GENERIC INTEGRATED SECURED WSN- CLOUD COMPUTING FOR U-LIFE CARE

Sudarsan Rao Vemuri[1],   Dr.N.Satyanarayana [2] , V.Lakshmi Prasanna[3]

[1] *Associative Professor ,Department of Computer Science & Engineering,Khammam Institute of Technology & Sciences(KITS), Khammam, A.P-India,* **Sudharshan.cse@gmail.com**

[2] *Professor ,Department of Computer Science & Engineering,   Nagole Institute of Technology & Sciences(NITS), Nogole,Hyderabad,Andraparadesh(AP),India,***nsn1208@gmail.com**

[3] *Asstistant Professor, Department of Computer Science & Engineering, Khammam Institute of Technology & Sciences(KITS), Khammam, A.P-India,***vanama.Lakshmiprasanna38@gmail.com**

Abstract

This paper presents a Secured Wireless Sensor Network-integrated Cloud computing for u-Life Care (SC3). SC3 monitors human health, activities, and shares information among doctors, care-givers, clinics, and pharmacies in the Cloud, so that users can have better care with low cost. SC3 incorporates various technologies with novel ideas including; sensor networks, Cloud computing security, and activities recognition.
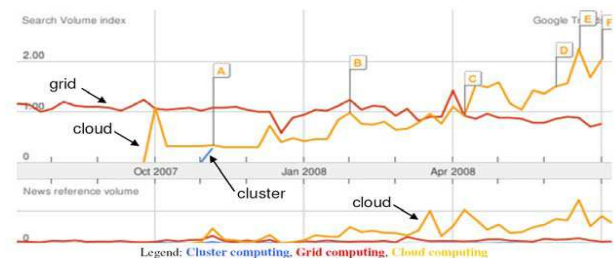
Index Terms: Korea u-Care System for a Solitary Senior Citizen (SSC),More mobility, Securities for WSN, Cloud computing to support u-Life care *etc.*

--- *** --

1. INTRODUCTION

1.1. What is Cloud Computing?

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**".
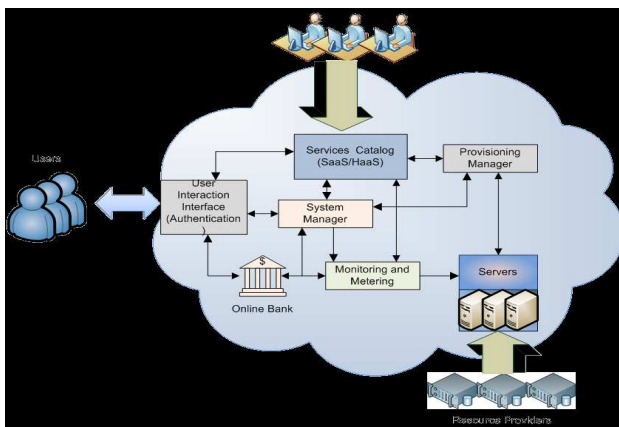
The Web search popularity, as measured by the Google search trends during the last 12 months, for terms "Cluster computing", "Grid computing", and "Cloud computing" is shown in Figure 1. From the Google trends, it can be observed that cluster computing was a popular term during 1990s, from early 2000 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: **Reduced cost, higher gains**: Cloud technology is paid

SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

incrementally, saving organizations money. **Increased storage**: Organizations can store more data than on private computer systems. **Highly automated**: No longer do IT personnel need to worry about keeping software up to date. **Flexibility**: Cloud computing offers much more flexibility than past computing methods.

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 **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 in Figure 3

1.2.Why Cloud Computing in u-Life care?

As the standard of living rises, people are more interested in their health and desire well-being life. Today due to aging of population, rising cost of workforce and high quality treatment, threat of new panepidemies and diseases, the cost of life care or healthcare system is increasing worldwide. According to OECD (Organization of Economic Cooperation and Development) Health data 2008 (shown in Figure 4), total health spending accounted for 15.3% of GDP in the United States in 2006, the highest share in the OECD, and more than six percentage points higher than the average of 8.9% in OECD countries. Korea was 6.4% of GDP to health in 2006. The United States also ranks far ahead of other OECD countries in terms of total health spending

per capita, with spending of 6,714 USD (adjusted for purchasing power party (PPP)), more than twice the OECD average of 2,824 USD in 2006. For Korea it was 1480 USD.
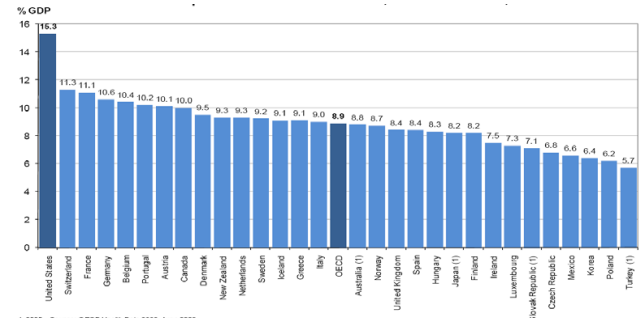

Figure 4-Health expenditure as a share of GDP, OECD countries,2006

1.3. Problems of Existing Cloud computing to support u-Life care

Poor Security and Privacy Support

Data for life care services normally composes of personal information, contextual information (e.g. location, user activity information), medical data (e.g. medical history, drug information, medical health record), etc. Such information is **highly sensitive** and people do not want to disclose them to the public. For example, a patient with HIV positive test may not want to expose his result to the other, even to their family.

