

# A New Framework to Integrate WSN with Cloud Computing and Security Using Dynamo DB

Lalleshwari. B. P  
Dept. of CSE  
SJBIT, BANGALORE-560060  
KARNATAKA, INDIA  
Lalleshwari2812@gmail.com

Sunitha. K., asst. prof  
Dept. of CSE  
SJBIT, BANGALORE-560060  
KARNATAKA, INDIA  
ksunitha@sjbit.edu.in

**Abstract**-Wireless sensors networks have several applications of their own. These applications can be further enhanced by integrating a local wireless sensor network to internet, which can be used in real time applications where the results of sensors are stored on the cloud. We propose an architecture that integrates a wireless sensor network to the internet using cloud technology. The resultant system is proved to be reliable, available and extensible. In this paper a new framework is proposed for WSN integration with Cloud computing model, existing WSN will be connected to the proposed framework. Three deployment layers are used to serve user request (IaaS, PaaS, SaaS) either from the library which is made from data collected from data centric DC by WSN periodically. The integration controller unit of the proposed framework integrates the sensor network and cloud computing technology which offers reliability, availability and extensibility.

**Keywords**-Saas, Paas, IaaS, Dynamo DB

## I. INTRODUCTION

The idea of wireless networks was developed by sending messages through fire and smoke. It was a sign of presence of people in specific territory. In 80's researches came up with the idea of TNC (Terminal Node Controller). The aim of this invention was to communicate between a computer and radio, but desired performance was not achieved. Later on in 1985 FCC (Federal Communication Commission) allocated ISM bands for different applications. The assigned ISM bands were 902 MHz and 5.85 GHz. and access was limited to licensed users. Wireless Sensor Network (WSN) consists of wireless communications. The nodes are connected in ad hoc fashion, operating independently of other nodes. There are various factors associated with the performance of WSN such as power management, data dissemination and routing of information. A lot of work has been undergoing in these areas where energy awareness of essential design issue; routing and data dissemination is application dependent. WSN architecture could be either centralized or distributed. In centralized architecture the central node is the weak point of the network. If it fails, whole network collapse. However, distributed architecture provides failure resistant sensor network [1]. Comprehensive architecture and various wireless sensor applications emergence is represented and discussed as we can

see in the Figure 1. distributed nodes with the capability of sensing, computation

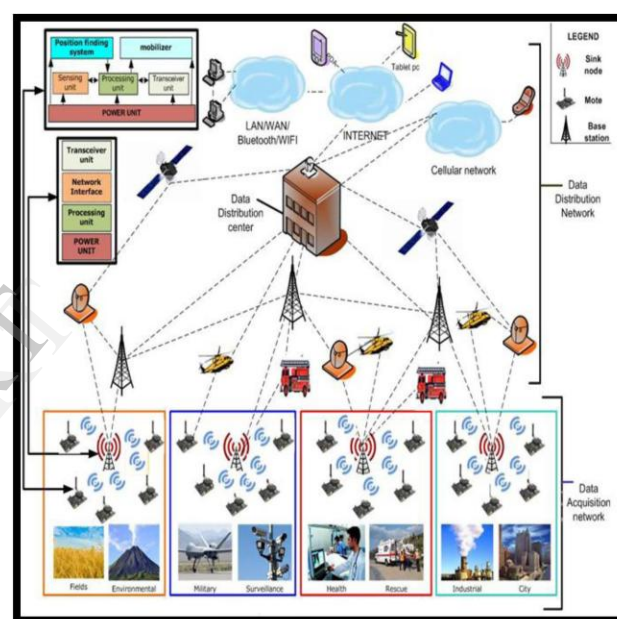


Figure 1: Emergence of Wireless Sensor Network in Various Applications

## A. Issues in Wireless Sensor Network

Ad hoc network inherited some of the tribulations of wireless communication networks like lossy links, unreliable time in varying and asymmetric channel, hidden node and exposed node and improperly defined coverage boundary. Ad hoc network puts a messy contribution in this knotted portfolio in the form of multi hop environment, location awareness, and node mobility, dynamically changing topology, vulnerability of channel and nodes and different aspects in QoS. Specifically in WSN, in addition to most of the aforementioned issues, network partitioning, localization, calibration, data fusion, aggregation and dissemination, coverage issues, self-organizing and self-administration, scalability, load balancing, node clustering, topology management, end-to-end delay constraint routing, security and privacy, heterogeneity, and other energy, memory, power and bandwidth constraints are the active challenges. In the closer view, node scheduling, whole problem, avoiding and coping with void node areas, node failure and QoS relating factors are under great concentration of researchers where QoS is a level of service in

