Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption

Jayant D. Bokefode\textsuperscript{a,}\textsuperscript{*}, Avdhut S. Bhise\textsuperscript{b}, Prajakta A. Satarkar\textsuperscript{a} and Dattatray G. Modani\textsuperscript{c}

\textsuperscript{a}SVERI’s College of Engineering, Pandharpur, Solapur University, India
\textsuperscript{b}SVERI’s College of Engineering (Poly), Pandharpur, India
\textsuperscript{c}Gharda Institute of Technology, Lavel, Chipilun, Mumbai University, India

Abstract

Internet of things is one of the most emerging and popular technology, which has changed our life, by impacting different areas such as shopping, enterprise production, storage, monitoring physical devices, etc. The Internet of Things (IoT) is an atmosphere in which all physical objects, peoples or animals are having unique identity and they are able to transfer data over a network without any interaction. An improvement in electronic sensing devices and rapid growth in communication infrastructure, and their monitoring systems give very fast access to retrieve data and allow communication with physical devices. Now days, Organizations use IoT devices to collect real time and continuous data and make better business decisions to increase customer satisfaction. But collected data need to be processed and transferred in appropriate format to store on storage system – which is triggering organizations to rethink their data storage infrastructures. An enterprise has to store data generated from the Internet of Things and this data grows exponentially, it forces to think about cloud storage for storing IoT data. The proposed work allows the organization to store the IoT data on the cloud securely by applying different Access control policies and the cryptography concepts.

Keywords: Cryptography; Cloud Security; IoT; Role Based Access Control Model; Sensors.

1. Introduction

The IoT can be considered as one type of environment in which all physical objects, peoples and animals are having unique identity and they are able to transfer data over the network without any interaction\textsuperscript{1}. IoT is the combination of different technologies, it evolved the internet, wireless technologies and micro-electromechanical systems (MEMS). This terminology can be considered as the Internet of Everything. A thing presents in the IoT environment can be a man-made object, a person with a heart monitor implant, any animal with a biochip transponder and any vehicle with sensor. All these things are assigned with one unique IP address and has the ability to transfer data over the Internet. So far, IoT closely related to Machine-to-Machine (M2M) communication in manufacturing, oil and gas power industries. The IPv6s having huge address space and with help of IPv6 we can assign a unique address to each object present on the surface of earth. IPv6 is a very significant feature for the development of Internet Things. The

\textsuperscript{*}Corresponding author. Tel.: +919730154777.
E-mail address: bokefode.jayant@gmail.com
Internet of Things (IoT) hypothesis is that the objects or things interact and exchange large scale information. Nowadays, organizations use IoT devices to collect real-time and continuous data and make better business decisions to increase customer satisfaction. An enterprise has to store data generated from the Internet of Things and this data grows exponentially, it forces to think about cloud storage for storing IoT data. The cloud appears to be a noticeable choice for IoT data storage, various organizations store this information on-site considering it is either costly or sensitive to store on the cloud. The cloud has more advantages to store IoT data than on-premises storage. First, a direct connection is provided between the devices and the public cloud provider. This direct link allows to store data faster, therefore, it needs less storage and lower per-device cost. Second, data management and storage management is the cloud provider problem, therefore, organization has to use the service only.

Cloud becomes an ideal storage location for storing and processing IoT data but there are some problems to use the cloud for IoT data storage. The main and major issue is security of cloud storage. In many situations data collected from IoT devices is more sensitive or very important for the organization. When cloud storage is used, then organizations worried about the cloud security issues. This paper describes some of the security issues which hampers the cloud and their resolutions which make sure to the organization that the data stored on a cloud is secured.

A first, sharing the computing resource with cloud providers, physical security is lost. Data is stored with the third party cloud provider therefore the user does not have knowledge where the data is stored and not have control over it. This issue can be solved by insuring secure Data Transfer. The second issue is preserving the integrity and truthfulness of the data. This issue can be handled by providing Secure User Interfaces. The third issue is, there may be the possibility that the privacy rights will not be followed by cloud service providers. This issue can be solved by applying cryptographic techniques to data. If we provide good software which insures about security of the cloud storage system, then there is no problem to accept cloud storage to store IoT data.

