Secure Storage for the Data Extracted from the Wireless Sensor Network with Cloud

Athira .M .S[1], Madhu .N[2],

[1]M. Tech, 4th semester CSE, AIT, Bangalore, India

[2]Assistant Professor, Department of Computer Science & Engineering, AIT, Bangalore, India

Abstract: ***WSN have several applications in different domains including home automation, healthcare, environmental monitoring, business etc. But the gathered information is not used adequately because of the lack of expertise and storage for further use. To overcome this problem collected information is transformed in to a valuable resource like cloud and providing a reliable system for the access of the information. a new framework is proposed for WSN integration with Cloud computing model, existing WSN will be connected to the proposed framework. This framework enhances the wireless sensor applications by integrating sensor networks with the cloud technology. The integration controller unit of this proposed framework integrates the sensor networks with cloud computing and provide a secure storage and computational capability for the stored data. The resultant system offers reliability, availability and extensibility.***

Keywords: Wireless Sensor Network; Cloud computing; Integration Framework; Security Algorithm

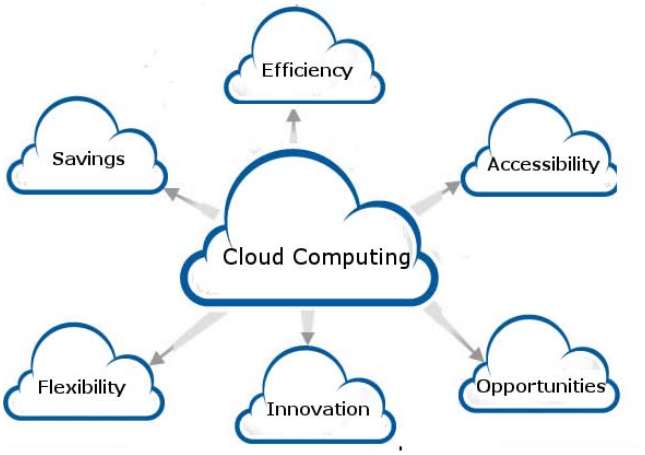
1. Introduction

Wireless sensor network is used in many fields. Research on sensor networks started around 1980 with the Distributed Sensor Networks (DSN) program at DARPA (Defense Advanced Research Projects Agency) [3]. Where Arpanet (predecessor of the Internet) approach for communication was extended to sensor networks. In 1997 IEEE allocated some registered bands for the wireless communications. Wireless sensor network consist of several sensors capable of sensing, computation, and wireless communication. Each sensor nodes have mainly 4 parts, one microprocessor , at least one sensor and transceiver ,a power source. Sensors in the wsn collect a huge amount of data but this data is not used adequately because of the lack of storage and expertise. To overcome this problem we integrate the wireless sensor networks with cloud technology. Cloud Computing is principally designed and promoted to be data centre centric and efficient interaction with the outside world is an area where improved solutions are being sought. WSN are designed to collect data in the real world [6]. There is a possible linkage between WSN and Cloud Computing and the eventual shift of data into the cloud and over time into the public domain.

WSN architecture could be either centralized or distributed [4]. In centralized architecture the central node is the weak point of the network. If it fails, whole network fails. But, distributed architecture provides failure resistant sensor network. Wireless sensor networks design constraints are application specific and dependent on monitored environment. Based on the monitored environment, network size in WSN varies. For monitoring a small area, fewer nodes are required to form a network whereas the coverage of a very large area requires a huge number of sensor nodes. For monitoring large environment, there is limited communication between nodes due to obstructions into the environment, which in turn affects the overall network topology (or connectivity) [1]. All these limitations on sensor networks would probably impede the service performance and quality. The key constraints of the WSN short communication range, communication security privacy, limited storage, and computational capability [5]. Here in this paper integration controller transferring the data to the cloud and providing computational capability for the data and a secure storage for the computed data.

2. Cloud Computing

Cloud computing can be defined as 'a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned, and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers' Some of the examples for emerging Cloud computing infrastructures/platforms are Microsoft Azure, Amazon EC2, Google App Engine, and Aneka



There are mainly 4 types of clouds they are public cloud, private cloud, hybrid cloud and community cloud. Private cloud that operates with in the firewall of an organization, access is limited to only the authorized user. But public cloud that provides an infrastructure for general use. Hybrid cloud is the combination of both the public cloud and private

cloud. Community cloud is used by a set of organizations sharing the same community.