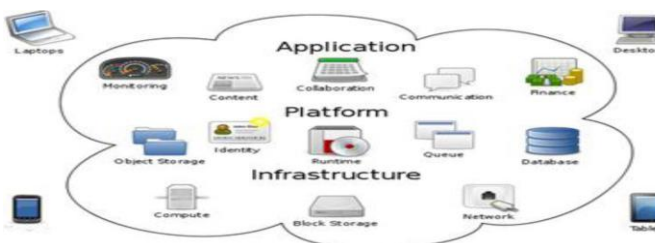
achieving the target with sufficient resources by fulfilling the requested QoS parameters. End-to-End performance, delay, bandwidth, energy consumption, transmission power, memory usage, probability of packet loss, jitter, bit error rate, miss ratio, packet overhead and packet success delivery are considered under the umbrella of QoS parameters. Real-time routing has the core importance in QoS aware network layer issues which ensures catching the destination within a limited required time and resources.

Application Area	Usage
Military	Military situation awareness [3]. Logistics in urban warfare [4]. Battlefield surveillance [5]. Computing, intelligence, surveillance, reconnaissance, and targeting systems [6].
Mobile wireless low-rate networks for precision location	Including industrial, retail, hospital, residential, and office environments, while maintaining low-rate data communications for monitoring, messaging, and control [7].
Airports	Smart badges and tags [7,3] Wireless luggage tags [7] Passive mobility (e.g., attached to a moving object not under the control of the sensor node) [8]
Medical/Health	Monitoring people's locations and health conditions [5]. Sensors for: blood flow, respiratory rate, ECG (Electrocardiogram [9] Monitor patients and assist disabled patients [6]
Ocean	Monitoring Fish [5]

Table 1: Wireless Sensor Network Applications

## II. CLOUD COMPUTING

Cloud Computing is internet based computing, where resources allocations are shared, software and information are provided to computer and all other devices on demand as requested. It is considered as an alternative to traditional server or web hosting servers. Cloud provides much more services than that, having different layer to provide application based services. [2].



Cloud Computing  
Figure 2: Overview of Cloud Computing

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" [10]. 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" [11].

### Cloud Computing Architecture Layers

- a) SaaS (Software as a Service)
- b) PaaS (Platform as a Service)
- c) IaaS (Infrastructure as a Service).

General overview of cloud computing architecture layers as we can see in the Figure 3.

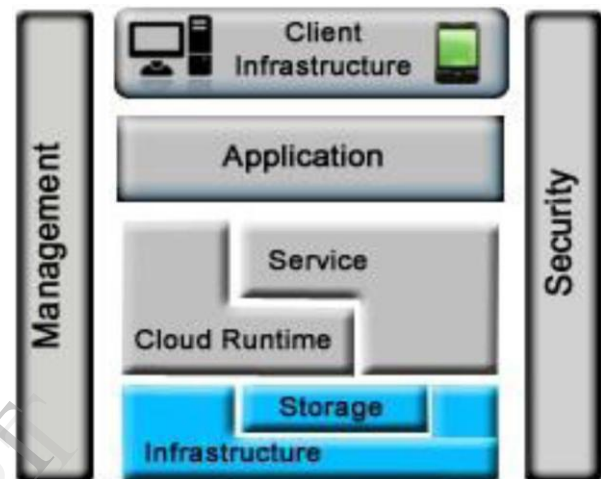


Figure 3: Cloud Computing Architecture

SaaS provides board market solutions where the vendor provides access to hardware and software products through portal interface [12].