Another important issue is how to control the user access on stored IoT data. To deal with this issue, different access control models are used. Based on Access Control model, the user can access resources, application, and data. Access control models specify the constructs and constraints to access the system and its resources. There are three types of Access control models; MAC (Mandatory Access Control model), DAC (Discretionary Access Control model) and RBAC (Role Based Access Control model). If MAC is incorporated in the system, then the system administrator has all the rights to manage the user’s roles and their rights. In MAC, as all the rights for modifying access policies are with administrator, other users fail to access the system. This access control is added in a very sensitive environment. For example, military and research centers. If a DAC is incorporated into the user has rights to modify the access rules for any objects but, if the attacker got the access rights over the user account it is too hazardous, therefore giving the complete rights to any user is not worthy for any organization. If RBAC policies are applied to the system, then the access rights are given to use the resources according to the role played by the user in the organization. This is very effective to use in organization where responsibilities are assigned to the user according to their role. In presented work, all access control models with cryptographic technique are incorporated in the system to ensure the security over the IoT data stored in a cloud.

2. Architectural Elements of IoT

To develop or design IoT environment, embedded systems are playing the very important role. In general, the IoT system has four main components. First and more important is the Internet. The second, important thing is a device which having capability to transfer the real-time data over the network. The third, proper and well-established network with gateway which translates communication protocols to Internet Protocol and the last Back-End Services which are used to store the collected data it may be enterprise database systems or the cloud. Designing and building the IoT systems are not that much complicated but can be a complex task. For IoT systems, new hardware and software are being designed and developed and different tools are available to bring the IoT into the reality. With rapid development occurs in sensors, many sensors incorporated with different devices to capture the real-time data. For example, Many IoT devices have sensors that can measure the changes in temperature, sound, pressure, different motions, and light. All these sensors are manufactured through the lithography process and come under the category called a Microelectro Mechanical System (MEMS). These sensors are one type of circuits designed to perform specific tasks and also paired with microprocessor and attached with the wireless radio for communication. Selecting a communication
technology for IoT systems directly effects on device hardware requirements and costs. Consider a factory as a case for IoT Systems. Factories require a large number of connected sensors and actuators over a wide-ranging area. For this wireless technology is best suited. A Wireless Sensor Network (WSN) is made up of large sprayed sensors 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.

2.1 Example: how IoT sensors work?

Let’s take one example of the IoT based navigation system which guide to the user by giving the speech based instruction for navigating through the aware and unaware environment. IoT based navigation system follows the client-server methodology, in which, the smart phone (android) considered as the client and the server is capable to provide the navigation directions for the multiple user at time. IoT based navigation system designed and developed by C-DAC pune as Proof of Concept (PoC) phase of NISG. This system consist 3 Linksys WRT54g Wi-Fi access points and Samsung galaxy S2 mobile phone. In this system, received signal strength indicator (RSSI) based fingerprinting technique in Wi-Fi is used for IoT arrangement. The received a signal strength of each access device is measured and stored to find out the exact location. The calculation for determining the exact location of the individual is done in two phases; training phase and tracking phase. In training phase, signal strength is measured from different location to provide the correct location to the server as the radio map. During the tracking phase multiple users are connected to the server by using smartphones. Then online data is matched with offline location data and based on this navigation, instructions are given to the specific user. To improve the exact location and correct navigation different routing algorithms and advanced navigation can be combined.

3. 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 intermediate between the internet and things.

- **Network Infrastructure** Internet is a worldwide structure of interconnected IP networks that links billions of computers together. Network infrastructure comprises routers, gateways, switches, repeaters, and many other
devices which controls the data traffic and connect with cable and telecom networks handled by different service providers.

- **Cloud** Cloud contains large pools of virtualized servers and servers connected together. To support the IoT environment cloud infrastructure runs different applications which are capable to analyze the data collected from different devices and sensors to make the correct decision.

