2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks

Integrating Wireless Sensor Networks with Cloud Computing

Khandakar Ahmed
RMIT University
S3278694@student.rmit.edu.au

Mark Gregory
RMIT University
mark.gregory@rmit.edu.au

Abstract— **Wireless Sensor Networks (WSN) has been a focus for research for several years. WSN enables novel and attractive solutions for information gathering across the spectrum of endeavour including transportation, business, health-care, industrial automation, and environmental monitoring. Despite these advances, the exponentially increasing data extracted from WSN is not getting adequate use due to the lack of expertise, time and money with which the data might be better explored and stored for future use. The next generation of WSN will benefit when sensor data is added to blogs, virtual communities, and social network applications. This transformation of data derived from sensor networks into a valuable resource for information hungry applications will benefit from techniques being developed for the emerging Cloud Computing technologies. Traditional High Performance Computing approaches may be replaced or find a place in data manipulation prior to the data being moved into the Cloud. In this paper, a novel framework is proposed to integrate the Cloud Computing model with WSN. Deployed WSN will be connected to the proposed infrastructure. Users request will be served via three service layers (IaaS, PaaS, SaaS) either from the archive, archive is made by collecting data periodically from WSN to Data Centres (DC), or by generating live query to corresponding sensor network.**

Keywords-Identity and Access Management, Publish/Subscribe Broker, Kerberos Protocol, Diffie-Hellman.

I. INTRODUCTION

Cloud Computing permits companies to increase capacity quickly without the need for new infrastructure investment and similarly companies can decrease capacity quickly and efficiently. In a recent IBM report it was stated that the "Cloud is a new consumption and delivery model for many IT-based services, in which the user sees only the service, and has no need to know anything about the technology or implementation." [1]. According to the US National Institute of Standards and Technology (NIST) "Cloud Computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources" [2]. With pools of computing power, network, information and storage resources the cloud offers the use of a collection of services, applications, information and infrastructure. Cloud components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down providing for an on-demand utility-like model of allocations and consumption [3]. On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service are five essential characteristics of Cloud Computing depicted by NIST [4].

Services provided by Cloud Computing can be categorized into three classes: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). IaaS provides consumers with an opportunity to consume processing, storage, network, and other fundamental computing resources. Here the consumer is able to store data, deploy and run arbitrary software such as operating systems and applications. The consumer does not need to control and manage the underlying infrastructure but has control over the operating system, applications, storage, and network components. In this service approach, the customer contracts to use servers, the data centre fabric, networking, storage and other facilities [5]. By adopting PaaS consumers can host applications using platforms which include the runtime software necessary to host consumer developed applications. Here also the consumer has no control on the underlying infrastructure but does have control over the deployed applications and application hosting specific configurations. Web 2.0 application runtime, Java runtime, middleware, database, and development tooling are a few example of services provided in this layer [6][7]. In SaaS a vendor supplies hardware infrastructure and software products through a front-end portal. The SaaS concept provides a broad market solution that may include anything from web based email to inventory control and database processing. End users can access the service over the Internet. Service examples include: collaboration, business processes, industry applications, e-Health and CRM/EPR/HR [8].

A vast sea of sensors which have been connected to the global network has started another information revolution and an explosion in our ability to create, store and mine digital gathered information from the sensors. Wireless Sensor Networks (WSN) has moved from an early research topic to the point where the number of implemented WSN is growing rapidly.

Cloud Computing is principally designed and promoted to be data centre centric and efficient interaction with the outside world is an area where improved solutions are being sought. WSN are designed to collect data in the real world, yet, the question arises as to what to do with the data when the organisation that collected the data no longer requires it. There are many reasons for the data to be kept including historical, future research, and re-analysis at some future point in time.

978-0-7695-4610-0/11 $26.00 © 2011 IEEE
DOI 10.1109/MSN.2011.86

There is a possible linkage between WSN and Cloud Computing and the eventual shift of data into the cloud and over time into the public domain.