Storing data in Cloud leads to **more security and privacy problems than traditional computing** systems such as distributed systems or grid computing systems. Sensitive data processed outside the enterprise brings with it an **inherent level of risk**, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. More dangers and vulnerabilities may cause disrupts of services, theft of information, loss of privacy, damage of information. On the other hand, because any one can access to Clouds, it brings more chances for malicious users to launch their hostile programs. Hostile people can also give instructions to good programs, or bad guys corrupting or eavesdropping on communications.

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 as shown in Figure 7can measure heart rate, heart rate variability, Oxygen saturation and blood pressure for the person wearing the ring.
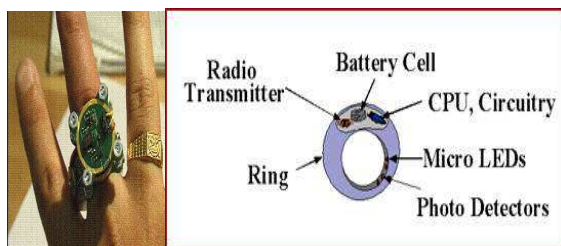
SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

Figure-7 MIT wireless sensor ring and its internal architecture

Collection, analysis (knowledge processing, ontology reasoning etc.), storing and disseminating of these sensor data is a great challenge since sensor nodes constituting a WSN have limited sensing capability, processing power, and communication bandwidth. There is a lack of uniform operations and standard *representation for sensor data.*

1.4. Practical Usage

Our proposed SC3 can be deployed for various u-Life care services, including but not limited to:

Safety monitoring services for home users o SC3's WSN can monitor home user's movement, location by using various sensors. The sensor data is then disseminated to the Clouds, from that SC3's Life care services such as emergency caregivers can monitor and has immediate response in case of emergent situations like heart attack.

Information sharing services o With SC3, patient information and data can be accessed globally and resources can be shared by a group of hospitals rather than each hospital having a separate IT infrastructure. Cloud computing would help hospitals to achieve more efficient use of their hardware and software investments and increase profitability by improving the utilization of resources to the maximum. The SC3 can provide a flexible platform for public-health departments to upload real-time health data in a timely manner to assist state and national health officials in the early identification and tracking of disease outbreaks, environmental-related health problems, and other issues.

Emergency-connection services o SC3 can be deployed to real-time monitor home environments, including gas, fire, thief, etc. Through SC3, an alarm system connects to users, u-119, police department can give an emergency alert in case any emergent situation occurs.

Users can monitor their home, their family health anywhere, any time with any device o SC3 Clouds and WSN enable user to access their home environment, their family's health information with any kind of connected devices over Internets such as cell phone, PDA, laptop, computer.

2. CONTRIBUTION OF THIS STUDY

Our proposed SC3 can help in enhancing capabilities and provides tremendous value by achieving efficient use of software and hardware investments. Our infrastructure drives profitability by improving resources utilization and increasing their scalability while maintaining strong privacy and security essential in u-Life care. SC3 can provide cost efficient model for automating hospitals and other life care agencies, managing real-time data from various sensors, efficiently disseminating information to consumers, support privacy and strong authentication mechanism, reducing IT complexity and at the same time introducing innovative solutions and updates. Our versatile architecture makes it possible to launch web 2.0 applications quickly and also upgrade u-life care IT applications easily as and when required. Our automated secure framework of cloud computing would provide increasingly cheaper and innovative services. Technically, our SC3 infrastructure can contribute in the following ways in u-Life care:

Our architecture helps in eliminating the time and effort needed to roll a healthcare IT application in a life care centre

Flexible and swift access to expert opinion

Intelligent personal health monitoring system

Synergy of information from individual sensors (better insight into the physiological state and level of activity).

Hospitals, silver care centers and life care agencies could share our secured infrastructure with vast number of systems linked together (i.e. secured sensor network to support real time information) for reducing cost and increasing efficiency. This means real-time availability of patient information for doctors, nursing staff and other support services not within the country but possibly across various countries as medical professionals can access patient information from any internet enabled device without installing any software.

The EMR software or the LIS software and information can be located in our Cloud and not on the users or computer. Patient information and data can be accessed globally maintaining proper privacy and security policy and resources can be shared by a group of hospitals or life care agencies rather than each hospital having a separate IT infrastructure.

Rapid response to critical life care regardless of geographic barriers (anytime, anywhere)

Management of medical expertise also in rural areas

Swift medical care in emergencies and medical data management in Catastrophes

Promotion of healthy life styles with continuous health monitoring

Savings for ubiquitous healthcare service providers and patients in procedural, travel, and claim processing cost

SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

Reduced use of traditional emergency services

Improved non-emergency services

Decreased waiting time for nonemergency services

Greater awareness of services among rural and remote residents and caregivers

Timely accessibility of critical information in the event of emergencies.

2.1 Korea u-Care System for a Solitary Senior Citizen (SSC):

Numerous projects within industry and academia are already started or being used in reality. in 17 July 2008, an RFP of Ministry for Health, Welfare and Family Affairs, Korea has released **u-Care System for a Solitary Senior Citizen** (SSC) [1]. The system provides a number of featured services including: **24 hours × 365 days safety monitoring services for a SSC**: monitoring SSC's movement or location by using motion or tripwire sensors, voice communication between a SSC and a life-care giver at all times, emergency call service for heart attack, etc. **Emergency-connection services**: real-time monitoring of gas spillage or fire by using gas and detection sensors, if any emergency situation occurs like gas or fire, automatically notify to u-119 system. **Information sharing services**: sharing a SSC database to related organization such as fire-station, care givers, or central information system, and a history of care givers activities to build an efficient SSC management systems, etc.

