International Journal of Science Engineering and Advance Technology

The Trust and Reputation Systems towards Data for Cloud and Wireless Sensor Networks Integrity

Sudanagunta Venkata Prathyusha*[1], N Mahesh[2]
M.Tech Scholar (CSE), Department of Computer Science & Engineering,
Assist.Prof, Depart of Computer Science & Engineering, QIS Institute of Technology, Ongole, AP, India.

Abstract:

Cloud Computing has powerful data storage and data processing capabilities as well as Wireless sensor network has capability of gathering large amount of data. Presented on by including ordering data storage besides to human sources capacities of cloud computing moreover to pervasive data gathering capacity of wireless systems, cloud computing-wireless systems reconciliation permit us lifted consideration from different groups. The blend worldview of cloud computing-wireless systems focuses by conceivable application circumstances. It starts an original copy and bona fide confide in furthermore to status computation and administration system implied for the blend of cloud computing-wireless systems. The prescribed system will accomplish works for example confirmation of cloud administration also to sensor network suppliers to avoid vindictive pantomime assaults overseeing of trust and standing concerning administration of cloud administration furthermore to sensor network suppliers and helping cloud benefit clients to pick alluring cloud suppliers and helping them in choice of suitable suppliers of sensor network. However, in spite of these past endeavours, a few trust administration issues, for example, recognizable proof, protection, personalization, incorporation, security, and adaptability have been normally dismissed and should be tended to.

Keywords: Cloud, sensor networks, integration, authentication, trust, reputation.

I. Introduction

Computing is being changed to a model comprising of administrations that are commoditized and conveyed in a way like customary utilities, for example, water, power, gas, and communication. In such a model, clients get to administrations in light of their prerequisites without respect to where the administrations are facilitated or how they are conveyed. Cloud computing (CC) is a model to empower advantageous, on request network access for a mutual pool of configurable computing assets (e.g., servers, networks, storage, applications, and administrations) that could be quickly provisioned and discharged with negligible administration exertion or specialist organization communication. WSN are the appropriated network of minor minimal effort sensors conveyed in the vast scale to screen condition and helpfully forward the data to the base station or sink node. It's generally utilized as a part of military applications, modern mechanization and condition observing. Because of Adhoc nature data detecting and sending among sensors are powerless against different assaults. Despite the fact that many research exercises are focussed in different assaults and their answers still its should be enhanced as a result of their dynamic conduct. Network security is likewise turning out to be extremely mind boggling errand today because of the fast development of web clients and expanding the volume of data partook in through the network. The majority of the rising administrations, for example, e-administration, online business, elearning and e-social insurance are working in PC networks as it were. It is important to guarantee the security of the mystery data which is exchanging through the network. Conventions are assuming significant part to transfer the data/data from source node to goal node in any networks. Extraordinarily, in specially appointed networks such directing conventions in various when contrasted and steering conventions in wired networks, for example, Local Area Networks (LAN), Wide Area Networks (WAN) and Metropolitan Area Networks (MAN). Steering conventions in specially appointed networks are characterized into three to be specific proactive directing conventions, responsive steering conventions and half breed between the proactive and receptive directing. The table driven convention is a substitute name of a proactive steering convention, for example, Destination Sequence Distance Vector (DSDV) which is every node just to mindful about the following node to the sink and furthermore mindful what number of nodes away the sink. This data are put away in node and shaped as table, consequently the

expression "table driven directing", while the receptive conventions, for example, Ad-hoc On-request Distance Vector (AODV) Routing conventions. On the off chance that a node needs to speak with another node which it has no course, the directing convention will attempt to set up such a course. The AODV convention works in view of the Route Request Message (RREQ) and Route Reply (RREP). Is there any blunder happens amid the correspondence is Route Error (RERR) and it will be sent to the source node.