PaaS allows the consumer to run the specified application on the platform. In these types of services, consumer has no control over the infrastructure as well as the installed applications [13], [14]. IaaS provides consumers with the benefit to consume the infrastructure that includes processing power, data storage, and network etc.

## III. LITERATURE SURVEY

The Cloud computing, coined in late of 2007, currently emerges as a hot topic due to its abilities to offer flexible dynamic IT infrastructures, QoS guaranteed computing environments and configurable software services. Cloud computing can be defined as follows: "A Cloud is a type of parallel and distributed system consisting of a collection of interconnected 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 customers and can be ubiquitously accessed from any connected devices over the internet" Cloud computing started quietly from several seeding technologies such as grid computing, virtualization, Salesforce.com innovative

subscription-based business model or Amazon's effort to scale their e-commerce platform. However, it differs from traditional ones in that:

- (1) it is massively scalable,
- (2) can be encapsulated as an abstract entity that delivers different levels of services to customers anywhere, anytime, and
- (3) it is driven by economies of scale that is the services can be dynamically.

Configured (via virtualization or other approaches) and delivered "on-demand". The Web search popularity, as measured by the Google search trends during the last 12 months, for terms "Cluster computing", "Grid computing", and "Cloud computing" is shown in Figure 1. From the Google trends, it can be observed that cluster computing was a popular term during 1990s, from early 2000 Grid computing become popular, and recently Cloud computing started gaining popularity. Meanwhile, market-research firm IDC expects IT Cloud-services spending to grow from about \$16 billion in 2008 to about \$42 billion by 2012 as Figure 2 shows. IDC also predicts Cloud computing spending will account for 25 percent of annual IT expenditure growth by 2012 and nearly a third of the growth the following year.

Cloud Computing has many benefits that the public sector and government IT organizations are certain to want to take advantage of. In very brief summary form they are as follows:

*A. Reduced cost, higher gains:*

Cloud technology is paid incrementally, saving organizations money.

*B. Increased storage:*

Organizations can store more data than on private computer systems.

*C. Highly automated:*

No longer do IT personnel need to worry about keeping software up to date.

*D. Flexibility:*

Cloud computing offers much more flexibility than past computing methods.

*E. More mobility:*

Employees can access information wherever they are, rather than having to remain at their desks. In Cloud computing, customers do not own the infrastructure they are using; they basically rent it, or pay as they use it. One of the major selling points of cloud computing is

*F. Lower costs:*

Companies will have lower technology-based capital expenditures, which should enable companies to focus their money on delivering the goods and services that they specialize in. There will be more device and location independence, enabling users to access systems no matter where they are located or what kind of device they are using. The sharing of

costs and resources amongst so many users will also allow for efficiencies and cost savings around things like performance, load balancing, and even locations (locating data centers and infrastructure in areas with lower real estate costs, for example). The general architecture of Cloud computing is shown below.

*G. No Existing Infrastructure for Integration of WSN to Cloud:*

In the past few years, wireless sensor networks (WSNs) have been gaining increasing attention to create decision making capabilities and alert mechanisms, in many Life care application areas including Life care monitoring for patients, environmental monitoring, pollution control, disaster recovery, military surveillance etc. For example, MIT wireless sensor ring can measure heart rate, heart rate variability, Oxygen saturation and blood pressure for the person wearing the ring.

Our proposed Dynamo DB can be deployed for various u-Life care services and WSN services.

