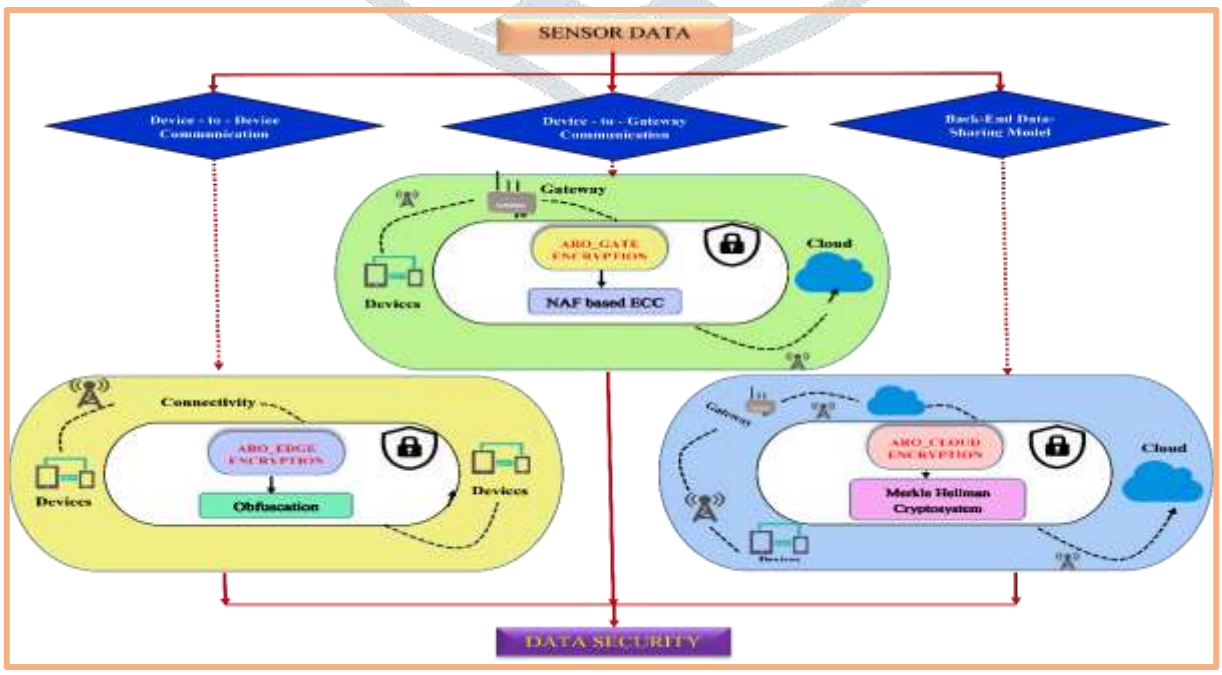

Figure 6. A Unified Framework for Data Security in Internet of Things

5.1. ARO_EDGE

The proposed ARO_EDGE technique helps to secure the data collected from the sensor by using data obfuscation technique. To ensure the data confidentiality in device-to-device communication, the data are encrypted using obfuscation technique before sending the data to the local server / gateway. This is symmetric key encryption technique. In terms of existing techniques, symmetric encryption is suitable for embedded devices and effective in devices with limited resources. The scope of this technique is to encrypt the numerical sensor data sensed from the medical IoT devices and communicated with other devices. This obfuscation technique includes mathematical functions to scramble the given input into unintelligible form and to prevent from unauthorized access.

5.2. ARO_GATE

The proposed ARO_GATE technique to secure the data collected from the sensor and transmitted to the local serve/gateway and get encrypted in the gateway. This belongs to the device-to-gateway communication model. To ensure the data security at gateway level, the data are encrypted using ElGamal based Elliptic Curve Cryptography (ECC) encryption. In ECC encryption, scalar multiplication plays a major role. To increase the computation speed of scalar multiplication in ECC, a block method for computing Non-Adjacent Form (NAF) is used. The proposed {0,1,15}-NAF will recode the integer k in scalar multiplication which helps to increase the computational speed and data security.

5.3. ARO_CLOUD

The proposed ARO_CLOUD technique to secure IoT data transmitted over the cloud server (Application service provider). Here, the data are encrypted before the cloud server communicated with each other. This belongs to the back-end data-sharing model in Internet of Things. The proposed technique uses Merkle-Hellman Knapsack Cryptosystem and Euler's totient function to encrypt the data. This encryption technique uses three keys to encrypt and decrypt the data which gives more security and infeasible for the intruder to break the cryptosystem. This technique increases the data security and decreases the computational time for both encryption and decryption.

6. Application

In Internet of Things everything is connected and communicated with each other. There are many possible areas of IoT such as smart city, smart home, smart healthcare, agriculture and breeding, augmented maps, assisted driving etc [9]. Among many applications smart healthcare requires high-level data security. IoT medical devices were developed for healthcare services based on wireless sensor network. These devices are used to measure the patient's conditions and transmit the data to the other devices or local gateway through wireless network. After reviewing wide range of existing IoT-based healthcare system, several requirements for the design of such systems become apparent [10]. The proposed framework is suitable for this e-healthcare, the encryption techniques used in this framework will secure the data sensed from the medical IoT devices.

6.1 Hardware Requirements

***Arduino Uno*:** Arduino is an open-source gadget prototyping stage considering adaptable, simple to-utilize equipment and programming. [11].

Figure 7. Arduino Uno

***Body Temperature Sensor*:** The digital thermometer provides Celsius temperature measurements and can derive power directly from the data line, eliminating the need for an external power supply.

