A Cloud-based Architecture for Secure and Reliable Service Provisioning in Wireless Sensor Network

Fatemeh Banaie
Network Research Laboratory, Department of Engineering
Ferdowsi University of Mashhad
Mashhad, Iran
banaie_f@stu-mail.um.ac.ir

Seyed Amin Hosseini Seno
Network Research Laboratory, Department of engineering
Ferdowsi University of Mashhad
Mashhad, Iran
hosseini@um.ac.ir

***Abstract*—Nowadays, the use of wireless sensor networks in various applications areas such as environmental monitoring, military and industrial fields has rapidly increased. However, the limitations of WSN in the terms of memory, computation, energy and scalability, limit the usability of sensor data. We need a powerful and scalable computing infrastructure to increase the utilities of WSN. Sensor-cloud infrastructure has been proposed to provide a flexible platform for collecting, processing and sharing of large amount of sensor data from different applications. This paper focuses on secure processing of sensor data in the collaboration of WSN and cloud, and proposes a novel data processing framework for integrating WSN with cloud computing.**

Keywords*—computing infrastructure; cloud computing; flexible platform; integrating (keywords)

I. INTRODUCTION

In recent years, wireless sensor network applications have been used in various industrial, commercial and environmental fields. A typical sensor network contains distributed sensor devices that can cooperatively monitor physical and environmental conditions [1]. These sensors have limited sensing capability, low processing power and communication bandwidth. But when the area is vast like environmental monitoring and industrial automation, the amount of data gathered by wireless sensor networks is large. This creates many challenges in the terms of sensing and computational resources and storage capacity. Thus, there must be an infrastructure on which users could easily access the data produced by sensor networks [2].

In the midst of these issues, cloud computing has emerged as a new computing paradigm to provide unlimited resources, dedicated servers, software and data on demand. Cloud computing also provides users with virtual servers. Users can utilize the virtual servers from anywhere anytime without concern about their detailed specifications [3].

Sensor-cloud infrastructure is the extended form of cloud computing to solve the issues in large-scale sensor network applications [1]. Fig. 1 shows an overview of sensor-cloud infrastructure. As seen, multiple sensor networks with different owners can join this infrastructure, and share their physical sensors. There are some templates for virtual sensors. Users can select among them for requesting a virtual sensor [3]. The advantages of this integration is storage capacity of data and processing of these data using immense processing power and providing quick response to the user. Such an infrastructure enables the collecting, processing and sharing of large amount of sensor data from different applications [4].

Despite the benefits of the sensor-cloud, this system bring various security threats. Since multiple applications may use resources from multiple networks with different owners, it is complicated to provide security in such a heterogeneous environment. Therefore, the design and integration of security issues, like authentication and data confidentiality for ensuring trusted computing of the emerging technology, need to be taken into account.

In this paper, our primary goal is to develop an infrastructure for secure sensor-cloud services. The rest of this paper is organized as follows. In section 2, we provide a brief overview of concepts including definitions and security challenges of sensor-cloud. Section 3 describes the proposed security framework in integration sensor network with cloud.

978-1-4799-5487-2/14/$31.00 ©2014 IEEE

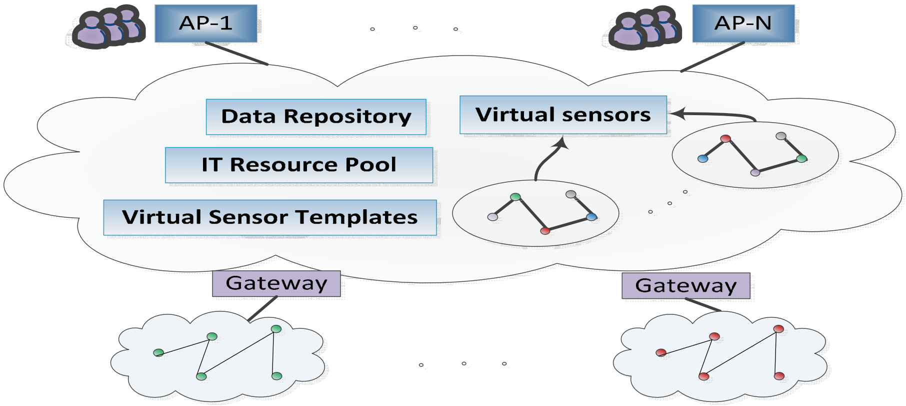

Figure 1. Brief overview of sensor-cloud Architecture.