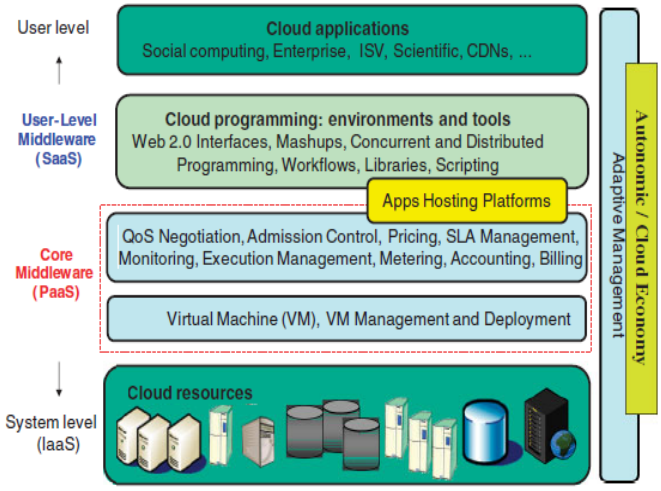


Figure 2: Layered cloud computing architecture

IBM report stated that "Cloud is a new consumption and deliver model for many IT-based services, in which the user sees only the service, and has no need to know anything about the technology or implementation". NIST classify the cloud computing as "Cloud computing is a model for enabling convenient, on demand network access to shared pool of configurable computing resources" [14].

The cloud computing have three architecture layers mainly Software-as-a-Service SaaS), Platform-asa-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Figure 2 shows the layered design of Cloud computing architecture. Physical Cloud resources along with core middleware capabilities form the basis for delivering IaaS and PaaS. The user-level middleware aims at providing SaaS capabilities. The top layer focuses on application services (SaaS) by making use of services provided by the lower-layer services. PaaS/SaaS services are often developed and provided by third-party service providers, who are different from the IaaS providers [10]

Cloud applications: This layer includes applications that are directly available to end-users. We define end-users as the active entity that utilizes the SaaS applications over the Internet. *User-Level middleware*: This layer includes the software frameworks, such as web 2.0 Interfaces (Ajax, IBM Workplace), that help developers in creating rich, cost-effective user-interfaces for browser-based applications. SaaS provides board market solutions where the vendor provides access to hardware and software products through portal interface [4].

Core middleware: This layer implements the platform-level services that provide run-time environment for hosting and managing User-Level application services. The core services at this layer include Dynamic SLA Management, Accounting, Billing, Execution monitoring and management, and Pricing (are all the services to be capitalized?). The well-known examples of services operating at this layer are Amazon EC2, Google App Engine, and Aneka. PaaS supplies all the resources required to build an applications and services completely from the internet without having to download or install the software. Paas include application design development, testing and deployment and hosting.

System Level: The computing power in Cloud environments is supplied by a collection of data centers that are typically installed with hundreds to thousands of hosts. At the System-Level layer, there exist massive physical resources (storage servers and application servers) that power the data centers. These servers are transparently managed by the higher-level virtualization services and toolkits that allow sharing of their capacity among virtual instances of servers. These VMs are isolated from each other, thereby making fault tolerant behavior and isolated security context possible. IaaS provides consumers with an opportunity to consume processing, storage, network, and other fundamental computing resources. Here the consumer is able to store data, deploy and run arbitrary software such as operating systems and applications [14]. The consumer does not need to control and manage the underlying infrastructure but has control over the operating system, applications, storage, and network components.

The data collected by the wireless sensor network is transferring to cloud for storage. The Sensor-Cloud collects and processes information from several sensor networks, enables information sharing on big scale, and collaborates with the applications on cloud among users. It integrates several networks with a number of sensing applications and cloud computing platform by allowing applications to be cross-disciplinary that may span over multiple organizations [15].

3. Proposed Frame Work Overview

The major components of the framework are Data Processing Unit (DPU), Data Broker, Request Subscriber, Identity and Access Management Unit (IAMU) [18] and Data centre (DC). The data that collected by the sensors are passed through a gateway to the DPU. The DPU that converts the data in to the storage format and store the data in to the data centre. Data that received are segregated and stored in different file. This file index is transferred to the registry as well as to the event queue in the data broker .Users will connect to the Cloud through the secured IAMU (Identity and Access Management Unit). This will provide both authentication and access control. The IAMU systems have two major components: Access Control Enforcement Unit (ACEU); and Access Control Decision Unit (ACDU). ACEU is used to authenticate the user and it consists of Edge Node (EN) and three servers i.e. Authentication Server (AS), Ticket Granting Server (TGS) and Service Server (SS). The request received by EN is sent to AS. EN implements Kerberos [13][15] in order to authenticate the user with AS. ACDU is used to enforce the policy rules. It consists of RBAC (Role Based Access Control) processor and policy storage. It communicates with ACEU through SS [16]. After successful authentication; user is given the access to the resources as constrained by the access policies. Now the user can send the data request. This request is forwarded to the Request Subscriber (RS). RS will create a subscription on the basis of this request and forward this subscription to the data Broker. The data Broker compares each subscription with the file index in the event queue. If data Broker finds any subscription matches, it will start retrieving

data from the DC and forward the data to the user via the RS and the Cloud thread. Authorized users are not allowed to make any changes to the stored data. Secure storage is provided to the data using security algorithm [15]. According to the user's request the computations are possible on the cloud environment. We can store the computational result as well as the original data for the future scientific and economical purpose.

