INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

**ISSN: 2454-132X**
**Impact factor: 4.295**
***(Volume 4, Issue 5)***
Available online at: www.ijariit.com

# Securely handling the data in Internet of things: An architect model

*Priyanga G*
*gpriyangatpt@gmail.com*
*Sacred Heart College, Vellore, Tamil Nadu*

*Arun Nehru T*
*Nehru.ctan04@gmail.com*
*Periyar University College of Arts and Science, Pappireddipatti, Tamil Nadu*

*Thomas Immanuel V*
*thomas@shctpt.edu*
*Sacred Heart College, Vellore, Tamil Nadu*

## ABSTRACT

***Nowadays in every filed the data is got increased by exponentially in this context when the IOT and the Cloud come together we need the support of Big data to handle the amount of data. "I found that there are lots of drawbacks in the security concern about the data stored in Cloud". Towards that I am going to provide the new framework and Architecture for the cloud security at the user side. The previous concept is that the cloud service provider they give certain security to our data and also they have the rights to sell our data to vendors. Here is my solution, the user can have the right to choose the security level based on the need he/she can have full security even the cloud service provider cannot have the chance to view our data So, it will be more secure in the cloud.***

***Keywords***— *Big data, IoT, Secure in cloud, Framework, Architecture*

## 1. CORRELATION BETWEEN IOT AND BIG DATA

The future of technology lies in data and its analysis. More objects and devices are now connected to the Internet, Transmitting the information they gather back for analysis. The goal is to harness this data to learn about patterns and trends that can be used to make a positive impact on our health, transportation, energy conservation, and lifestyle. However, the data itself doesn't produce these objectives, but rather its solutions that arise from analyzing it and finding the answers we need.

Two terms that have been discussed in relation to this future: big data and the internet of things (IoT) it's hard to talk about one without the other, and although they are not the same thing, the two practices are closely intertwined. Big data analytics tools are capable of handling masses of data transmitted from IoT devices that produce a continuous stream of information.
Let's the take a closer look at the two practices before we examine their connection.

## 2. FORECASTING THE TECHNOLOGY AND SECURITY LEVEL

This disruptive technology requires new infrastructures, including hardware and software applications, as well as an operating system; enterprises will need to deal with the influx was the data starts flowing in and analyzing it in real-time.

The IOT delivers the information, from which big data analytics can draw the information to create the insights required of it. However the IOT brings data on a different scale, so the analytics solution should accommodate its needs of rapid ingestion and processing followed by an accurate and fast extraction.

The challenges by 2020 are projected that 20.8 billion "things" will be used globally, as the Internet of Things continues its expansion; as a result, we can see major cybercriminals issues and safety concerns arise, as cybercriminals could potentially break into the connected system that contains sensitive data.

Internet security platforms like Zscaler offer IOT devices for protection against security breaches with a cloud-based solution. You can route the traffic through the platform and set policies for the device so they won't communicate with unnecessary servers. The internet of things and big data share a closely knitted future. There is no doubt the two fields will create new opportunities and solution that will have a long and lasting impact.

### 2.1 Zscalar

Zscalar the world's largest security as a service (SaaS) cloud platform which provides the cloud-delivered web and mobile security solution. Zscalar infrastructure provides its feature by using three key components: the Zscalar central Authority, Zscalar central Authority, Zscalar Enforcement Nodes, and Nano log Cluster.

### 2.2 Zscalar Included with Cloud

The zscalar cloud that is used solely for the centralized distribution of various feeds to the Zscalar clouds Zscalar feed its threat intelligence and to the CA, which then sends updates to the ZENs, ensuring that every ZEN has the latest version of the URL database and the latest malware and threat information.

## 3. EXISTING ARCHITECTURAL ELEMENTS OF IOT

In designing and building the IoT systems new hardware and software are begin designed and developed and different tools are available to bring the IoT into the reality, with rapid development occurs in the sensor, many sensors incorporate with different devices to capture the real-time data.