#### IV. PROPOSED FRAME WORK OVERVIEW

Figure 5 shows the proposed integration framework of cloud computing and WSN. The major components of the Publisher/Subscriber Broker, Request Subscriber, Identity and Access Management Unit (IAMU) and Data Repository (DR). The data gathered from WSN is passed through gateway to DPU, which process data and add it to DR. In order to access the stored data from cloud services, user connects through secured IAMU; on successful connection established user will be given the access according to the account policies. User data request is forwarded to RS which creates a request subscription and forward the subscription to the Pub/Sub Broker. When DPU receives the data from gateway, it forwards the data to Pub/Sub Broker. When the event matches the subscription, data is made available to the respective user. There has to be effective way for user to access the data sensed by the sensors. The idea of connecting a standalone wireless network to internet is comparatively new and still is an open research area. The sensor networks are known to be pervasive and ubiquitous. It is impossible to connect each and every node to internet, as we are constrained by the IP addresses. This article proposes architecture as a solution where industrial sensor networks can be integrated with internet through cloud technology and Service Oriented Architecture (SOA). The system proposed main modules as application server, integrated controller, and a register agent. The role of integrated controller is to provide the storage as well as the recovery mechanism to the sensed data. This has been achieved by uploading the sensed data to internet using cloud services. The user can access the data from any location in the world. The sensor networks are ideally considered to be energy efficient and it's the major criticality of the network that must be answered. In addition to that, short range hop communications is preferred in order to communicate with a long range destination. Therefore, the information from source is distributed across intermediate nodes in the path towards destination node. The intermediate nodes must process the received data, aggregate it to remove duplication and to minimize the network traffic.



#### A. Access Control Enforcement Unit:

ACEU is used to authenticate the user and it 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.

#### 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.

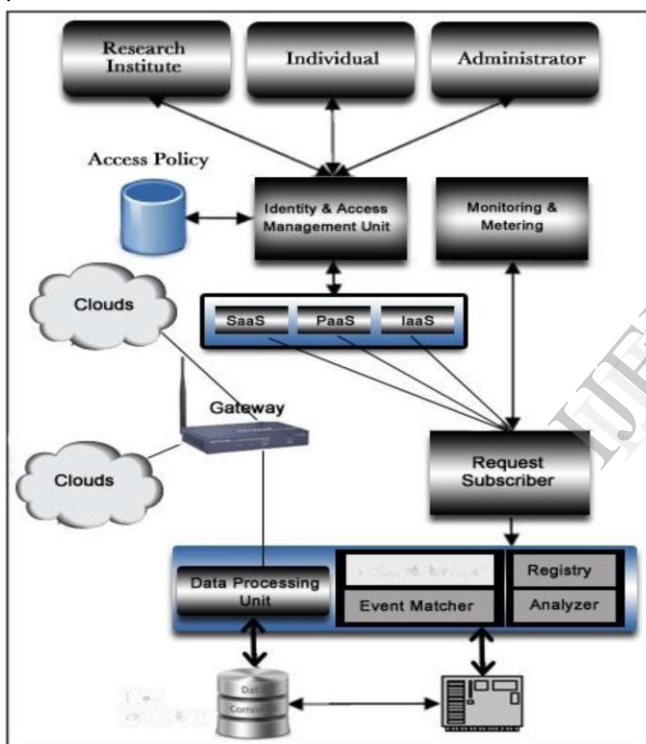


Figure 5: Proposed Architecture General Overview

## V. DYNAMO DB

Dynamo DB is a fast, fully managed NoSQL database service that makes it simple and cost-effective to store and retrieve any amount of data, and serve any level of request traffic. Its guaranteed throughput and single-digit millisecond latency make it a great fit for gaming, ad tech, mobile and many other applications.

#### A. Features and benefits:

Dynamo DB delivers seamless throughput and storage scaling via API and easy-to-use management console, so you can easily scale up or down to meet your needs. Many of our customers have, with the click of a button, created Dynamo DB

deployments in a matter of minutes that are able to serve trillions of database requests per year.

Dynamo DB tables do not have fixed schemas, and each item may have a different number of attributes. Multiple data types add richness to the data model. Secondary indexes add flexibility to the queries you can perform, without impacting performance.

Performance, reliability and security are built-in, with SSD-storage and automatic 3-way replication. Amazon Dynamo DB uses proven cryptographic methods to securely authenticate users and prevent unauthorized data access.

#### B. Scalable:

Amazon Dynamo DB is designed for seamless throughput and storage scaling.

#### C. Automated Storage Scaling:

There is no limit to the amount of data you can store in a Dynamo DB table, and the service automatically allocates more storage, as you store more data using the Dynamo DB write APIs.