In this system, *u-Care Center* maintains Data Server, DB Server, and Web Server to store data from SSC's home and provide access to various services, as illustrated in Figure 8. However, its biggest issue is a **high cost of deployment** when it becomes widely used. With recent advanced in MEMS technology which enables low cost

sensors, each user may carry on a number of sensors and wearable devices, leading to a huge amount of data produced. On the other hand, more and more life care applications and services access to the system to provide better care for users. It obviously causes a problem of economy to maintain the system.
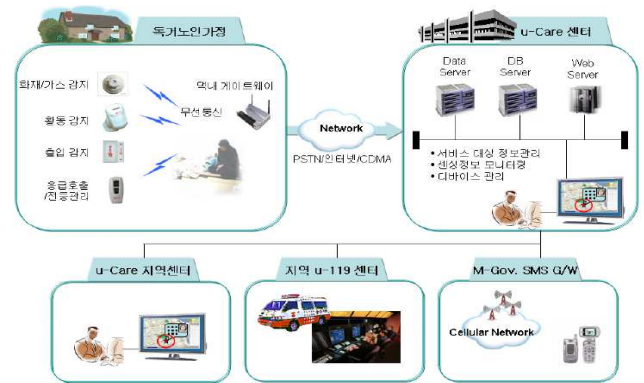

Figure 8 Hardware architecture of u-Care System for a Solitary Senior Citizen (source: Korea Ministry)

In another sector of healthcare applications, several providers explore advantages of Cloud computing to reduce cost and increase care services. Among those, Microsoft and Google are two pioneers who bring Cloud healthcare platforms to reality.

2.2 Microsoft HealthVault :-

Microsoft developed a platform to store and maintain health and fitness information, called **HealthVault** [1]. It is a cloud service that helps people collect, store, and share their personal health information. Health Vault's data can come from providers, pharmacies, plans, government, employers, labs, equipment and devices, and from consumers themselves. Access to a record is through a Health Vault account, which may be authorized to access records for multiple individuals, so that a mother may manage records for each of her children or a son may have access to his father's record to help the father deal with medical issues.

2.3 Google Health

Meanwhile, Google provides a personal health information centralization services, known as **Google Health** [3]. The service allows Google users to volunteer their health records, either manually or by logging into their accounts at partnered health services providers, into the Google Health system, thereby merging potentially separate health records into one centralized Google Health profile. Volunteered information can include health conditions, medications, allergies, and lab results. Once entered, Google Health uses the information to provide the user with a merged health record, information on conditions, and possible interactions between drugs, conditions, and allergies. In general, Health Vault and Google Health serve as Cloud health information storages and operate separately. As consumers of different Cloud applications rely on Cloud Providers (CLP) to supply all their computing needs (process, store and analyze huge sensor data and user generated data) on

SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

demand, they will require specific QoS to be maintained by their providers in order to meet their objectives and sustain their operations. To solve **the problem of Cloud interoperation**, an Unified Cloud Interface (UCI) standardization has been proposed.

2.4 Amazon's Cloud computing based Healthcare efforts

At an invitation-only event sponsored by Harvard Medical School and Amazon Web Services, a few dozen experts convened in Boston for a day to ponder the possibilities of cloud computing in their work. Participants included health care IT leaders, academics, biomedical researchers, medical and scientific consulting firm representatives, and officials from vendors like Amazon, Oracle, and Hewlett-Packard [54]. For its part, Amazon in recent weeks unveiled the AWS Hosted Public Data Sets, or "Public Data Computing Initiative," which provides on the cloud a "hosted-for-free, centralized public repository" for data -- such as United States census and human genome research data -- useful to researchers, Now we will describe some existing solutions or standard regarding Cloud computing.

2.5 Secured Cloud Overlay: VPN-Cubed

One of the security challenges of Cloud Computing - and specifically Infrastructure as a Service (IaaS) is securely connecting enterprise network to one or more Cloud providers without deploying VPN hardware.

VPN-Cubed™ is the first commercial solution by CohesiveFT that enables customer control in a cloud, across multiple clouds, and between private infrastructure and the clouds. VPN-Cubed provides an overlay network that allows the user to control of addressing, topology, protocols, and encrypted communications for devices deployed to virtual infrastructure or cloud computing centers [55]. When using public clouds corporate assets are going into 3rd party controlled infrastructure. VPN-Cubed gives you flexibility with control in 3rd party environments. Here consumer has most of the responsibility to secure his/her own data.

2.6 Unified Cloud Interface (UCI) standardization

The Unified Cloud Interface (UCI) standardization [4] or Cloud broker will serve as a common interface for the interaction with remote platforms, systems, networks, data, identity, applications and services. UCI will be composed of a semantic specification and an ontology. The ontology provides the actual model descriptions, while the specification defines the details for integration with other management models. One of the key drivers of the unified cloud interface is to create an API about other API's. A singular programmatic point of contact that can

encompass the entire infrastructure stack as well as emerging cloud centric technologies all through a unified interface. The draft proposal will be submitted for approval by the Internet Engineering Task Force (IETF) for inclusion as a XMPP Extension and presented at the IEEE International Workshop on Cloud Computing (Cloud 2009) being held in May 18-21, 2009, in Shanghai, China.