Figure 8. Temperature Sensor

Heart Rate Sensor: The heart rate sensor provides the human body heart rate. Heart Beat can be measured based on optical power variation as light is scattered or absorbed during its path through the blood as the heart beat changes [12].

Figure 9. Heart Rate Sensor

The data collected from the sensor are encrypted at three levels such as device level, gateway level and back-end data-sharing by using the proposed three encryption technique such as ARO_EDGE, ARO_GATE and ARO_CLOUD. The IoT data encryption and decryption process by using proposed technique are given below.

Figure 10. Data collected from different sensors

Figure 11. Encrypted data using proposed algorithm

7. Conclusion

Now-a-days, the devices are communicating with each other and sending data through wireless network. The importance of data in smart system are increased. A variety of medical IoT devices and software applications are applied to improve the quality of medical services. To protect data security and privacy at all stages of data flow will consider as a great challenge in Internet of Things research. This paper discussed the internet of things communication models and need of data security at various levels. Here, smart healthcare given great attention; and solution to secure healthcare data at various stages is proposed

Acknowledgement

This research was supported by a grant from University Grants Commission (UGC) awarded to A. Vithya Vijayalakshmi under Senior Research Fellowship.

References

1. Isha and Ashish Kr. Luhach, "Analysis of Lightweight Cryptographic Solutions for Internet of Things", Indian Journal of Science and Technology, 2016, ISSN: 0974-6846, Vol. 9. Iss.28, pp. 1-7.
2. Fagen Li, Zhaohui Zheng and Chunhua Jin, "Secure and Efficient Data Transmission in the "Internet of Things, Springer, Journal of Telecommunications Systems, Vol. 62, Iss. 1, 2016, pp. 111-122.
3. Dharmendra Singh Rajput and Rakesh Gour, "An IoT Framework for Healthcare Monitoring Systems", nternational Journal of Computer Science and Information Security (IJCSIS), 2016, ISSN: 1947-5500, Vol. 14, No. 5, pp. 451-455.

4. Sukant K. Mohapatra, Jay N. Bhuyan, Pankaj Asundi and Anand Singh, "A Solution Framework for Managing Internet of Things (IoT)", International Journal of Computer Networks & Communications (IJCNC), 2016, Vol. 8, No. 6, pp. 73-87. DOI: 10.5121/ijcnc.2016.8606.
5. Ebrahim AL Alkeem, Chan Yeob Yeun and M. Jamal Zemerly, "Security and Privacy Framework for Ubiquitous Healthcare IoT Devices", IEEE, International Conference for Internet Technology and Secured Transactions, 2015, pp. 70-75.
6. Wolfgang Leister, Mohamed Hamdi, Habtamu Abie, Stefan Poslad and Arild Torjusen, "An Evaluation Framework for Adaptive Security for the IoT in eHealth", International Journal on Advances in Security, 2014, Vol. 7, no. 3, pp. 93-109.
7. Santosh Kulkarni and Sanjeev Kulkarni, "Communication Models in Internet of Things: A Survey", International Journal of Science Technology & Engineering, 2017, ISSN: 2349-784X, Vol. 3, Iss. 11, pp. 87-91.
8. A.Vithya Vijayalakshmi and Dr. L. Arockiam, "A Study on Security Issues and Challenges in IoT", International Journal of Engineering Sciences & Management Research, 2016, ISSN 2349-6193, Vol. 3, Iss. 11, pp. 1-9.
9. A. Dalvin Vinoth Kumar, A.Vithya Vijayalakshmi1 and Dr. L. Arockiam, "TENSOR: A Technique to Enhance IoT Data Security using Bluetooth Low Energy Network for Smart Home Environment", Chapter 19, Statistical Approaches on Multidisciplinary Research, Volume I, DOI://doi.org/10.5281/zenodo.263014, Surragh Publishers, India, 2017.
10. Stephanie Baker and Wei Xiang, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities", IEEE, 2017, ISSN: 2169-3536, Vol. 5, pp. 26521 – 26544., DOI: 10.1109/ACCESS.2017.2775180.
11. https://www.elprocus.com/heartbeat-sensor-working-application/

Authors Biography

A. Vithya Vijayalakshmi is a full-time research scholar in Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli. She received her M.Phil. degree from St. Joseph's College (Autonomous), Tiruchirappalli, MCA degree from Holy Cross College (Autonomous), Tiruchirappalli and UG degree from Lady Doak College (Autonomous), Madurai. She has presented papers in National and International Conferences and attended many workshops, seminars and short courses. She has also acted as a resource person for the Seminar and State Level Workshop. Her area of research interests are Internet of Things and Cloud Computing.

Dr. L. Arockiam is working as an Associate Professor in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu. He has 29 years of experience in teaching and 21 years of experience in research. He has published 306 research articles in the International / National journals and conferences. He has also presented 3 research articles in the Software Measurement European Forum in Rome, Italy, a research article in the International Conference on Computational Intelligence and Cognitive Informatics in Bali, Indonesia and a research article in the International Conference on Intelligent Network and Computing at Curtin University, Sarawak, Malaysia. He has chaired 100 technical sessions and delivered invited talks in National and International Conferences. He has co-authored books on "Success through Soft Skills", "Research in a Nutshell", "Object Oriented Programming with C#.NET" and "WEKA: A Practical Guide to Beginners". His area of research interests are: Internet of Things, Cloud Computing, Big Data, Data Mining, Software Measurement, Cognitive Aspects in Programming, Web Services and Mobile Networks.