CHAPTER 7

INTEGRATION OF WSN WITH CLOUD COMPUTING

7.1 INTRODUCTION

Wireless Sensor Networks are characterized by distributed, dynamic, small, low cost, self-organizing and independent battery powered embedded devices called sensor motes. They are equipped with on-board modules with extreme resource constraints in computing, memory, power and communication ability. These sensor motes can be deployed in any hostile environment to obtain the physical information as sensor data. This information is forwarded to the gateway or the base station for further interpretation and processing to visualize the real time scenario. Wireless Sensor Networks are now employed in various application domains such as emergency and health care monitoring, environment and disaster monitoring, transportation monitoring, e-governance, surveillance and military monitoring, precision agriculture, industrial automation, and various location tracking systems.

Accumulation of the abundantly available sensory data from various WSN applications into an interpretable form under unanimous roof and visualizing the same at anytime, anywhere by any potential user (Concept of IoT) is possible only with virtually unlimited scalable resource. This is made possible with cloud computing infrastructure. Imparting intelligence is feasible not only to computers but also to all real world object by the integration of wireless sensor networks with cloud computing. The proposed
Integrated Cryptographic Network Architecture (ICNA) provides smart connectivity between existing limited resource networks with resource enriched infrastructure. This in turn leads to scalability in terms of data storage and processing power as well as accessibility to information from any location with optimized resources paid as on-demand utility (Patil et al. 2014; Buyya et al. 2009; Jensen et al. 2009; Koyama et al. 1992).

Cloud computing provides software, platforms and infrastructure over internet and satisfies the growing demand for storage and data processing needs of WSN applications. In order to make the efforts of researchers true and enhance the confidence level of the beneficiaries, the following threats in cloud computing have to be addressed:

Cloud Security and privacy

- Data lock-in, Multi-tenancy
- Data management
- Service portability
- SLA management
- Performance prediction

From the survey conducted by the IDC enterprise panel, it is clear that the significant barrier to cloud environment can be overcome only when the information security and privacy issues are addressed though the solution to other stake issues listed above come into existence. An attempt is made to provide unique security solution which addresses not only the fundamental requirements of confidentiality, Integrity and availability of the outsourced data but also to provide the best access control policy to the attributes of the data. In this proposed work, the privacy and security issues are investigated.
and a specific scalable secure solution that can be adopted for the data security requirements of the consumers is presented.

7.2 BACKGROUND

Cloud computing is a paradigm shift in the field of computing that has achieved a major transition from parallel computing, distributed computing, grid computing, utility computing and autonomic computing. Similar to various consistent, pervasive and inexpensive public utilities such as water, electricity, telephone and gas, a prominent migration towards utilizing the computing services as an on-demand utility is gaining momentum in the recent years. In the wake of any small enterprise, change from laborious management, maintenance of dynamic and automated control of systems, data and workload in terms of IT cost and time involved in a large organization to easy access of IT resources and data storage is provided on-demand. In addition, this environment promises its users computing services as on-demand utility with increased scalability, high availability, broad network access, reliable location independence, good sustainability and reduced financial burden on administration and maintenance. Despite the potential benefits, the cloud computing model has a lot of challenges and issues concerning the adoption, growth and policy making.

7.3 PROPOSED ICNA ARCHITECTURE

The main functions of the proposed architecture can be listed as follows:

- Secure storage of colossal data from WSN
- Availability of this information to any users viewing through web pages with smart phone, laptops, desktops etc.,
- Controlling the application of WSN through web pages.
- Management, loading or updating of applications in WSN monitoring environments using cloud services through the WSN gateway which communicates with individual nodes in the Network.

Out of the listed functionalities the implementations of the first two has been taken care by the design of the proposed architecture whereas the extensions for the rest of the functionalities are yet to be focused. The Integrated Cryptographic Network Architecture is as shown in Figure 7.1.

**Figure 7.1 Integrated Cryptographic Network Architecture**

The architecture comprises the stake holders such as data owners, data consumers, storage as service and the trusted authority. The data owner comprises the sensor nodes and the gateway. The sensor nodes are individual resource constrained embedded devices which are loaded with operating system components and network management components and application
programs to collect, process and transmit data through wireless communication channels to the gateway. The Routing Protocol plays a vital role in accommodating the network characteristics and managing the self-organizing topology of the network. The WSN gateway is the aggregator of the data file which can be stored only in a resource-full environment due to the abundance of the available real time data. Security of the outsourced data is the prime task of the proposed architecture. The data consumer can access the data stored in the cloud server using any device such as smart phone, laptop, tablet, desktop etc. The Infrastructure as a service model is utilized for data storage as a service with the cloud computing environment.

7.3.1 Authentication Mechanism

The trusted authority (TA) is the apex management body in the hierarchical structure of system users. TA is responsible for strong authentication by using Single Sign-On mechanism and a One Time Password logic. The Single Sign-On mechanism provides accessibility to cloud storage for any application or service information with a single login identity. The registration procedure is coupled with the session key distribution phase with the help of the KMC using the One Time Password (OTP) method which is highly personalized utilizing the other network/web services. The access policy is controlled by the policy manager upon receiving authorization from the owner of the data who decides the access tree structure.