In this paper an integration framework is proposed between WSN and Cloud Computing. The objective of the integration framework is to facilitate the shift of data from WSN to the Cloud Computing environment so that the scientifically and economically valuable data may be fully utilised.

The paper is organized as follows: Section II presents related work. Section III describes implementation scenarios. Section IV illustrates the proposed framework. Section V presents the conclusion and future work.

II. PROPOSED FRAMEWORK EASE OF USE

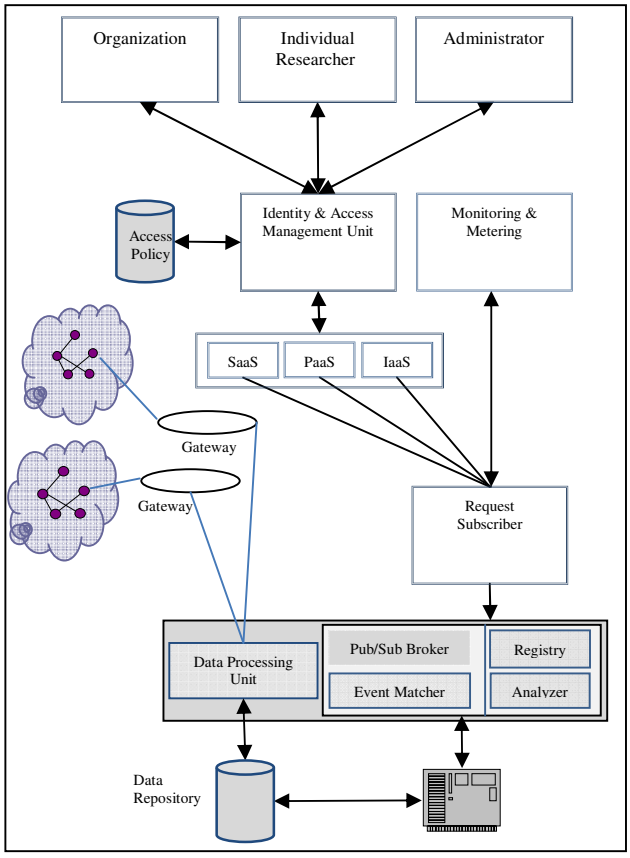

Figure 1: Sensor-Cloud Integration Framework

Figure 1 shows the WSN and Cloud Computing integration framework. The framework components include: Data Processing Unit (DPU), Pub/Sub Broker, Request Subscriber (RS), Identity and Access Management Unit (IAMU), and Data Repository (DR). Data collected from the WSN moves through a gateway to the DPU. The DPU will process the data into a storage format and then send the data to the DR.

Users will connect to the Cloud through the secured IAMU and will be given access on the basis of the policy stored against their user account. After access has been granted users can put forward data access requests. The requests will be forwarded to the RS and the RS will create a subscription on the basis of this request and forward this subscription to the Pub/Sub Broker. Data received in the cloud will be identified by the DPU which will create a published data event and send the event to an event queue at the Pub/Sub Broker. When a new event is published, each subscription is evaluated by the event matcher. Once the event matching process finds a match the published data is made available to the user after further processing is carried out if required.