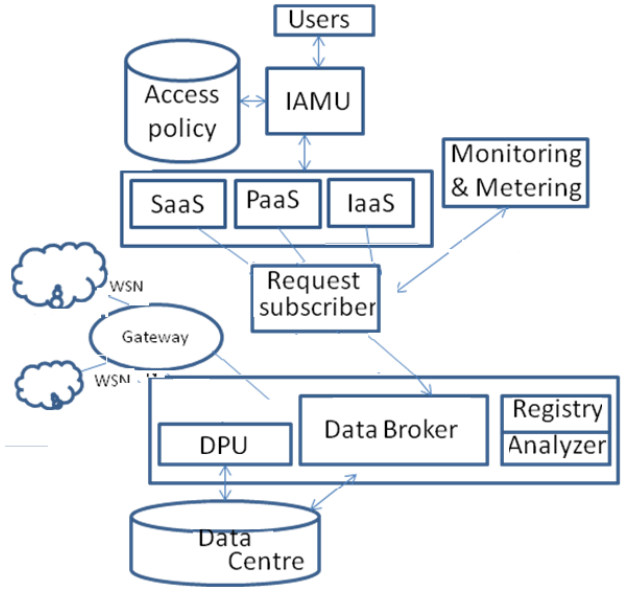


Figure 3: Sensor Cloud Integration Framework

This article presents a framework which integrates cloud computing and WSN. The objective is to facilitate the shift of data from WSN to cloud computing storage so that it may be further utilized in scientific and economic analysis. The proposed system suggests that sensor nodes and Integration Controller (lC) can interact through SOA. Sensor nodes are considered as service providers and sink nodes are consumers, they receive information through Ic. The sensor nodes are deployed into the application server as service description. It has location information and provides a service end point, a target namespace and a transport name. These components exchange messages in xml format.

A. Access Control Enforcement Unit

ACEU is used to authenticate the user and it is consists of EN and three servers i.e. AS, TGS and SS. The request received by EN is sent to AS. EN implements Kerberos in order to authenticate the user with AS [16].

B. Access Control Decision Unit

ACDU is used to enforce the policy rules. It consists of RBAC processor and policy storage. It communicates with ACEU through SS. After successful authentication; user is given the access to the resources as constrained by the access policies.

C. Communication flow between User and IAMU.

The description of different messages those have been exchanged among different servers and edge node (EN) are left out of the scope of this poster due to the space constraint.

IAMU includes Diffie-Hellman, Kerberos, Role Based Access Control and XML [15][12]. The main rationale of this model is first, to provide authentication between consumer and cloud provider. Second, to provide policy based access control over the cloud resources. Consumers directly communicate IAMU for authentication and access control. Access Control Enforcement Unit (ACEU) and Access Control Decision Unit (ACDU). Edge Node (EN) is used as replacement of kerberos. It is actually based on Kerberos with slight modifications. It also implements Diffie-Hellman public key [14].

4. Flow of Interaction among Framework Components

The user attempts to login by sending login information:

1) IAMU will authenticate the user and sends ACK if the authentication is successful.
2) After successful login the user will send a service access request.
3) Cloud thread will identify the service type and generate a corresponding request message.
4) Cloud will then send the request message to Request subscriber (RS).
5) RS will unify the request and create a subscription on the basis of the request received from Cloud thread.
6) Then the RS will send this subscription to the PUB/SUB Broker.
7) DPU will continuously send index of the data to the PUB/SUB broker. This event can happen at any point.
8) PUB/SUB broker will store all of the data indexes in its registry.
9) Immediately after receiving a subscription request from RB, Pub/Sub Broker will start EM to find the matched published data for this particular subscription.
10) If Pub/Sub Broker finds any subscription match it will start retrieving data from the DPU.
11) Retrieved data will be forwarded to the user via the RS and the Cloud thread.

5. Secure Data Storage in Cloud with RSA Algorithm

Security of data has become a major concern. When data mobility is at a high level then the risks and issues increase many folds especially when data is transferred to another country with different regulatory framework. High levels of data relocation have negative implications for data security and data protection as well as data availability.