Finally, the paper is concluded in section4.

II. STATE OF THE ART

Sensor networks are usually deployed for specific purposes, and these sensors are only used by their own application. Sensor-cloud infrastructure enables users to easily collect, access, share and utilize a large number of sensor data from multiple applications by virtualization of the physical sensors on cloud computing platform [1]. But the benefits of this integration could be hindered by various security challenges in the terms of data confidentiality, privacy and integrity. Data gathered by sensors may contain sensitive information, and the owner of data wants to conceal sensitive data from others. Hence, the confidentiality and protection of sensed data should be guaranteed while being stored and processed in cloud [5]. Therefore, we need some trusted services to protect sensitive information. These services should be formed quickly and efficiently to maximize the service productivity.

Several works have been proposed to address security issues in cloud computing. Cloud Security Alliance (CSA) [6] provides some open standards like SAML [7], TLS [8], etc to achieve authentication for service providers. The work presented in [9], proposed a security model of Identity-Based Cryptography (IBC), which was firstly introduced by Shamir in [10], and are based on bilinear pairing on elliptic curve. Hierarchical identity-based cryptography (HIBC) was proposed by [11], to improve the scalability of these schemes.

Identity-based cryptography (IBC) is a kind of public-key based schemes that uses the identity of users as the public key rather than a random string. IBC significantly reduced the complexity of key management and signature as public keys are not required to be distributed securely to participants. An IBC based system consists of 4 phases as follow:

1. *Setup:* PKG creates a master key K_m , which is kept secret and used to derive user's private keys, and a set ρ of system parameters that are made public.
2. *Key Extraction:* This algorithm takes ρ, K_m and identity of the user $ID \in \{0,1\}^*$ and generate the private key P for user.
3. *Encryption:* User can use ρ, reciver's ID and a message $m \in M$ to generate the cipher text $c \in C$.
4. *Decryption:* Receiver can use system parameter ρ and his private key P to decrypt the cipher text.

With federated identity management service providers can easily share identity information to access different networks. In this method, when user log in successfully one time, they can access multiple networks without having to log in again [12].

III. PROPOSED ARCHITECTURE

Sensor-cloud infrastructure provides various real-time auto generated data to support wide ranges of application services. However, sensors have different levels of resource capabilities, and applications have their own characteristics and requirements in terms of bandwidth, delay, packet loss and etc. Thus, application developers need to understand these details for implementing the application services [13]. The proposed infrastructure has an appropriate communication middleware to facilitate connecting sensors and application services.

A. System Overview

Fig. 2 illustrates the overall view of the proposed sensor-cloud integration framework. It is divided mainly into three major components: Application Processing Layer (APL), Managerial Layer (ML) and Data Management Layer (DML).

1) *Application Processing Layer:* The Application Processing Layer encapsulates applications and an associated local processing unit (LPU) with each application. The required resources and QoS parameters is evaluated by its associated LPU, then they are forwarded to the Global Managerial Layer.

2) *Global Managerial Layer:* This layer makes the management decisions (e.g. life-cycle of Virtual sensors (VS), number of VS allocated to the applications and etc.) based on received parameters from other layer. It also provides users by secure sensor information services for authentication and access management to prevent users from accessing and breaching confidential information.

3) *Data Management Layer:* DML receives the data from gateway, then process data and add it to data repository. It also gives sensor owners the menus for registering and deleting their physical sensors to the sensor-cloud infrastructure.

In the following, we describe the inner workings of layers components.

B. Dynamic collaboration of sensor-cloud components

As seen in Fig. 2, sensor data is passed through gateway to data processing unit (DPU) in Data Management Layer. DPU determines whether to send the received data immediately or to store in data repository for periodic send. Sensor owners connect to the physical sensor manager for registering or deleting their physical sensors. Physical sensor manager provisions templates for virtual sensors. User data request is forwarded to LPU, which assess the level of the requested service on the basis of service-level metrics (response time, data rate and etc.). Global Processing Unit (GPU) is responsible for managing resource requirements coming from APL. After authenticating the users and applications, GPU will give the access to them according to the account policies. GPU receives required resources from APL and system-level performance metrics such as CPU load and available memory from physical and virtual servers. Then, it makes managerial decisions including allocating and preempting a virtual servers and virtual server groups to the applications, changing virtual server's resource capacity and e.t. It should allocate VS group $G_i = (g_{i1}, \dots, g_{in})$ for each application A_i so that maximize the global utility and minimize the number of active physical servers [14]. To ensure that the total load on servers is less than or equal to the capacity, the allocation of VS to applications must constrained by the total of capacity of resources in servers such as CPU and memory.