A. *Identity and Access Management Unit:*

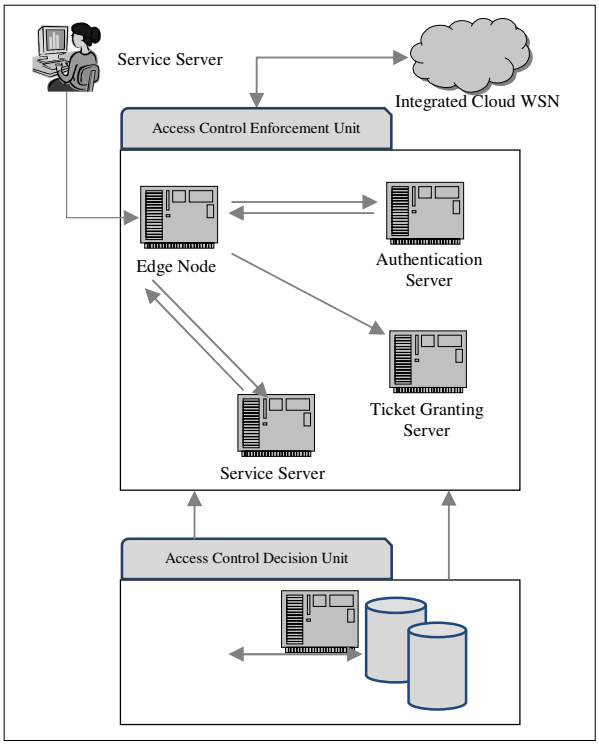

Figure 2: Schematic Diagram of Overall IAMU System

In this section a prototype Identity and Access Management Unit (IAMU) is described that includes Diffie-Hellman, Kerberos, Role Based Access Control (RBAC) and Extensible Markup Language (XML) based upon previous work [9]. The primary purpose of this model is two-fold: firstly to provide strong authentication between customer and provider; and secondly to provide a strong policy based access control to cloud resources. Clients will communicate with the provider through the Identity and Access Management Unit (IAMU) which will provide both authentication and access control. Figure 2 shows the IAMU system which includes two major components: Access Control Enforcement Unit (ACEU); and Access Control Decision Unit (ACDU). A slight modification has been to the Kerberos authentication implementation [10] introducing a new unit called the Edge Node (EN) which also implements the Diffie-Hellman public key

1) *Access Control Enforcement Unit*

The ACEU consists of the Edge Node (EN) and three servers: Authentication Server (AS), Ticket Granting Server (TGS), and Service Server (SS). A request arrives at the EN and then it goes to the AS. The EN implements Kerberos to authenticate the client with the AS.

2) Access Control Decision Unit

The ACDU consists of the RBAC Processor and the user policy storage. The ACDU will communicate with the ACEU through the SS.

The authentication process associates users with access policies and after this process has completed the user gains access to data resources within the limitations imposed by the access policies. The proposed framework includes control, group and user management and other information that is stored utilizing XML.

3) Flow of Interaction Between User and IAMU

Figure 3 shows the interaction between user and Identity and Access Management Unit. The description of different messages those have been exchanged among different servers and edge node (EN) are left out of the scope of this poster due to the space constraint.

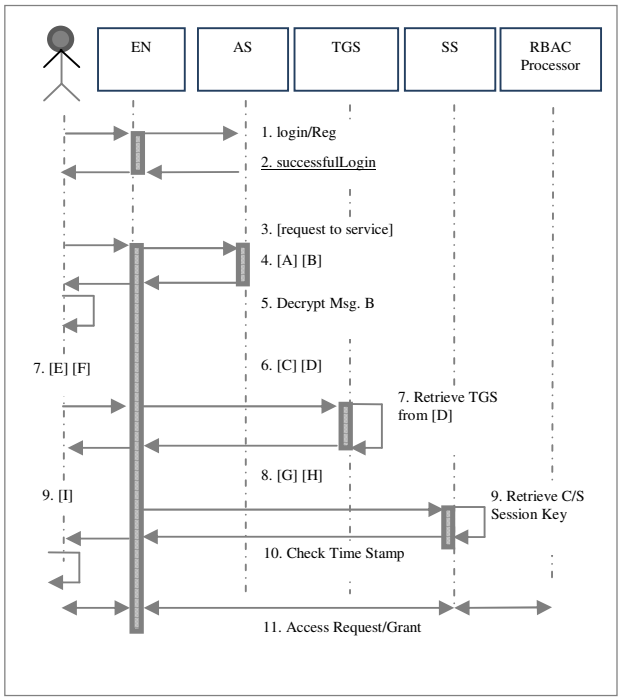

Figure 3: IAMU Sequence Diagram

B. Flow of Interaction among Framework Components

Figure 4 shows the interactions among different components of the framework. The description of the flow left out of the scope of this poster due to space constraint.