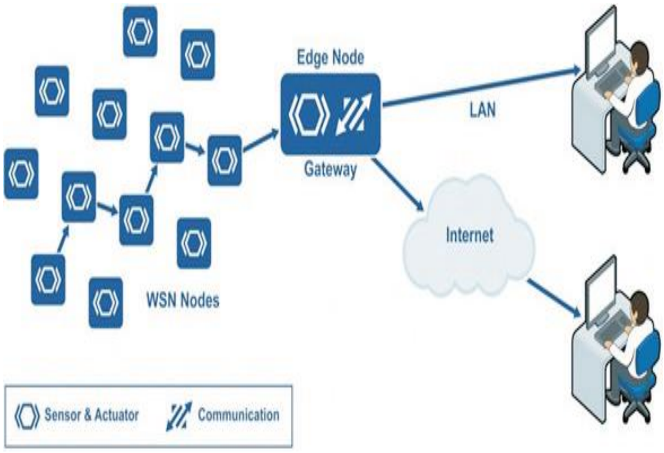

**Fig. 1: Architectural elements of IOT**

A wireless sensor network (WNS) is made up of large sprayed sensor that continuously monitor the physical and environmental conditions, for example, temperature, pressure etc. The data collected from the sensor are transferred via one network node to another.

All these sensors are manufactured through the lithography process and come under the category called a micro electro mechanical designed system (MEMS), these sensors are one type of circuit perform a specific task and also paired with a microprocessor and attached with the wireless radio for communication.

To develop or design IoT environment, an embedded system is playing the very important role. In general, the IoT system has four main components.

1) First and more important is the internet.
2) The second, important thing is a device which has the capability to transfer the real time over the network.
3) The third, proper and well-established network with a gateway which translates communication protocols to Internet Protocol.
4) The last back-end services which are used to store the collected data it may be an enterprise database system or cloud.

**Note**

- Technology for IoT system directly effects on devices hardware requirements and costs.
- The Proposed Architecture to maintain the security over the IoT Data.
- IOT architecture can be represented with the help of four types of interconnected system such as things, gateways, network, and cloud.

### 3.1 Thing

Today there are large numbers of things available in the industrial and commercial setting. Now a Days, they acquire home and mobiles also. Already cars, many devices sensors, mobile phones access the internet through the wireless network. IoT environment requires the type of thing which are intelligent and capable to filter the data as wells manage this data and they are easy to connect with gateways, For example, mobile phones, security alarm at home, smart building and industrial automation.

### 3.2 Gateway

Many of the designed things are not capable to connect with the internet. For solving this issues gateways is used as an intermediate between the internet and things.

### 3.3 Network Infrastructure

A worldwide structure of interconnected IP networks the links billions of computers together. Network infrastructure comprises routers, gateways, switches, repeater and many other.

### 3.4 Cloud

The cloud is the only technology suitable for filtering, analyzing, storing and accessing IoT and other information, in this one of the deployment models such as a community cloud can be used in development. A community cloud is managed and used by a particular group or organizations that have shared interests, such as specific security requirements or a common mission.

### 3.5 The outlook of the cloud computing

- Cloud computing is a web-based service that can be accessed without any special assistance or permission from other people.
- Cloud computing resources can be accessed through a wide variety of internet-connected devices such as tablets, mobile devices, and laptops.
- Cloud computing allows for resource pooling, meaning information can be shared with those who know where and how (have permission) to access the resource, anytime and anywhere. This leads to broader collaboration or closer connections with other users. From an IoT perspective, just as we can easily assign an IP address to every "thing" on the planet, we can share the "address" of the cloud-based protected and stored information with others and pool resources.
- Cloud computing features rapid elasticity, meaning users can readily scale the service to their needs. You can easily and quickly edit your software setup, add or remove users, increase storage space, etc. This characteristic will further empower IoT by providing elastic computing power, storage, and networking.