#### D. Provisioned Throughput:

When creating a table, simply specify how much request capacity you require. Dynamo DB allocates dedicated resources to your table to meet your performance requirements, and automatically partitions data over a sufficient number of servers to meet your request capacity. If your throughput requirements change, simply update your table's request capacity using the AWS Management Console or the Amazon Dynamo DB APIs. You are still able to achieve your prior throughput levels while scaling is underway.

#### E. Distributed, Shared Nothing Architecture:

Amazon Dynamo DB scales horizontally and can seamlessly scale a single table over hundreds of servers.

#### F. Easy Administration:

Amazon Dynamo DB is a fully managed service – you simply create a database table and let the service handle the rest. You don't need to worry about hardware or software provisioning, setup and configuration, software patching, operating a reliable, distributed database cluster, or partitioning data over multiple instances as you scale.

#### G. Flexible:

Amazon Dynamo DB gives you the flexibility to query on any attribute using secondary indexes which have the same performance, scalability, and fault-tolerance characteristics as that of a Dynamo DB table.

## VI. SECURITY

The data owner and all of the cloud servers in the cloud share a synchronized clock, and there is no transmission and queuing delays when executing read and write commands.

### A. Intuition

The data owner will first generate a shared secret key to the CSP. Then, after the data owner encrypts each file with the appropriate attribute structure and time slice, the data owner uploads the file in the cloud. The CSP will replicate the file to various cloud servers. Each cloud server will have a copy of the shared secret key. Let us assume that a cloud server stores an encrypted file

$F$  with  $A$  and  $TS_i$ . When a user queries that cloud server, the cloud server first uses its own clock to determine the current time slice. Assuming that the current time slice is  $TS_i+k$ , the cloud server will automatically re-encrypt  $F$  with  $TS_i+k$  without receiving any command from the data owner. During the process, the cloud server cannot gain the contents of the ciphertext and the new decryption keys. Only users with keys satisfying  $A$  and  $TS_i+k$  will be able to decrypt  $F$ .

### B. Protocol Description

We divide the description of the basic R3 scheme into three components: data owner initialization, data user read data and data owner write data. We will rely on the following functions. Table II shows the notations used in the description.

1) Setup()  $\rightarrow$  (PK, MK, s) : At  $TS_0$ , the data owner publishes the system public key PK, keeps the system

#### Algorithm 1 Basic R3 (synchronized clock with no delays)

while Receive a write command  $W(F, seqnum)$  at  $TS_i$  do  
Commit the write command in order at the end of  $TS_i$   
while Receive a read command  $R(F)$  at  $TS_i$  do  
Re-encrypt file with  $TS_i$

master key MK secret, and sends the shared secret key  $s$  to the cloud.

2) GenKey(PK, MK, s, PK<sub>Alice</sub>, A, T)  $\rightarrow$  (SK<sub>Alice</sub>, {SKT<sub>Alice</sub>, A}) : When the data owner wants to grant data user Alice attributes  $A$  with valid time period  $T$ , the data owner generates SK<sub>Alice</sub> and {SKT<sub>Alice</sub>, A} using the system public key, the system master key, the shared secret key, Alice's public key, Alice's attributes and eligible time.

3) Encrypt(PK, A, s, TSt, F)  $\rightarrow$  (CtA) : At  $TSt$ , the data owner encrypts file  $F$  with access structure  $A$ , and produces ciphertext CtA using the system public key, access structure, the system secret key, time slice, and plaintext file

4) Decrypt(PK, CtA, SK<sub>Alice</sub>, {SKT<sub>Alice</sub>, a<sub>ij</sub>}<sub>1 ≤ j ≤ n<sub>i</sub></sub>)  $\rightarrow$  F : At  $TSt$ , user  $U$ , who possesses version  $t$  attribute secret keys on all attributes in  $CC_i$ , recovers  $F$  using the system public key, the user identity secret key, and the user attribute secret keys.