IoT technology can be used in various fields or department, but have the main problem that is the security about the data. For example, IoT can be used in defense department to design the remotely controlled unmanned system to handle the battlefield situation as well as for controlling the environment to monitor the health of each and every solider. The Defense Information Systems Agency (DISA) added IoT as the next technology to use in different military application. IoT helps in the defense department by providing more information about the field which makes awareness about the current situation. The director of the DISA, Lt. Gen. Ronnie Hawkins Jr., USAF, DISA director, said that IoT will be very beneficial for war fighters but having major challenges. He also points out that if we have greater data access, we can avoid the war and war casualty but when everything is connected, everyone is vulnerable. Therefore, IoT can be considered as the two-edged sword. If everything is connected to the internet so providing security to collected information is very important. To deal with this, we proposed the secure system which going to collect data from IoT device and store it into the cloud in encrypted format so the cloud provider, or any other person will not be able to see the information. And also we are going to use role based access control policy for providing access to the correct user. In the proposed system, AES algorithm is used with 128 bit key to encrypt as well as to decrypt the collected data. This is symmetric key cryptography algorithm which is more secure to the IoT data uploaded on the cloud. The secure cloud storage system is designed using asp.net. Here we are going to use public cloud to store the encrypted data for that we have taken the instance of Microsoft azure cloud and the private cloud is used to store the entire user details and his credentials used to access the designed system. The credentials of the system users also stored in encrypted format using the same algorithm that is AES. The private cloud is designed using windows server 2012 with i3 processor and 4 GB ram.

In the proposed Architecture, IoT devices are placed to collect the data, if devices are not able to connect to the internet and cannot transfer the data, then gateways are used as intermediate between things and cloud to provide the needed connectivity. In the designed secure system, the administrator will define the roles according to the job functionalities played in the organization, then he/she adds the user in the system who wants to access the stored data from the cloud storage according to their needs. Administrator also create one role manager and give access rights to manage the roles of the user. The Role Manager allocates the specific roles to the user and has authority to remove the role assigned to the user. After that, the collected data from devices are encrypted by the administrator and stored it in to the cloud storage for the particular role so that only the users with appropriate roles can decrypt and view this data. The data collected from IoT devices is stored in encrypted format, therefor cloud provider is not able to see or read this data.

Basically, there are two types of cryptography algorithm. First symmetric key cryptography algorithm, in which same secret key is used for data encryption and decryption and Second asymmetric-key cryptography algorithm,
in which one key is used for encryption and second one is used for decryption. In symmetric-key cryptography algorithms, the AES is more popular and used algorithm for large data. This algorithm need low RAM for processing therefore it gives high speed. The AES uses the same secret key for encryption as well as decryption purpose, due to that the secret key needs to transfer securely sender side to receiver side. As compared to symmetric-key algorithm, Asymmetric-key algorithm such as RSA does not having any problem to exchange the key\(^{14–17}\). For solving the issue of key transport and to obtain the high performance AES and RSA algorithm was combined together. In implementation, asymmetric-key algorithm that is RSA is used only to encrypt the symmetric key, for this it requires negligible computational cost. To encrypt and decrypt the collected data Advanced Encryption Standard (AES)\(^{19}\) algorithm is used, AES is symmetric key algorithm whatever the key generated by this algorithm, this key also be encrypted to transfer the key securely and for that RSA algorithm\(^{20}\) is used. In the proposed system, Role based access control mechanism is applied for authenticating users and for providing access to uploaded files. Administrator adds the roles in the system, for each and every role one public key and the private key is generated using RSA algorithm. This public key is used to encrypt the secret key generated after the encryption of the data and private key is given to the user who having this role. If the user wants some data he/she has to request for the cipher text from the public cloud then he has to use the private key to decrypt the symmetric key generated by AES for decrypting the cipher text. Working of the proposed methodology is given below. AES algorithm having four stages Add round key, Substitute bytes, Shift rows and Mix Columns. The algorithm starts with Add Round Key stage. After this, 9 rounds of the above four stages are executed then the tenth round of three stages is executed. The last round does not execute the Mix Columns stage. Working of AES cryptographic technique is shown in Fig. 3. The inverse procedure is followed for decryption purpose. While decryption the first nine rounds are executed with Inverse Shift rows, Inverse Substitute bytes, Inverse Add Round Key and Inverse Mix Columns. Similarly, the tenth round will not execute the Inverse Mix Columns stage. For more details see\(^{18}\). RSA is used for encryption and decryption of secret key, which is generated by the AES algorithm.
Table 1. Testing Result of the Implemented Scheme.