## 4. LAYERED FRAMEWORK

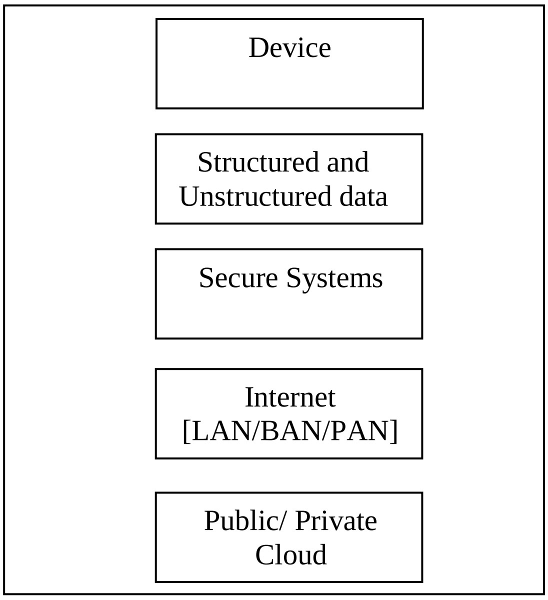

**Fig. 2: Layered framework**

## 5. SECURE SYSTEM

With RSA you cannot encrypt data that is bigger than the length of the asymmetric key. If you want to encrypt a bigger block of information, what exactly would you do? Preferably, you'd wish to make use of symmetric encryption algorithm such as AES, but the issue you encounter is that of secure and reliable key trade. With AES, each recipient has to have the same key. This all seems easy in principle but how do you get that same key securely to each person? You can't just easily send the key to them. So what you want to do is employ what is called a **hybrid encryption** system. This is where you use a combination of both RSA and AES. Let's assume we have two people involved: the sender, Nina, and the receiver, Tom. The process would look like the following for Nina sending data to Tom:

### 5.1 Encryption Using the Hybrid Approach

- Nina generates a 256-bit (32-byte) AES Key. This key is called a session key in this process.
- Nina generates a 128-bit (16-byte) IV.
- Nina encrypts the data with AES using the session key and the IV.
- Nina encrypts the session key with RSA and Tom's public key.
- Nina stores the encrypted data, encrypted AES session key, and IV in a separate structure or file. This is the packet of data that is sent to Tom.

### 5.2 Decryption Using the Hybrid Approach

- Tom decrypts the encrypted AES session key by using RSA and Tom's private key.
- Tom decrypts the encrypted data by using the decrypted AES session key and the IV.
- Tom reads the decrypted message.
- Now, let's look at the same process again but this time, Tom is sending a reply to Nina where Tom uses Nina's public key and Nina uses her private key.

### 5.3 Encryption Using the Hybrid Approach

- Tom generates a 256-bit (32-byte) AES Key. This key is called a session key in this process.
- Tom generates a 128-bit (16-byte) IV.
- Tom encrypts the data with AES by using the session key and the IV.
- Tom encrypts the session key with RSA and Nina's public key.
- Tom stores the encrypted data, encrypted AES session key, and IV in a separate structure or file. This is the packet of data that is sent to Nina.

### 5.4 Decryption Using the Hybrid Approach

- Nina decrypts the encrypted AES session key by using RSA and Nina's private key.
- Nina decrypts the encrypted data by using decrypted AES session key and the IV.
- Nina reads the decrypted message.

### 5.5 Hybrid Encryption Implementation

We shall use the Aes Encryption class to demonstrate this hybrid encryption approach. In the AES Encryption class, there is a new method added called Generate Random Number which will be used to generate our session key. For this example, we will use AES with a 256-bit (32-byte) key and we will use the algorithm in the default cipher block chaining mode with PKCS7 padding.
For the asymmetric encryption part of the hybrid encryption technique, we will use the same RSA with RSA Parameter Key class from our demonstration of RSA encryption. This class will store the generated RSA public and private keys as private members of the class for simplicity in this example. In a normal usage scenario, you would want to securely store your private key on a server or in a database.

First of all, we need a class to store our encrypted data packet. There are three parts to the packet that you will have once you have done the encryption. They are:

- **Encrypted Session Key**: This is the 256-bit AES session key that is generated and then encrypted with the RSA private key.
- **Encrypted Data**: This is our actual data that has been encrypted with the AES 256-bit session key.
- **Initialization Vector (IV)**: This is the 128-bit (16-byte) IV that is passed into the AES encryption algorithm. This does not need to be kept secret and can be stored inside our data packet.