2.7 Problems of Existing Works

Weak security support

o First, the customer needs to know her data is encrypted so nosey sysadmins at the cloud data center can't troll through the data for interesting tidbits. If the information is encrypted, who controls the encryption/decryption keys, the customer or the cloud vendor?

o Integrity relates to the integrity of the data, in that it changes only in response to duly authorized transactions. So we need standards to ensure that. But they don't exist -- yet.

o The last nagging security issue is availability: Will the data be there whenever you need it? The answer here is an unqualified "maybe." In February of this year, Amazon's S3 went down for almost four hours, wreaking havoc on several companies that use and depend on the S3 Cloud. Amazon ascribed the cause to an unexpected spike in customer transactions.

Weak Privacy Support

Private health data can goes public by mistake: Part of consumers' reticence to sign up for electronic personal health-care records — with or without services "in the cloud" — has to do with a handful of recent high-profile data breaches. In April, the largest health insurer in the U.S.,

WellPoint disclosed that records on as many as 130,000 of its customers had leaked out and become publicly available over the Internet. User heath data and information uploaded into Clouds are not controlled by user

o Consumer's privacy may get loss in the cloud: Is there a law that keeps your data from being misused? Yes. It is Health Insurance Portability and Accountability Act (HIPAA), but it does not offer health-care service themselves. Right now, disclosure of health information is out of control.

No infrastructure to support WSN integration to Cloud

The existing Cloud based Healthcare system does not integrate wireless sensor network which is necessary to get real time information of patient or environment to monitor and analysis emergency situation.

Appropriate information dissemination mechanism is not explicitly addressed in the existing system to deliver sensor data or events to appropriate users of Cloud applications who subscribed. Also there is a need to match published events with

SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

subscriptions efficiently. A fast, scalable and efficient event matching algorithm is required for information dissemination system on Sensor-Cloud framework.

Lack of Dynamic Collaboration between Cloud providers
When the Cloud provider is unable to provide quality of service to the end-user requests, it may result in service–level agreement (SLA) violation and end up costing the provider

Existing commercial Cloud services are proprietary in nature. They are owned and operated by individual companies. Each of them has created its own closed network, which is expensive to setup and maintain. Existing Cloud based solution does not consider the dynamic collaboration between Cloud providers which is obvious in near future.
Table 1 shows a comparison of the above existing work.

Existing Works / Features	Korea u-Care System	MS. HealthVault	Google Health	Amazon	VPN-Cube™	UCI
Security	X	Weak	Weak	Weak	Weak	X
Privacy Control	Weak	Weak	Weak	Weak	Weak	X
USN Integration to Cloud	X	X	X	X	X	X
Sensor data dissemination to Cloud	X	X	X	X	X	X
Collaboration btw Clouds	X	X	X	X	V	V

Table 1. A Comparison of Existing Works

3. SECURED WSN-INTEGRATED CLOUD COMPUTING

3.1 Overview

Our research scope falls into Wireless Sensor Network, Cloud Computing, and Security & Privacy for WSN ad Cloud, as shown in Figure 9. In this section, we present an overview of our proposed solution, Secured WSN-integrated Cloud Computing for u-Life Care, called SC3.
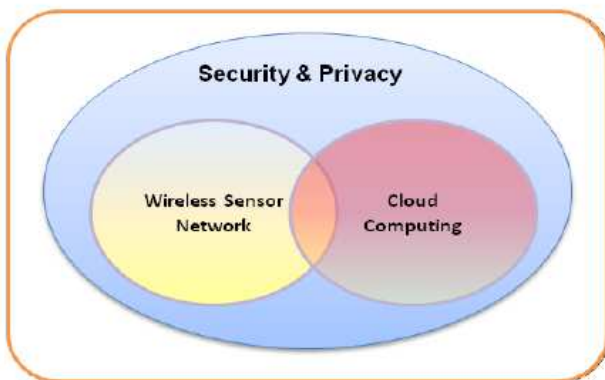