The cloud has many security issues. The authorized users are not allowed to change the data stored in the cloud. Cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

Using security algorithm we can provide security for the stored data. RSA is widely used Public-Key algorithm. User data is encrypted first and then it is stored in the Cloud. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas

Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

5.1 Key Generation

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps
Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.

1) Compute n = a * b.
2) Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
3) Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.
4) Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).
5) d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
6) The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
7) The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

5.2 Encryption

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:
1) Cloud service provider should give or transmit the Public-Key (n, e) to the user who wants to store the data with him or her.
2) User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3) Data is encrypted and the resultant cipher text (data) C is C = me (mod n).
4) This cipher text or encrypted data is now stored with the Cloud service provider.

5.3 Decryption

Decryption is the process of converting the cipher text (data) to the original plain text (data).

Steps
1) The cloud user requests the Cloud service provider for the data.
2) Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e., C.
3) The Cloud user then decrypts the data by computing, m = Cd (mod n).
4) Once m is obtained, the user can get back the original data by reversing the padding scheme.

6. Conclusion

Integration of WSN with Cloud Computing will provide secure storage and computational capability for huge amount of data from wireless sensor network benefits to organizations and the research community. Organizations will benefit by utilizing Cloud storage and an optimized framework for processing, storage and retrieval of WSN generation data. This framework will provide an optimal approach to user management, access control, storage and retrieval of distributed data.

References

[1] Sajjad Hussain Shah, Fazle Kabeer Khan, Wajid Ali, Jamshed Khan; New Framework to Integrate Wireless Sensor Networks with Cloud Computing ,Aerospace Conference, 2013 IEEE
[2] Secured WSN-integrated Cloud Computing for u-Life Care IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2010 proceedings.
[3] Chien-Chung Shen, Chavalit Srisathapornphat, Chaiporn Jaikaeo; "Sensor Information Networking Architecture and Applications"; IEEE Personal Communications, pp. 52-59, August 200 I.
[4] Sarjoun S. Doumit, Dharma P. Agrawal; "Self-Organizing and Energy Efficient Network of Sensors"; IEEE, pp. 1-6, 2002.
[5] Elaine Shi, Adrian Perrig; "Designing Secure Sensor Networks"; IEEE Wireless Communications, pp. 38-43, December 2004.
[6] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci; "A Survey on Sensor Networks"; IEEE Communications Magazine, pp. 102-114, August 2002. [27] (2006, October).
[7] Kay Romer, Friedemann Mattern; "The Design Space of Wireless Sensor Networks"; IEEE Wireless Communications, pp. 54-61, December 2004
[8] Wendi B. Heinzelman, Amy 1. Murphy, Hervaldo S. Carvalho, Mark A. Perillo; Middleware to Support Sensor Network Applications"; IEEE Network, pp. 6-14, January/February 2004.
[9] Jaeger, T. ; Pennsylvania State Univ., University Park, PA, USA ; Schiffman, J., "Outlook: Cloud Computing with a Chance of Security Challenges and Improvements," IEEE Computer and Reliability Socities 2010, pp. 77-80, Jan. 2010.
[10] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, C´esar A. F. De Rose and Rajkumar Buyya. "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms" Published online 24 August 2010 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/spe.1995.
[11] Jaeger, T. ; Pennsylvania State Univ., University Park, PA, USA ; Schiffman, J. "Outlook: Cloud Computing with a

[12] Chance of Security Challenges and Improvements," IEEE Computer and Reliability Socities 2010, pp. 77-80, Jan. 2010.
[13] Nils Hoeller, Christoph Reinke, Jana Neumann, Sven Groppe, Daniel Boeckmann, Volker Linnemann, "Efficient XML Usage within Wireless Sensor Networks" WICON '08, November 17-I 9, 2008, Maui, Hawaii USA.
[14] (2011) Wikipedia- Kerberos Protocol. [Online]. Available: http://en.wikipedia.org/wiki/Kerberos_(protocol).
[15] R. Marchany. (2010) VA Tech IT Security Cloud computingissues[online].available:http://www.security.vt.edu/Downloads/training/Cloud%20Computing%20Security%20Issues.pdf.
[16] (1993) RSA Laboratories. PKCS #3: Diffie-Hellman Key-Agreement Standard, Version 1.4.Revised November 1, 1993. [Online]. Available: http://www.rsalabs.com/pkcs/pkcs-3/index.html.
[17] (2011) Kerberos: The Network Authentication Protocol. [Online].Available: http://web.mit.edu/kerberos.