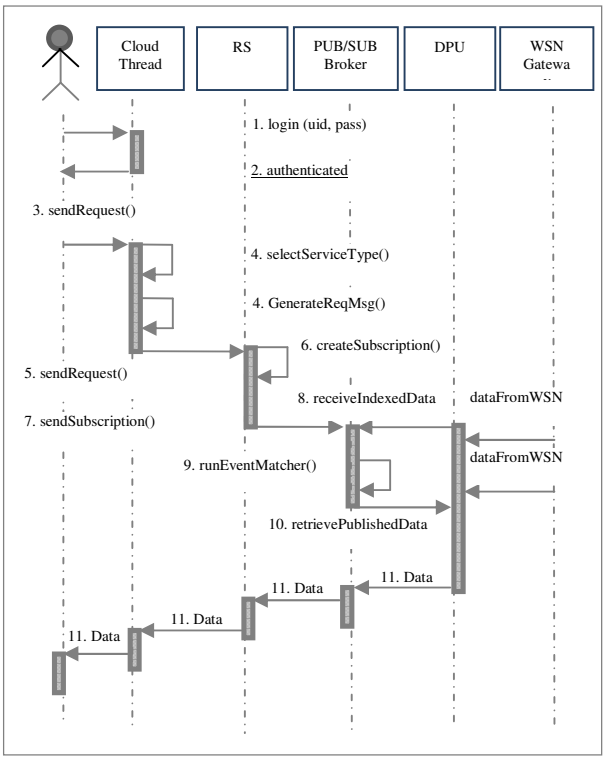

Figure 4: Flow of Interaction among Framework Components

REFERENCES

[1] F. Schepers. (2010) Security in Cloud Computing, IBM Tivoli Internet Security Systems. [Online]. Available: http://www.cpdpconferences.org/Resources/Schepers.pdf. Last accessed: 10/11/2010.

[2] P. McDaniel, and S. W. Smith, "Outlook: Cloud Computing with a Chance of Security Challenges and Improvements," IEEE Computer and Reliability Socities 2010, pp. 77-80, Jan. 2010.

[3] R. Marchany. (2010) VA Tech IT Security Cloud Computing Security Issues. [Online]. Available: http://www.security.vt.edu/Downloads/training/Cloud%20Computing%20Security%20Issues.pdf. Last accessed: 2/12/2010.

[4] P. Mell, and T. Grance. (2009) Effectively and Securely Using the Cloud Computing Paradigm (v0.25) NIST. [Online]. Available: http://csrc.nist.gov/groups/SNS/cloud-computing/index.html. Last Accessed: 10/11/2010.

[5] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, A. Warfield, "Xen and the Art of Virtualization," in *Proc. of 19th ACM symposium on Operating Systems Principles*, Bolton Landing, NY, USA, October 2003, pp. 164-177.

[6] (2010) Google App Engine. [Online]. Available: http://code.google.com/appengine/. Last Accessed: 15/07/2011

[7] (2007) Sales Force. [Online]. Available: http://www.salesforce.com/platform/. Last Accessed: 10/11/2010

[8] A. Dubey, and D. Wagle. (2007) Delivering software as a service - The McKinsey Quarterly. [Online]. Available: http://www.mckinsey.de/downloads/publikation/mck_on_bt/2007/mobt_12_Delivering_Software_as_a_Service.pdf Last Accessed: 15/08/2011.

[9] K. Ahmed, *Identity and Access Management in Cloud Computing*, 1st ed., LAP Lambert Academic Publishing, Germany, April 2011, ISBN: 978-3-8443-3069-4.

[10] D. Harkins and D. Carrel. (1998) The Internet Key Exchange (IKE), RFC 2409, IETF Network Working Group. [Online]. Available: http://www.ietf.org/rfc/rfc2409.txt. Last Access: 12/01/2011.