Figure-9 Our Research Scope

The abstract model is shown in Figure 10. We deploy a secure wireless sensor networks in u-Home environments for a purpose of monitoring and collecting sensor data. To enable u-Lice care applications, we propose an Activity Recognition engine module for u-Life care in WSN layer. This is very important engine to detect and report current user's activities for different purpose of life care services. The sensor data is transferred to Clouds by using sensor data dissemination and integration mechanisms. We provide a security and privacy control of data and applications stored in Clouds. Different Clouds can collaborate with each other by using our dynamic collaboration method. Numerous u-Life care services can access Clouds to provide better and low cost cares for end-users such as secure u-119 service, secure u-Hospital, secured u-Life care research, secure u-Clinic, etc. Figure 11 and Figure 12 shows the functional architecture and proposed architecture of the SC3. SC3 is composed of the following modules: security for WSNs (trust management), security and privacy control for Clouds (authentication and access control), integration mechanism of wireless sensor networks to Clouds, sensor data dissemination mechanism, dynamic collaboration mechanism between different Cloud providers (CLPs), and activity recognition engine for u-Life care.
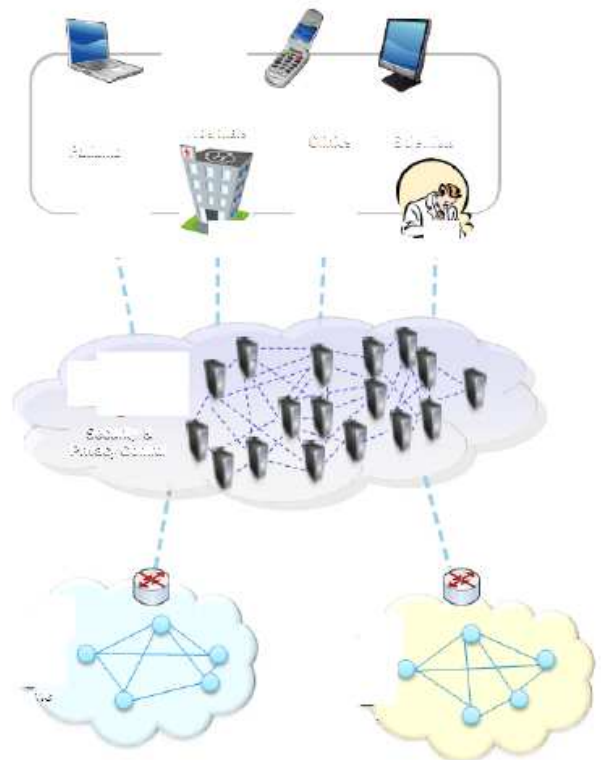

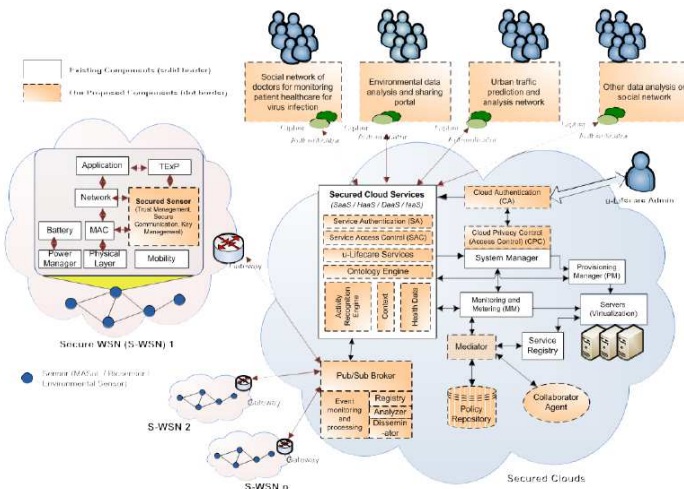**Figure 10** Overall Architecture of SC3
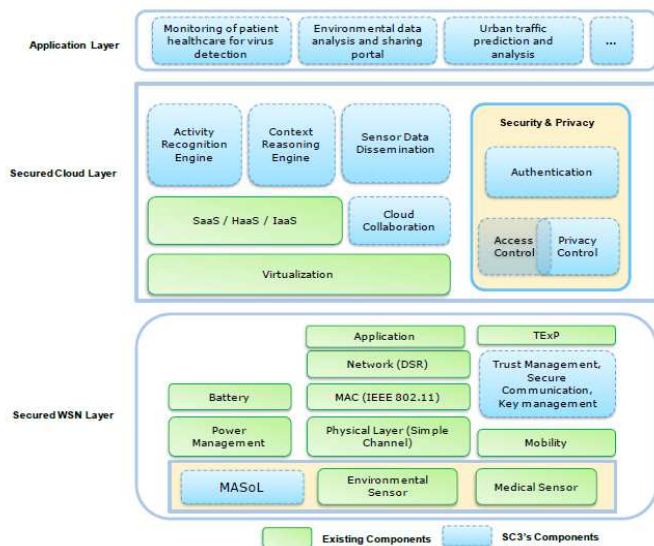
Figure-11 Functional Architecture of SC3

Figure-12 Layered Architecture of SC3

Privacy Control Cloud Collaboration Sensor Data Dissemination **Secured WSN Layer Secured Cloud Layer Application Layer** Activity Recognition EngineAuthenticationSaaS / HaaS / IaaS **Existing Components SC3's Components** Monitoring of patient healthcare for virus detectionEnvironmental data analysis and sharing portalUrban traffic prediction and analysis…Access ControlVirtualizationContext Reasoning Engine**Security & Privacy**MASoLEnvironmental Sensor Medical Sensor Physical Layer (Simple Channel)Power Management Battery MAC (IEEE 802.11)Network (DSR)TExP Mobility Trust Management, Secure Communication, Key management Application

3.2 Challenges

Low resource sensors Sensor nodes are very limited in term of energy, communication, and computation. Therefore, in order to make the algorithms feasible on sensor devices, they must be lightweight and energy-efficient. A huge number of users, and it increases dramatically As the number of users accessing Clouds increase dramatically, how to support individual users to declare their privacy preferences accurately. Authentication method must be usable on various devices with wired or wireless-enable connection over the Internet. Besides, appropriate privacy policy implementation is very hard. User must agree to provide his/her sensitive information which is not always possible Data dissemination challenges In case of dissemination of information to mobile clients, the mobility can cause their access brokers to be changed, which can bring problems in dissemination of subscriptions and distribution of matching results. Dynamic collaboration challenges Finding appropriate group strategy to minimize collaboration cost in dynamic collaboration is really a major challenge.