<table>
<thead>
<tr>
<th>Input Size in MB</th>
<th>Intel Core 2 Duo (Time in min) (t)</th>
<th>Intel Core i3 (t)</th>
<th>Intel Core i5 (t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10–20</td>
<td>0.56</td>
<td>0.36</td>
<td>0.26</td>
</tr>
<tr>
<td>20–30</td>
<td>1.2</td>
<td>0.58</td>
<td>0.41</td>
</tr>
<tr>
<td>50–60</td>
<td>1.34</td>
<td>1.12</td>
<td>0.59</td>
</tr>
<tr>
<td>100–110</td>
<td>1.8</td>
<td>1.6</td>
<td>1.05</td>
</tr>
<tr>
<td>200–210</td>
<td>3.2</td>
<td>1.89</td>
<td>1.12</td>
</tr>
<tr>
<td>400–410</td>
<td>6.1</td>
<td>2.9</td>
<td>1.7</td>
</tr>
<tr>
<td>500–510</td>
<td>7.3</td>
<td>3.45</td>
<td>1.8</td>
</tr>
<tr>
<td>600–620</td>
<td>7.9</td>
<td>3.86</td>
<td>2.1</td>
</tr>
<tr>
<td>700–730</td>
<td>8.2</td>
<td>5.29</td>
<td>2.9</td>
</tr>
<tr>
<td>800–840</td>
<td>8.8</td>
<td>6.1</td>
<td>3.08</td>
</tr>
<tr>
<td>900–1000</td>
<td>9.3</td>
<td>6.9</td>
<td>3.2</td>
</tr>
</tbody>
</table>

while encrypting the data. Let us consider $S$ is the secret key and $C$ is the cipher key, then at encryption $C=S \mod n$ and at decryption side $S = C \mod n$. $n$ is the very large number which is created during the key generation process.

4. Analysis of Implemented Scheme

4.1 Testing result of the implemented scheme on different configuration

The popular secret key algorithm that is AES with RSA was implemented together. Performance of the said algorithm is calculated by applying encryption on different files, which are of different sizes and contents. The algorithm was tested on three different machines.

4.2 Comparative analysis of different cryptographic techniques

Following table shows the performance of cryptographic algorithms in terms of encryption time. Here, it compares the time for encryption of DES, AES, AES and RSA algorithm on the different packet size on I3 system having 2 gb
Table 2. Comparative Analysis of Different Cryptography Techniques.

<table>
<thead>
<tr>
<th>Input Size in KB</th>
<th>DES (t)</th>
<th>AES (t)</th>
<th>AES-RSA (t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>25.0</td>
<td>14.2</td>
<td>16</td>
</tr>
<tr>
<td>557</td>
<td>58.2</td>
<td>38.2</td>
<td>52.38</td>
</tr>
<tr>
<td>50–60</td>
<td>1.34</td>
<td>1.12</td>
<td>0.59</td>
</tr>
<tr>
<td>1024</td>
<td>110.0</td>
<td>72.2</td>
<td>99.0</td>
</tr>
<tr>
<td>5120</td>
<td>542.3</td>
<td>1362.2</td>
<td>488.1</td>
</tr>
</tbody>
</table>

Fig. 5. CPU Utilization Based on the Number of Users.

RAM. AES gives better security but AES uses the same key for encryption and decryption, and in AES there is issue of key transportation. To overcome the problem of key transportation, AES and RSA cryptographic techniques are merged together. It is observed that after merging this two algorithm, AES and RSA require more time than AES but gives higher security. In the integrated AES-RSA approach RSA is used to encrypt key used in AES. This is an additional task introduced in AES.

4.3 CPU utilization of implemented scheme based on number of users

Implemented scheme tested to find out CPU utilization based on number of users accessing the system. The following figure shows the results.

5. Conclusions

This system, addresses the security issues in a cloud storage environment. The presented approach, allows an organization to upload IoT data securely in a public cloud, while organizational information stored on a private cloud. The implemented approach provides great efficiency during encryption and decryption of the message. The implemented system is useful in various commercial organizations, where data is collected from IoT devices and job functionalities are divided according to the roles played by the user in organizations. The collected data from IoT devices is securely uploaded on cloud storage by enforcing AES and RSA cryptographic techniques.
References