II. Related Work

Trust administration is a standout amongst the most critical issues in the range of data security and a few studies have been directed. One of the initial couple of perceptions that handles trust issues is finished by Grandison and Sloman [1]. This perception plots put stock in definitions from software engineering, monetary, and social brain research points of view. It likewise traces the trust relationship properties and trust classes that speak to various sorts of trust. Suryanarayana and Taylor arrange trust administration into three sorts, in particular policybased, notoriety based, and informal community based [2]. The creators look at nine trust administration systems in view of eleven unique criteria parameters. Ruohomaa and Kutvonen diagram a few trust models [3]. They characterize trust on-screen characters and group trust administration into three errands, including i) introduction of trust connections, ii) conduct perception and iii) activities after another experience. Artz and Gil look at a few trust definitions for various research regions in the field of software engineering [4]. In particular, the creators examine the pertinence of trust and the semantic Web and bring up some interesting trust administration challenges for the region. At last, Fernandez-Gago et al. play out a trust administration overview focusing on wireless sensor networks. The perception outlines existing trust administration answers for specially appointed and the shared (P2P) wireless sensor networks [5]. A couple reviews concentrate on the notoriety based trust administration systems. For instance, Marti and Garcia-Molina misuse a scientific categorization strategy to arrange distinctive notoriety based trust administration systems [6]. Sabater and Sierra outline the reputationbased put stock in administration and investigate, the relationship between existing arrangements and specialist based point of view [7]. Operator based or multi-specialist trust and notoriety systems utilize a computerized reasoning way where self-ruling and wise programming operators are utilized to notice and scan for reliable elements with a specific end goal to settle on better choices. Josang et al. talk about general thoughts of trust (e.g., trust classes and trust reason) and clarify the covering ideas amongst trust and notoriety terms. A couple trust models are thought about in the study [8]. Silaghi et al. examine whether existing trust administration layouts can be connected to Grid situations [9]. A couple of directions are given in the review that might be helpful to later research and the improvement of trust administration systems in Grids. Wang and Vassileva display a systematic audit of a few trust and notoriety systems. They sort these systems into three classifications including brought together versus decentralized, people/operators versus assets, and worldwide versus customized [10]. A couple of potential research headings are given in the reviews that help create solid Web administrations. In [Hoffman et al. 2009], Hoffman et al. review a few assaults and protection instruments of notoriety systems, especially in P2P situations [10]. They indicate the notoriety system's parts and characterize assaults against every segment. Different protection systems are additionally proposed. The vast majority of the current perceptions do not have an incorporated view on trust administration systems (e.g., approach, notoriety, suggestion, and expectation) [2]. Specifically, trust administration issues, for example, questioned criticisms, poor distinguishing proof of trust inputs, protection of trust members, and the absence of trust criticisms mix have not been completely examined. Furthermore, our perception thinks about thirty delegate trust administration explore models in view of fourteen unique measurements (i.e., appraisal parameters) [3]. Our work particularly concentrates on trust administration issues in cloud situations, which makes unique commitments by showing trust administration points of view, a classification of different trust administration systems and an expository structure for trust administration models appraisal [4].

III. 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.

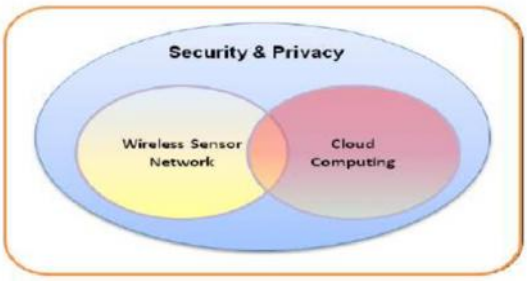

Fig.1 Our Research Scope

We deploy a secure wireless sensor networks in u-Home environments for a purpose of monitoring and collecting sensor data. To enable uLice 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. 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.