$$\sum_{i=1}^{n} c_i . r_k^{Resource} \leq \sum_{k=1}^{m} C_k^{Resource} \qquad (1)$$

Where $C_k^{Resouce}$ is the resource capacity of server j, c_i is the number of VS assigned to application A_i and $r_k^{Resource}$ is the required resources by VS_i. The allocation of virtual sensors to applications needs to maximize global utility, while minimizing overall cost function.

$$maximize \sum_{i=1}^{n} U(C_i) - C(S_i) \times \gamma_{ik}$$

Subject to:

$$\sum_{i=1}^{n} c_i . r_k^{Resource} \leq \sum_{k=1}^{m} C_k^{Resource} \qquad (2)$$

$$r_k^{Resource} \geq 0$$

Where $C(S_i)$ is cost function which is the number of active servers and γ_{ik} is defined as:

$$\gamma_{ik} = \begin{cases} 1 & if\ VS_i\ is\ assigned\ to\ server\ k \\ 0 & otherwise \end{cases}$$

To provide requested data for applications, GPU calls the provisioning server. PS receives input parameter such as template *ID*, user *ID* and sensor group *ID* and provisions the virtual sensors, and virtual sensor groups. After provisioning it notifies the global processing unit.

GPU permanently monitors servers and applications and decides to allocate new VS to the applications or physical servers or preempt them based on the workload of the servers and the satisfaction of applications.