3.3 Desired Components of SC3

In the following sections, we present SC3 in details. As shown in Figure 12, we propose SC3 with the following components:

Security and Privacy Control

Security for WSN including Trust Management Security and Privacy Control for Clouds including Authentication, Access Control, Privacy Control Integration of WSNs to Clouds. Sensor Data Dissemination Mechanism   Cloud Dynamic Collaboration Mechanism Activity Recognition Engine for u-Life care

4 Securities for WSN

4.1 Group-based Trust Management Scheme

4.1.1 Introduction

A WSN is an essential technology for any health-care or life-care systems. Since life-care systems carries sensitive and private data, therefore security must be enforced in robust and reliable manner. Current security solutions of WSNs [5]-[9] are not capable of providing corresponding access control based on judging the quality of a sensor nodes and their services. This can only be achieved by in-cooperation of trust management scheme. The in-cooperation of trust in a security solution also provides other benefits such as: Trust solves the problem of providing reliable routing paths that does not contain any malicious, selfish or faulty node(s). Trust makes the traditional security services more robust and reliable by ensuring that all the communicating nodes are trusted during authentication, authorization or key management phases.

SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

4.1.2 Problems of Existing Approaches

To the best of our knowledge, very few comprehensive trust management schemes (e.g. RFSN [10], ATRM [11] and PLUS [12]) have been proposed for sensor networks. Although, there are some other works available in the literature e.g. [13]-[16] etc., that discuss trust but not in much detail. Within such comprehensive works, only ATRM [7] scheme is specifically developed for the clustered WSNs. However, this and other schemes, suffer from various limitations such as these schemes do not meet the resource constraint requirements of the WSNs; and more specifically, for the large-scale WSNs. Also, these schemes suffer from higher cost associated with trust evaluation especially of distant nodes. Furthermore, existing schemes have some other limitations such as dependence on specific routing scheme, like the PLUS scheme works on the top of the PLUS R routing scheme; dependence on specific platform, like the ATRM scheme requires an agent-based platform; and unrealistic assumptions, like the ATRM assumes that agents are resilient against any security threats, etc. Therefore, these works are not well suited for realistic WSN applications. Thus, a lightweight secure trust management scheme is needed to address these issues.

4.1.3 Proposed Solution

Our proposed Group-based Trust Management Scheme (GTMS) scheme calculates the trust value based on direct or indirect observations. Direct observations represent the number of successful and unsuccessful interactions and indirect observations represent the recommendations of trusted peers about a specific node. Figure 13 shows our Trust Management component in general sensor node architecture.
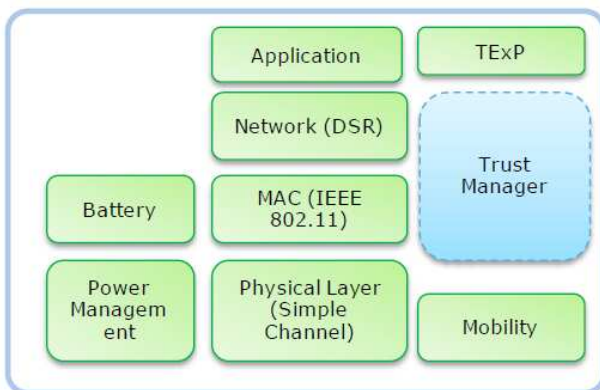

Figure-13 Sensor Node Architecture with our Trust Management Component

Interaction means cooperation of two nodes. For example, a sender will consider interaction as a successful interaction if he got assurance that the packet is successfully received by the neighbor node and he has forwarded it toward destination in an unaltered fashion. First requirement of successful reception is achieved on reception of the link layer acknowledgment (ACK). IEEE 802.11 is a standard link layer protocol, which keeps packets in its cache until the sender received ACK. whenever receiver node successfully received the packet he will send back ACK to the sender. If sender node did not received ACK during timeout then sender will retransmit that packet.

Second requirement is achieved with the help of using enhanced passive acknowledgments (PACK) by overhearing the transmission of a next hop on the route, since they are within radio range [17]. If the sender node does not overhear the retransmission of the packet within a timeout from its neighboring node or overheard packet is found to be illegally fabricated (by comparing the payload that is attached to the packet) then the sender node will consider that interaction as an unsuccessful one. If the number of unsuccessful interactions increases, then the sender node decreases the trust value of that neighboring node and may consider it as a faulty or malicious node.

The proposed trust model works with two topologies. One is the intra-group topology where distributed trust management is used. The other is inter-group topology where centralized trust management approach is employed. For the intra-group network, each sensor that is a member of the group, calculates individual trust values for all group members. Based on the trust values, a node assigns one of the three possible states: 1) trusted, 2) un-trusted or 3) un-certain to other member nodes. This three-state solution is chosen for mathematical simplicity and is found to provide appropriate granularity to cover the situation. After that, each node forwards the trust state of all the group member nodes to the CH. Then, centralized trust management takes over. Based on the trust states of all group members, a CH detects the malicious node(s) and forwards a report to the base station. On request, each CH also sends trust values of other CHs to the base station. Once this information reaches the base station, it assigns one of the three possible states to the whole group. On request, the base station will forward the current state of a specific group to the CHs. Our group based trust model works in three phases: 1) Trust calculation at the node level, 2) Trust calculation at the cluster head level, and 3) Trust calculation at the base station level.