7.3.2 Key Management Centre (KMC)

The Key Management Centre is responsible for providing the One Time Password, maintaining the generation and distribution of necessary symmetric keys, private keys and public keys in the designated files. Separate protection of these keys using password protect functions which encrypt the
keys with passwords and are decrypted on the fly to the corresponding user. The steps involved by the KMC are clearly depicted in the sequence diagram.

### 7.3.3 Policy Manager

The policy manager provides the option in the access policy as either fine grained or coarse grained access control to vary the level of privacy achieved depending on the requirement. It is an access policy that decides who can access to what and what portion of the information can be revealed. The data owner decides the attributes of the data that can be accessed by any user, depending on which a hierarchical access tree structure (T) is created and can be seen as a logical expression combining several attributes through AND, OR or other operators. Each non-leaf node of the tree represents a threshold gate, described by its children and the threshold gate value (AND, OR or other operators). Each leaf node of the tree is described by an attribute from universal attribute set U and a threshold value.

### 7.3.4 Encryptor/Decryptor

The Encryptor/Decryptor consists of a set of cryptographic credentials such as AES, SHA, RSA with Digital signature, ECC with Digital signature. The data owner can choose any one of the credentials for encryption depending on the level of security needed for a particular application. The symmetric and asymmetric keys are generated by KMC and are distributed to the authenticated user. The comparative study (Abdul et al 2008; Cohen et al 2005; Nadeem & Javed 2005) based on various factors such as key size, block size, cryptanalysis resistance makes clear that AES is a fast and efficient encryption algorithm among the Symmetric key algorithms. Also RSA and ECC algorithms are chosen among the various Asymmetric key counterparts. The ECC algorithm has a high level of Confidentiality, Integrity and availability compared to RSA (Canetti et al 2003; Chou 2003; Golle et al
The user have a choice of selecting the algorithm depending of the level of CIA needed for the protection of the data.

Finally the encrypted data is stored in the cloud storage. The user after successful completion of the registration and authentication process can request access to data which is possible only when the keys are distributed by the KMC. This is carried out after verifying the authentication server and the policy manager. The data can be retrieved from the cloud storage using the decryption algorithm with the received key. The above mentioned steps involved in establishing security and privacy of the data in cloud storage are depicted clearly in Figure 7.2.

![Figure 7.2 Sequential diagram for ICNA](image-url)
7.4 IMPLEMENTATION

In the proposed architecture, the individual applications are installed as individual web services in a set of 6 desktop PC with Pentium 4, 3.00GHz CPU and 8GB memory. The systems are internetworked in client–server model and are operated to establish a cloud scenario using Microsoft Visual Studio 2012 and SQL server. Each PC access the web service from different application domains such as transport monitoring, environment monitoring and healthcare monitoring gateway. Separate server for Authentication and policy adoption is also implemented and the execution time for key generation, key updation, encryption/decryption time is calculated and the results are obtained. The key encryption and decryption time is also calculated for various key sizes of the cryptographic engines. The several attributes of each customer is encrypted using fine grained access Attribute Based Encryption in a hierarchical manner using various cryptographic engines.

7.5 RESULTS AND DISCUSSION

![Figure 7.3 Comparison of Key Generation Time Vs No. of users with various Cryptographic algorithms](image-url)
The key generation time vs No. of users accessing the data at a particular instant of time using the various cryptographic credentials such as AES, RSA, SHA, and ECC algorithm is illustrated in Figure 7.3. The type of cryptographic algorithm is chosen by the data Owner/Consumer for encryption and decryption of data before storage in the cloud. It clearly depicts that the key generation time is comparatively less for ECC than RSA among the asymmetric key algorithms and SHA algorithm is used for Digital signature to be coupled with RSA and ECC. AES is the symmetric key algorithm whose key generation time is less compared to RSA. The execution of these algorithms is carried out for a particular key size decided by the equivalence in the level of security.

![Comparison of Key Updation Time Vs No. of users with various Cryptographic algorithms](image)

**Figure 7.4** Comparison of Key Updation Time Vs No. of users with various Cryptographic algorithms

The Figure 7.4 shows the time required for key updation with the same set of users at a particular instant using the various cryptographic credentials. It is clear that the key updation time is very less for RSA.
algorithm compared to the other encryption/decryption algorithms for the same chosen key size as that of key generation due to fixed keys.

Figure 7.5  Comparison of Encryption Time Vs Data file Size with various Cryptographic algorithms

Figure 7.6  Comparison of Decryption Time Vs Data file Size with various Cryptographic algorithms
The Figure 7.5 and Figure 7.6 shows the encryption/decryption time needed for data files of various sizes for the cryptographic algorithms considered. Though the required time is less for RSA algorithm due to fixed keys, ECC algorithm is best suited due to small key size and key generation time is less compared to RSA algorithm. AES algorithm can be chosen with symmetric key distribution wherein recent research findings of dynamic key management algorithms can be adopted to achieve high security strength.

7.6 SUMMARY

Even though Cloud Computing is a promising Industry of revenue these days, the data security and privacy issues need to be solved to make the dream true. Typical e-commerce systems such as health care and universal banking facilities make a stress in developing a secure scenario with access control. A step towards the solution of these issues is effectively addressed by the proposed architecture. The performance-expressivity results show that as the data size and number of users at particular instant increases, the time complexity also increases there by. Apart from the implementation of this secure architecture; sabotage of physical hardware and communication channels must also be avoided by providing physical security to cloud storage sites that may vary among the service providers.