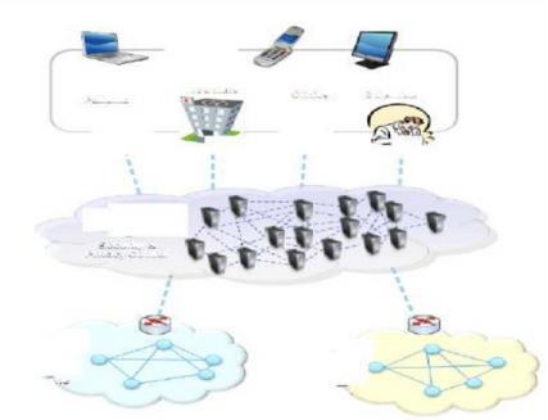

Fig. 2 Overall Architecture of SC3

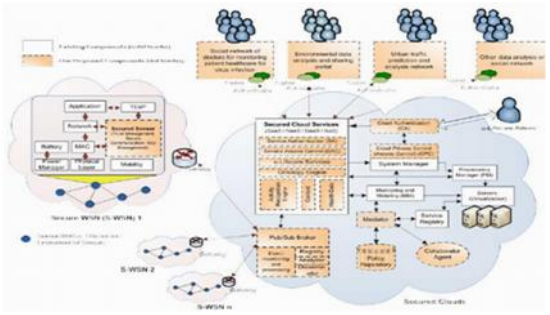

Fig 3. Functional Architecture of SC3

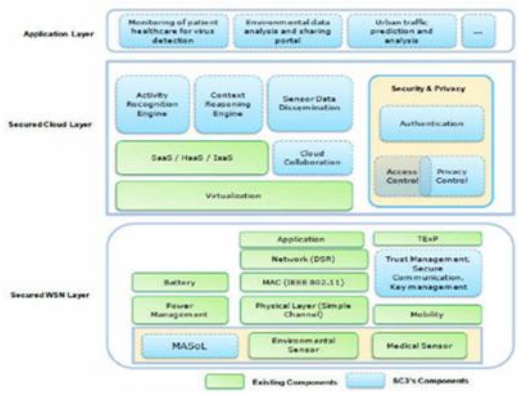

Fig. 4 Layered Architecture of SC3

Privacy Control, Cloud Collaboration, Sensor Data Dissemination are present in Secured Cloud Layer.

Activity Recognition are present in application layer.

Engine AuthenticationSaaS/HaaS/IaaS are Existing Components SC3's Components Monitoring the patient healthcare for virus detection Environmental data analysis and sharing portal urban traffic prediction and analysis…Access Control Virtualization Context ReasoningEngineSecurity&PrivacyMASoLEnviron-mental 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 3.1.4, we propose SC3 with the following components:

Security and Privacy Control

Security for WSN including Trust Management Security.

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 uLife care.

IV. 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 lifecare 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.

4.1.2 Problems of Existing Approaches

To the best of our insight, not very many complete trust administration plans (e.g. RFSN [10], ATRM [1] and PLUS [9]) have been proposed for sensor systems. In spite of the fact that, there are some different works accessible in the writing e.g. [3]-[6] and so forth., that talk about trust however not in much detail. Inside such thorough works, just ATRM [7] plan is particularly created for the grouped WSNs. Be that as it may, this and different plans, experience the ill effects of different confinements, for example, these plans don't meet the asset limitation necessities of the WSNs; and all the more particularly, for the substantial scale WSNs. Likewise, these plans experience the ill effects of higher cost related with trust assessment particularly of inaccessible hubs. Besides, existing plans have some different confinements, for example, reliance on particular steering plan, similar to the PLUS plan takes a shot at the highest point of the PLUS R directing plan; reliance on particular stage, similar to the ATRM plot requires an operator based stage; and unreasonable presumptions, similar to the ATRM accept that specialists are versatile against any security dangers, and so forth. In this way, these works are not appropriate for practical WSN applications. In this manner, a lightweight secure trust administration plan is expected to address these issues.

4.1.3 Recommended 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 shows our Trust Management component in general sensor node architecture.

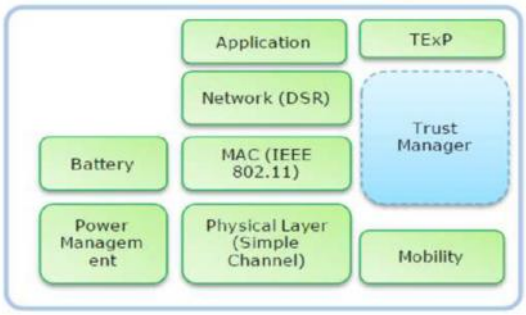

Fig 5. Sensor Node Architecture with our Trust Management Component.

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 necessity is accomplished with the assistance of utilizing improved aloof affirmations (PACK) by catching the transmission of a next bounce on the course, since they are inside radio range [17]. On the off chance that the sender hub does not catch the retransmission of the bundle inside a timeout from its neighboring hub or caught parcel is observed to be illicitly manufactured (by contrasting the payload that is appended with the parcel) then the sender hub will consider that connection as an unsuccessful one. On the off chance that the quantity of unsuccessful connections expands, then the sender hub diminishes the trust estimation of that neighboring hub and may consider it as a flawed or noxious hub.