The encryption process is very simple as shown in the following code example. The Encrypt Data method takes a string which, in this case, is our data to encrypt and the RSA with RSA Parameter Key object which contains our RSA keys.

This method first creates an instance of the AES Encryption object and generates the 256-bit (32-byte) session key. Then, the 128-bit (16-byte) IV is generated and stored in the encrypted packet object. Next, the data we want to be encrypted is encrypted with AES by using the generated session key and IV. The result is also saved in the encrypted packet object. Lastly, the generated AES session key is encrypted with the RSA public key. This encrypted session key is then saved in the encrypted packet.

This means our data is now encrypted using AES, but the key is protected using the RSA key pair.

The decryption process is just as simple. There is a method called Decrypt Data that takes the encrypted packet and the RSA encryption object that contains our public and private encryption keys. First, the encrypted AES session key is decrypted using the RSA with RSA Parameter Key object. This decrypts using the private key. Once the session key has been decrypted, the encrypted data is then decrypted with AES by using the session key and initialization vector. Then, the decrypted data is turned back into a string and returned to the caller.

This example shows how to get the best of both RSA and AES: You get the benefits of RSA's asymmetric keys (which make key exchange much easier) and you then get the benefit of AES for securely encrypting your data with the RSA- protected session key.

## 6. THE PROPOSED ARCHITECTURE TO MAINTAIN THE SECURITY OVER THE IOT DATA

IoT architecture can be represented with the help of four types of interconnected systems such as things, gateways, network, and cloud.

- **Things** Today there are large numbers of things available in industrial and commercial settings. Now a day, they acquire home and mobiles also. Already cars, many device sensors, mobile phones access the internet through the wireless network. IoT environment requires such type of things which are intelligent and capable to filter the data as well as manage this data and they are easy to connect with gateways. For examples: mobile phones, security alarm at home, smart buildings and industrial automation.
- **Gateways** Many of the designed things are not capable to connect with the internet. For solving this issue gateway is used as an intermediate between the internet and things.
- **Network Infrastructure** Internet is a worldwide structure of interconnected IP networks that link billions of computers together. Network infrastructure comprises routers, gateways, switches, repeaters, and many other.

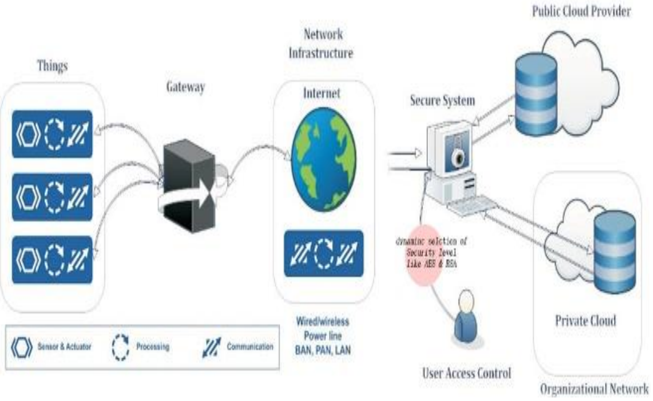

**Fig. 3: Security solution with new architecture**

## 7. CONCLUSION

Hence we know the security level of this proposed Architecture so, we can say this would be the best real-time solution for the next generation IoT, Cloud, and Big Data areas for the vastly growing Technologies.

## 8. REFERENCES

[1] Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption Jayant D. Bokefodea, Avdhut S. Bhiseb, Prajakta A. Satarkara and Dattatray G. Modanic

[2] Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT) Furqan Alama, Rashid Mehmood, Iyad Katiba, Aiiad Albeshria.

[3] Overview of the Internet of Things and Security issues Prof. Animations A, Economides University of Macedonia.

[4] The Internet of Things: Challenges & security issues, G. S. Matharu, P. Upadhyay, and L. Chaudhary, International Conference on emerging technologies (ICET), Islamabad, pp. 54-59, 2014.