5 WSN-CLOUD INTEGRATION

5.1 Introduction

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,

SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

military surveillance etc. Collection, analysis (knowledge processing, ontology reasoning etc.), storing and disseminating of these sensor data is a great challenge since sensor nodes constituting a WSN have limited sensing capability, processing power, and communication bandwidth. However, there is a lack of uniform operations and standard representation for sensor data.

5.2 Problems of Existing Works

Currently there is no framework to support the integration of WSNs to Cloud. There are many challenges exist to enable this framework as the entire network is very dynamic. On the WSN side, sensor or actuator (SA) devices may change their network addresses at any time Wireless links and SA devices are quite likely to fail at any time, and rather than being repaired, it is expected that they will be replaced by new ones. Besides, different Cloud applications can be hosted and run on any machines anywhere on the cloud. In such situations, the conventional approach of using *network address* as communication means between the SA devices and the applications may be very problematic because of their dynamic and temporal nature. Moreover, several Cloud applications may have an interest in the same sensor data but for different purposes. In this case, the SA nodes would need to manage and maintain communication means with multiple applications in parallel. This might exceed the limited capabilities of the simple and low-cost SA devices.

5.3 Proposed Solution

We propose a content-based publish/subscribe (pub/sub) [1] broker model on the Cloud that integrates WSNs to Cloud efficiently and effectively. The framework is shown in Figure 24. The terminologies used to describe the system architecture are listed in Table 2. In this framework, sensor data or events are delivered to the -51-consumers or applications on the Cloud *not based on their network addresses*, but rather as a *function of their contents and interests.* The pub/sub broker is located in the Cloud to gain high performance in terms of bandwidth and capabilities.
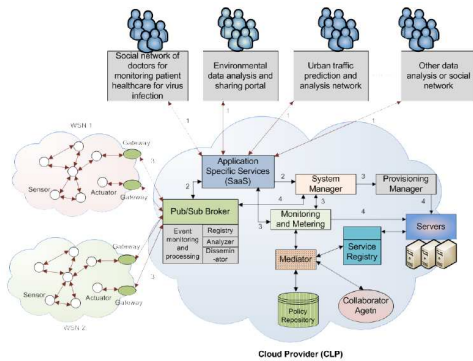

Figure 24 A Framework of WSN – Cloud Integration

Terminology	Description
Gateway	Sensor data comes to the pub/sub broker through gateway
Pub/Sub Broker	Responsible to monitor, process and deliver events to users (registered) through SaaS applications
SaaS (Software as a Service) Application	SaaS application which combines data and application together and runs on the Cloud server
System Manager (SM)	Manages the computer resources
Provisioning Manager (PM)	Carve out the systems from the cloud to deliver on the requested service. It may also deploy the required images.
Monitoring and Metering (MM)	Tracks the usage of the primary cloud resources as well as the resources of collaborator CLP's so the resources used can be attributed to a certain user.
Service Registry (SR)	Discovers and stores resource and policy information to local domain
Mediator	Responsible for negotiation among the collaborating CLPs and management of operations within a VO
Policy Repository (PR)	A storage of Web server, mediator and VO policies
Collaborator Agent (CA)	A resource discovery module in the collaborating CLPs environment

Table 2: List of commonly used terms

The pub/sub broker has four components describes as follows: *Sensor Stream or Event monitoring and processing component (SMPC):* The sensor stream comes in many different forms. In some cases it is raw data that must be captured, filtered and analyzed on the fly and in other cases it is stored or cached. The style of computation required depends on the nature of the streams. So the SMPC component running on the cloud monitors the event streams and invokes correct analysis method. Depending on the data rates and the amount of processing that is required, SMP manages parallel execution framework on Cloud. *Registry Component (RC):* Different SaaS applications register to pub-sub broker for various sensor data required by the community user. For each application, registry component stores user subscriptions of that application

SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

and sensor data types (temperature, light, pressure etc.) the application is interested in. Also it sends all user subscriptions along with application id to the disseminator component for event delivery. *Analyzer Component (AC):* When sensor data or events come to the pub-sub broker, analyzer component determines which applications they are belongs to and whether they need periodic or emergency deliver. The events are then passed to the disseminator component to deliver to appropriate users through SasS applications. *Disseminator Component (DC):* For each SaaS application, it disseminates sensor data or events to subscribed users using an event matching algorithm (described in section 6). It can utilize Cloud's parallel execution framework for fast event delivery.

6.   SCENARIO   DESIGN–SC3   SUPPORTS ALZHEIMER'S DISEASE

Our general system deployment is shown in Figure 63. The patient's house includes a kitchen, a bed-room, and a living room. Several sensors and cameras are deployed in the patient's house to collect sensory data and images. We deploy a cloud gateway in the living room to collect data from all sensors and cameras. It connects to the Cloud via Internet high speed router. Doctors, nurses, and patient's relatives (e.g. his daughter) can access easily via Web2.0 interface.
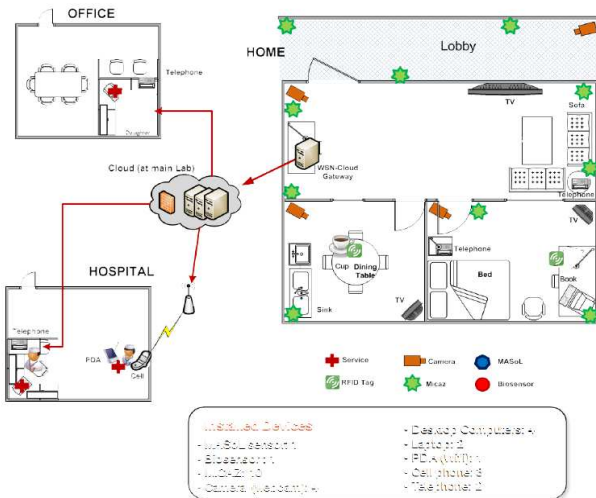