The proposed confide in model works with two topologies. One is the intra-assemble topology where circulated trust administration is utilized. The other is between gathering topology where brought together trust administration approach is utilized. For the intra-aggregate system, every sensor that is an individual from the gathering, figures singular trust esteems for all gathering individuals. In view of the trust esteems, a hub allots one of the three conceivable states: 1) confided in, 2) un-trusted or 3) un-sure to other part hubs. This three-state arrangement is decided for scientific effortlessness and is found to give suitable granularity to cover the circumstance. From that point forward, every hub advances the trust condition of all the gathering part hubs to the CH. At that point, concentrated trust administration assumes control. In view of the trust conditions of all gathering individuals, a CH identifies the malevolent node(s) and advances an answer to the base station. On ask for, each CH additionally sends trust estimations of different CHs to the base station. When this data achieves the base station, it allots one of the three conceivable states to the entire gathering. On ask for, the base station will forward the present condition of a particular gathering to the CHs. Our gathering based trust demonstrate works in three stages: 1) Trust estimation at the hub level, 2) Trust count at the bunch head level, and 3) Trust computation at the base station level.

V. 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, 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 Recommended 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 Figure5.3.1.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.

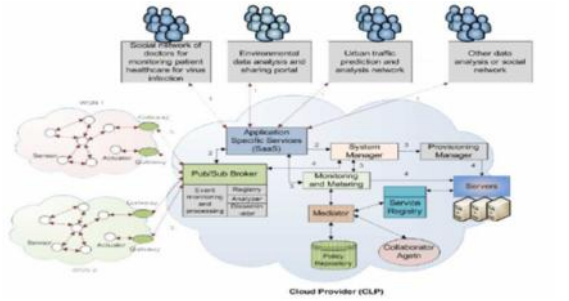

Figure 6. Framework of WSN cloud integration.

VI. Proposed Methodology

In this venture, we are investigated the confirmation and trust and notoriety computation and administration of CSPs and SNPs which are two exceptionally basic and scarcely investigated issues as for CC and WSNs combination. We proposed a novel ATRCM framework for CC-WSN mix. The proposed ATRCM framework accomplishes the accompanying three capacities for CC-WSN incorporation: Authenticating CSP and SNP to maintain a strategic distance from vindictive pantomime assaults. Figuring and overseeing trust and notoriety with respect to the administration of CSP and SNP. Helping CSU pick attractive CSP and helping CSP in choosing proper SNP, also, our framework security examination fueled by three enemy models demonstrated that our proposed framework is secure versus primary assaults on a trust and notoriety administration framework, for example, great mouthing, sassing, intrigue and white-washing assaults, which are the most critical assaults.

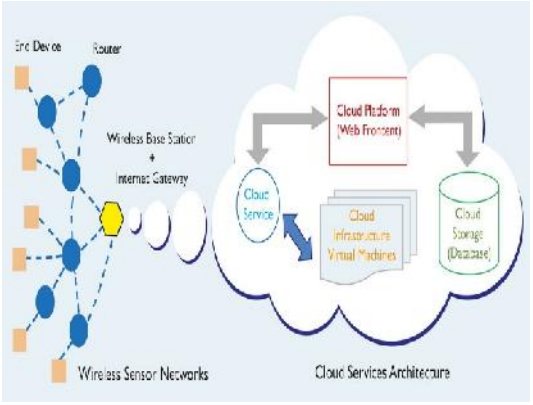

Fig 7 Proposed System Architecture.

Proposed Algorithm

A) Authentication flowchart of CSP and SNP:

Step 1: CSPs provide the certificate to CSU and CSU checks whether the signature of the certificate is valid and whether the certificate is revoked. CSU filters the CSPs that are not qualified.

Step 2: SNPs offer the certificate to CSP and CSP checks whether the signature of the certificate is valid and whether the certificate is revoked. CSP filters the SNPs that are not qualified.

B) Trust and reputation calculation and management between CS U and CSPs:

Step 1: CSU checks whether the characteristics of CSPs satisfy the attribute requirement of CSU. Filter the CSPs that are not satisfied.