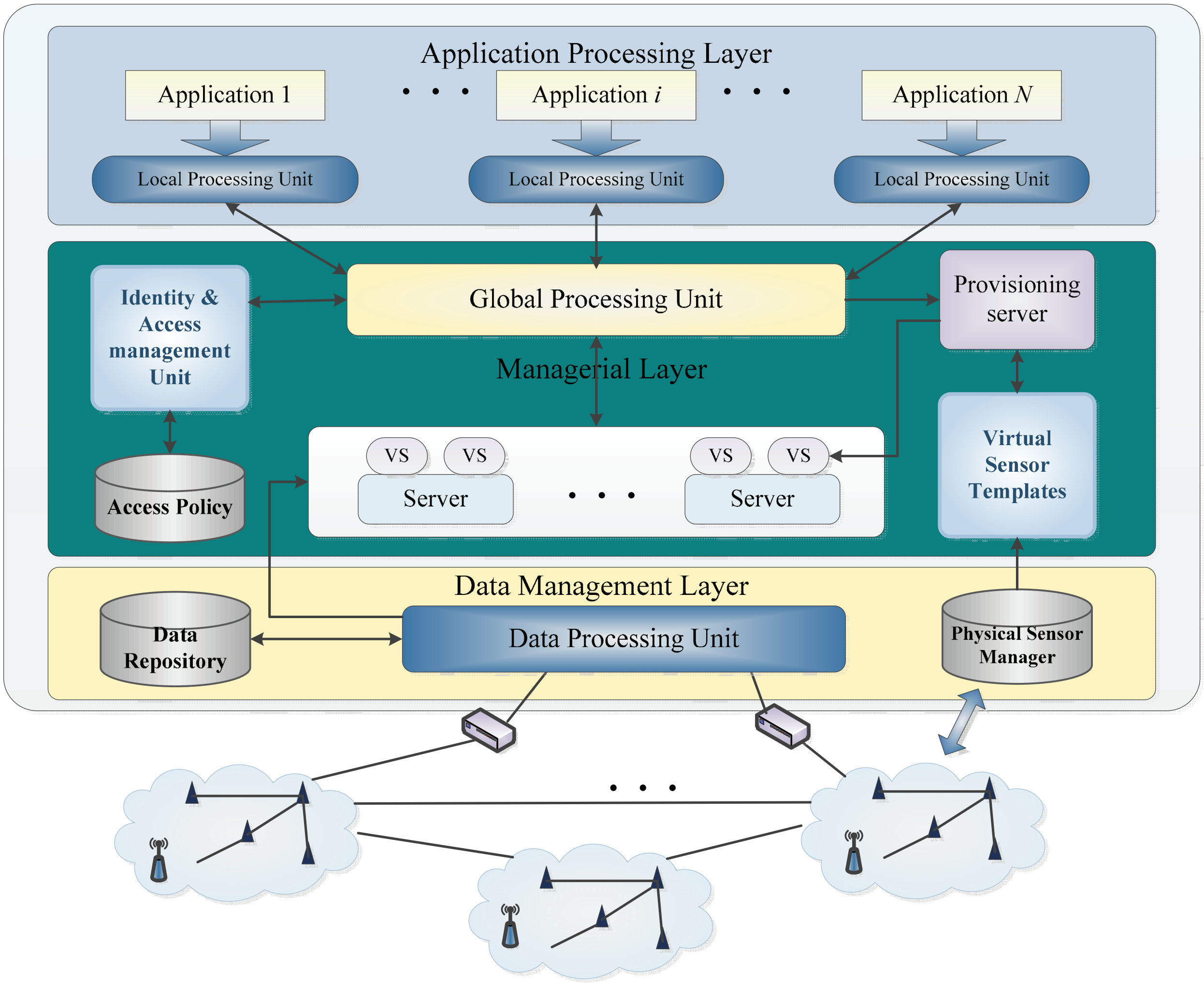

Figure 2. General overview of the proposed architecture..

C. Secure Service Provisioning

The aim of the proposed security model is to provide strong security by authentication and access control to sensor-cloud resources. In this paper, we propose to use identity based cryptography to simplify the key distribution and authentication in sensor-cloud Infrastructure. As discussed, identity based encryption uses uniquely known identification of user as public key for encryption and signature verification, which significantly reduces the complexity of key management process. There are several assumptions that must be considered before applying this method:

1. The identity of users which are publicly known must be unique.
2. A unique identity is assigned to each virtual sensor and virtual sensor group when they are generated.
3. We have two private key generators (PKG), one for users and the other for virtual sensors.

In the following, we describe the proposed key management scheme briefly.

a) Key Generation in System

Key generation and distribution are the important part of identity based cryptography. At first, each of PKG_s and

PKG_u generate an additive group G_1 and multiplicity group G_2, which are two subgroups of some large prime order q. Then they choose an appropriate admissible Weil pairing $\hat{e}: G_1 \times G_1 \rightarrow G_2$, with the following properties.

1. Billinear: For all $P, Q \in G_1$ and $a, b \in Z_q^*$, $\hat{e}(aP, bQ) = \hat{e}(bP, aQ) = \hat{e}(P, Q)^{ab}$.
2. Non degenerate: There exist $P, Q \in G_1$, such that $\hat{e}(P, Q) \neq 1$.
3. Computable: For all $P, Q \in G_1$, there is an effective method to calculate $\hat{e}(P, Q)$.

Each PKG chooses an arbitrary generator $P \in G_1$ and cryptography hash functions $H_1: \{0, 1\}^* \rightarrow G_1$ and $H_2: G_2 \rightarrow \{0, 1\}^*$. It also selects random number $\mu \in Z_q^*$, which is known only by PKG and sets $Q_0 = \mu P$. Therefore $(G_1, G_2, \hat{e}, P, Q_0, H_1, H_2)$ are system parameters and are public available and $\mu \in Z_q^*$ is the PKG's master key.

b) Identity-based Encryption and Digital Signature

The algorithm computes $Q_{S_i} = H_1(ID) \epsilon G_1^*$ and sets the private key d_{S_i} as $d_{S_i} = kQ_{S_i}$. When S_1 wants to send message m to S_2, it get the identity of S_2 by requesting PKG. Then, it selects a random number $n \in Z_q^*$ and computes $C = (nQ_0, H_2(\hat{e}(Q_{S_2}, Q_0)) \oplus m)$ where $\hat{e}(Q_{S_2}, Q_0) \epsilon G_2^*$.