Figure-6.1 Overall Scenario Design at ITRC

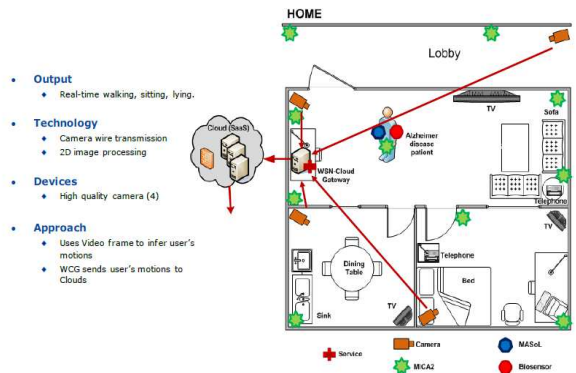The following figures show how we collect data from sensors and cameras and deploy to the Cloud.
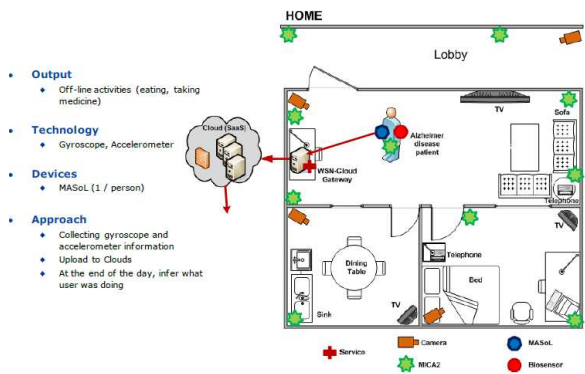

Figure -6.2 Camera Deployment for Video-based AR

Figure-6.3 Sensor Deployment for Sensor-based AR
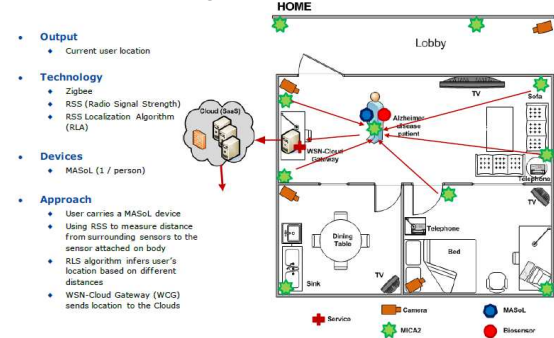
Location Tracking

Figure -6.4 Location Tracking Deployments

CONCLUSION AND FUTURE WORK

This paper introduces Secured WSN-integrated Cloud Computing for u-Life Care, called SC3. It provides a number of featured components, including security and privacy control, WSN-Cloud integration mechanism, dynamic collaboration between Clouds, and an activity recognition engine to enable many u-Life care services. We also present our primary result of development, and then discuss about its potentialities and benefits.

SUDARSAN RAO VEMURI* et al.   ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY   Volume-2, Issue-4, 897 – 907

FUTURE WORK

There are still many works ahead. The first future work that we plan to work on is to provide more services to different kinds of patient's disease such as stroke, Parkinson disease, etc. The number of activities will be increased to support more services. A number of wireless medical sensors are under developed. They will be used to collect health data of patient seamlessly. We also will focus more on security and privacy for Cloud Computing. Currently, most users do not want to store their personal health data on Clouds because it is not safe and reliable. Another work is to extend our development into various such as manufacturing, military services.

REFERENCES:

[1] Korea u-Life care system

[2] Microsoft HealthVault http://healthvault.com

[3] Google Health https://www.google.com/health

[4] Chris Karlof, Naveen Sastry, and David Wagner. TinySec: a link layer security architecture for wireless sensor networks. In Proc. of the 2nd Int. Conf. on Embedded networked sensor systems, pages 162–175, Baltimore, MD, USA, November 2004.

[5] Taejoon Park and Kang G. Shin. LiSP: A lightweight security protocol for wireless sensor networks. Trans. on Embedded Computing Sys., 3(3):634–660, 2004.

[6] Erik-Oliver Bla and Martina Zitterbart:. Towards acceptable public-key encryption in sensor networks. In proc. of 2nd International Workshop on Ubiquitous Computing, pages 88–93, Miami, USA, 2005.

[7] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in Proc. of ACM Security for Ad-hoc and Sensor Networks, Oct. 2004, pp. 66–67.

BIOGRAPHIES:

Sudarsan Rao Vemuri, Associative Professor , Department of Computer Science & Engineering, Khammam Institute of Technology & Sciences (KITS), Khammam, A.P India, Sudharshan.cse@gmail.com

Dr.N.Satyanarayana, Professor , Department of Computer Science & Engineering, Nagole Institute of Technology, & Sciences(NITS), Nogole, Hyderabad, Andraparadesh (AP), India, nsn1208@gmail.com

V.Lakshmi Prasanna[3], Asstistant Professor, department of Computer Science & Engineering, Khammam Institute of Technology & Sciences(KITS), Khammam,AP. India, vanama.Lakshmiprasanna38@gmail.com