Step 2: CSU issues requests to TCE and achieves the value of the service from CSP to the CSU. CSU checks whether the value is greater than or equal to the value. Filter the CSPs that are not satisfied.

$$T_{cu} \geq \bar{T}_{scu}$$

Step 3: CSU issues requests to TCE and achieves the value of the service offered by the CSP. CSU checks whether the Rc value is greater than or equal to the value. Filter the CSPs that are not satisfied.

$$R_c \geq \bar{R}_{sc}$$

Step 4: CSU calculates the value between CSC of CSP and DSP of CSU and checks whether the Cc value is within the range. Filter the CSPs that are not satisfied.

Step 5: CSU checks whether ctc is revoked and chooses the service offered by the CSP with the maximum Mc and informs TCE about signed SLA or PLA.

$$M_c = -\alpha_c \cdot \frac{C_c}{|C_{bc}|} + \beta_c \cdot T_{cu} + \gamma_c \cdot R_c$$

Step 6: CSU checks whether ctc is revoked before using the service from the CSP. CSU sends feedbacks about the service of the CSP to TCE (Trusted Center Entity) based on PLA (Privacy Level Agreement) and SLA (Service Level Agreement) after the termination of service. TCE stores and updates the value as well as the value.

VII. Conclusion:

There are numerous studies performed on trust otherwise status of cloud. Regarding rely on cloud computing-wireless systems integration, the

attached jobs are concentrate on how trust management might enhance security of cloud incorporated sensor network. Modern techniques of cloud computing and wireless systems integration focus simply on authentication of users otherwise data. Ideas introduce a manuscript and authentic trust furthermore to status calculation and management system intended for the mix of cloud computingwireless systems. In the last works, there's no study which has examined the authentication in addition to consider and standing of sensor network and cloud providers for cloud computing-wireless systems integration. Forecasted system will achieve three functions for example authentication of cloud service furthermore to sensor network providers to influence obvious of malicious impersonation attacks managing of trust and standing concerning service of cloud service furthermore to sensor network providers and assisting cloud service users to select desirable cloud providers and assisting them in choice of appropriate providers of sensor network. We inspect trust furthermore to authentication and standing calculation furthermore to handle over cloud service and sensor network providers that are two essential and hardly explored issues concerning cloud computing and wireless network integration.

References:

[1]Q. Zhang, L. Cheng, and R. Boutaba, —Cloud computing: State-of-theart and research challenges,‖ J. Internet Services Appl., vol. 1, no. 1, pp. 7–18, 2010. 130 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015.

[2]R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, —Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,‖ Future Generat. Comput. Syst., vol. 25, no. 6, pp. 599–616, Jun. 2009.

[3]J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, —Green cloud computing: Balancing energy in processing, storage, and transport,‖ Proc. IEEE, vol. 99, no. 1, pp. 149–167, Jan. 2011.

[4]K. M. Sim, —Agent-based cloud computing,‖ IEEE Trans. Services Comput., vol. 5, no. 4, pp. 564–577, Fourth Quarter 2012.

[5]I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, —Wireless sensor networks: A survey,‖Comput. Netw., Int. J. Comput. Telecommun. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.

[6]C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, and L. T. Yang, —A survey on communication and data management issues in mobile sensor networks,‖ Wireless Commun. Mobile Comput., vol. 14, no. 1, pp. 19–36, Jan. 2014.

[7]M. Li and Y. Liu, —Underground coal mine monitoring with wireless sensor networks,‖ ACM Trans. Sensor Netw., vol. 5, no. 2, Mar. 2009, Art. ID 10.

[8]M. Yuriyama and T. Kushida, —Sensor-cloud infrastructure—Physical sensor management with virtualized sensors on cloud computing,‖ in Proc. 13th Int. Conf. Netw.-Based Inf. Syst., Sep. 2010, pp. 1–8.

[9]G. Fortino, M. Pathan, and G. Di Fatta, —BodyCloud: Integration of cloud computing and body sensor networks,‖ in Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci., Dec. 2012, pp. 851–856.

[10] Y. Takabe, K. Matsumoto, M. Yamagiwa, and M. Uehara, —Proposed sensor network for living environments using cloud computing,‖ in Proc. 15th Int. Conf. Netw.-Based Inf. Syst., Sep. 2012, pp. 838– 843.