After receiving the ciphertext $C = < U, V >$ by S_2 , it decrypts the message by its private key $d_{S_2} \epsilon G_1^*$ as follow:

$$M = H_2(d_{S_2}, U) \oplus V$$

Several applications may run simultaneously on sensor networks. These applications may use one or multiple virtual sensors. So, information exchanged among one sensor group must be isolated from others. In other words, only sensors in the same group can exchange information with each other. For secure communication among virtual sensor, we can use identity based cryptography with virtual sensor ID and group ID. The communication process is as follow:

1. PKG_s chooses an arbitrary generator $P_s \in G_1$ and hash functions $H_1: \{0, 1\}^* \rightarrow G_1$ and $H_2: G_2 \rightarrow \{0, 1\}^*$.
2. It also selects random number $\mu \in Z_q^*$, and sets $Q_s = \mu P_s$. $(G_1, G_2, \hat{e}, P_s, Q_s, H_1, H_2)$ are system parameters and $\mu \in Z_q^*$ is the PKG_s 's master key.
3. The algorithm computes $Q_{S_i} = H_1(ID_{S_i} || ID_{g_j}) \epsilon G_1^*$ and set the private key d_{S_i} as $d_{S_i} = k_1 Q_{S_i}$.
4. Virtual sensor i encrypt message M as : $C = (nQ_s, H_2(\hat{e}(Q_{S_j}, Q_0)) \oplus m)$ where $\hat{e}(Q_{S_j}, Q_0) \epsilon G_2^*$ and $n \in Z_q^*$ ia a random selected number, and sends it to virtual sensor *j*.
5. VS_jobtains $M = H_2\left(d_{S_j}, U\right) \oplus V$, by its private key $d_{S_j} \epsilon G_1^*$.

IV. CONCLUSION

With the presence of sensor networks in several application fields many challenges have emerged in the terms of flexibility, scalability and heterogeneous information services. Cloud computing is a solution to overcome the limitations of WSNs. The integration of WSN with cloud provides greater flexibility, unlimited resources, immense processing power and providing quick response to the user. But storing data on cloud brings some security challenges, as the owner of data has no control over it. In this paper, we have presented a new architecture for securing sensor-cloud services. The proposed architecture simplifies the key distribution and authentication; therefore it accelerates service provisioning in sensor-cloud Infrastructure.

V. REFRENCES:

[1] A.Alamri, W.Sh Ansari, M.M. Hassan, M. Sh. Hossain, A.Alelaiwi, and M.A. Hussain, "A survey on sensor-cloud: Architecture, Applications, and Approaches", International Publishing Corporation, 2012.

[2] M. Hasmat ullah, J. No, G. H. Kim, " A Collaboration Mechanism Between Wireless Sensor Network and a Cloud Through a Pub/Sub-based Middleware Service", The Fifth International Conference on Evolving Internet, 2013.

[3] M. Yuriyama, T. Kushida, "Sensor-cloud Infrastructure: Physical Sensor Management with Virtualized Sensors on Cloud Computing", 13th International conference on Network-Based Information Systems, 2010.

[4] T-D. Nguyen, E-N Huh, "An efficient key management for secure multicast in sensor-cloud", ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering, 2011.

[5] M. Eggert, R. Haubling, M. Henze, L. Hermerschmidt and at all , “SensorCloud: Towards the Interdisciplinary Development of a Trustworthy Platform for Globally Interconnected Sensors and Actuators” , Wissenschaftliche Ergebnisse der Trusted Cloud Initiative, 2013.

[6] Security guidance for critical areas of focus in cloud computing v2.1. Cloud Security Alliance. Available: https://cloudsecurityalliance.org/csaguide.pdf, 2009.

[7] Security assertion markup language (saml) v2.0. Organization for the Advancement of Structured Information Standards (OASIS). Available: http://docs.oasisopen. org/security/saml/v2.0/saml-2.0-os.zip, 2009.

[8] B. P. Bruegge, D. Huhnlein, and J. Schwenk. “Tls-federation-a secure and relying-party-friendly approach for federated identity management”, In proceeding of: BIOSIG , 2008.

[9] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” *SIAM J. Comput.*, vol. 32, pp. 586–615, March 2003.

[10] A. Shamir, “Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg, 1985.

[11] C. Gentry, A. Silverberg, “Hierarchical ID-Based cryptography”, ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg, 2002.

[12] L.Yan, Ch. Rong, G. Zhao, “Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography”, CloudCom 2009, LNCS 5931, pp. 167–177, 2009.

[13] Y. Lim, J. Park, ‘Sensor Resource Sharing Approaches in Sensor-Cloud Infrastructure”, International Journal of Distributed Sensor Networks, 2014.

[14] H-N. Van, F-D. Tran, J-M. Menaud, “SLA-aware Virtual Resource Management for Cloud Infrastructures ”,IEEE Ninth International Conference on Computer and Information Technology.