5) REncrypt(CtA, s, TSt+k)  $\rightarrow$  Ct+k A : When the cloud server wants to return a data user with the file at  $TSt+k$ , it updates the ciphertext from CtA to Ct+k A using the shared secret key

### CONCLUSION

Both wireless sensor network and Cloud Computing technologies along with their applications are discussed in this paper. We gave an overview of architectural extension to wireless sensor network. Application of cloud computing to enhance the reliability and availability of wireless sensor networks is discussed with special emphasis on its application in distributed manufacturing engineering. The proposed system is based on ideas taken from an in depth study and support of various technologies. The proposed system has its useful applications and important role in medical sciences field. It is supposed to help in efficient cure of Strokes and Parkinson. However the security issues involved in the integration process are of key importance and need critical focus. Further efforts will help extend the applications to military and manufacturing services.

### REFERENCES

- [1] Wendi B. Heinzelman, Amy I. Murphy, Heraldo S. Carvalho, Mark A. Perillo; "Middleware to Support Sensor Network Applications"; IEEE Network, pp. 6-14, January/February 2004.
- [2] F. Schepers. (2010) Security in Cloud Computing, IBM Tivoli Internet Security Systems. [Online]. Available: <http://www.cpdconferences.org/Resources/Schepers.pdf>. Last accessed: 10/11/2010.
- [3] P. McDaniel, and S. W. Smith, "Outlook: Cloud Computing with a Chance of Security Challenges and Improvements," IEEE Computer and Reliability Societies 2010, pp. 77-80, Jan. 2010.
- [4] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, A. Warfield, "Xen and the Art of Virtualization," in Proc. of 19th ACM symposium on Operating Systems Principles, Bolton Landing, NY, USA, October 2003, pp. 164-177.
- [5] (2010) Google App Engine. [Online]. Available: <http://code.google.com/appengine/>. Last Accessed: 15/07/2011
- [6] (2007) Sales Force. [Online]. Available: <http://www.salesforce.com/platform/>. Last Accessed: 10/11/2010
- [7] A. Dubey, and D. Wagle. (2007) Delivering software as a service – The McKinsey Quarterly. [Online]. Available: [http://www.mckinsey.de/downloads/publications/mckinsey\\_on\\_bt2007/mobt\\_Delivering\\_Software\\_as\\_a\\_Service.pdf](http://www.mckinsey.de/downloads/publications/mckinsey_on_bt2007/mobt_Delivering_Software_as_a_Service.pdf) Last Accessed: 15/08/2011.
- [8] D. Harkins and D. Carrel. (1998) The Internet Key Exchange (IKE), RFC 2409, IETF Network Working Group. [Online]. Available: <http://www.ietf.org/rfc/rfc2409.txt>. Last Access: 12/01/2011. Heidemann, et al., Building efficient wireless sensor networks with low-level naming, in: Proc. Symposium on Operating Systems Principles, Chateau Lake Louise, Banff, Alberta, Canada, ACM. (Oct., 2001) pp. 146-159. Available in: <http://www.isi.edu/johnh/PAPERS/HeidemannOI.html>.

- [9] Nils Hoeller, Christoph Reinke, Jana Neumann, Sven Groppe, Daniel Boeckmann, Volker Linnemann, "Efficient XML Usage within Wireless Sensor Networks" WICON '08, November 17-19, 2008, Maui, Hawaii, USA.
- [10] Lim Hoc Beng, "Sensor cloud: towards sensor-enabled cloud services" Intelligent systems center, Nanyang Technological University, 13 April 2009.
- [11] P. McDaniel, and S. W. Smith, "Outlook: Cloud Computing with a Chance of Security Challenges and Improvements," IEEE Computer and Reliability Societies 2010, pp. 77-80, Jan. 2010.
- [12] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, A. Warfield, "Xen and the Art of Virtualization," in Proc. of 19th ACM symposium on Operating Systems Principles Bolton Landing, NY, USA, October 2003, pp. 164-177.
- [13] (2010) Google App Engine. [Online]. Available: <http://code.google.com/appengine/>. Last Accessed: 15/07/2011
- [14] (2007) Sales Force. [Online]. Available: <http://www.salesforce.com/platform/>. Last Accessed: 10/11/2010

IJERT