RESEARCH ARTICLE OPEN ACCESS

Security Issues Threats and Challenges in Data Management of Wireless Communication & Sensor Network over Cloud: A Review

Padmaja R Ayachit, N. G. Narole
(Department Of Electronics & Communication Engineering, RTMNU Nagpur)

ABSTRACT
Cloud computing is a colloquial expression used to describe a variety of different computing concepts that involve a large number of computers that are connected through a real-time communication network. The five key characteristics of cloud computing are: location-independent resource pooling, on demand self-service, rapid elasticity, broad network access, and measured service. These five characteristics represent the first layer in the cloud environment. Wireless sensor networks (WSNs) are comprised of a variable number of autonomous electronic devices, with possible mechanic components, that have the capability of remote sensing, signal processing and communication in an ad hoc fashion. Today almost every organization and even public sector is moving towards cloud computing, in the form of a provider or consumer. Even this electronically provisioned has not remained untouched by computer hackers, criminals and vandals to break into the web servers. The goal of this paper is to analyze the Cloud based Environment for Wireless Communication & Sensor Network Application along with the Security issues for Data Management.

KEYWORDS: Cloud, web services, security, *IT security, services*.

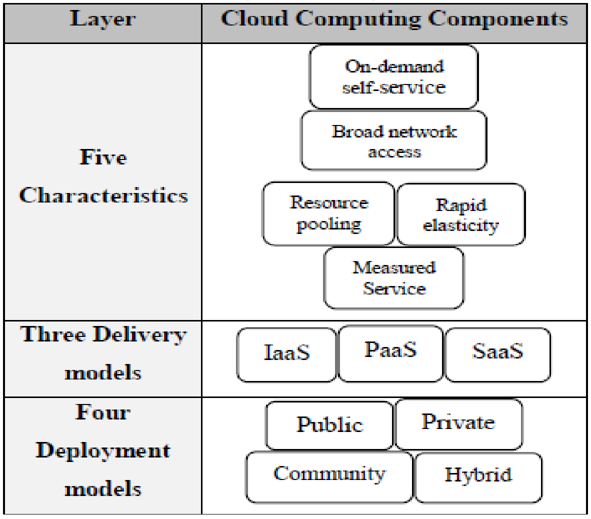
I. INTRODUCTION

Wireless sensor networks (WSNs) are comprised of a variable number of autonomous electronic devices (called motes or sensors), with possible mechanic components, that have the capability of remote sensing, signal processing and communication in an ad hoc fashion. The basic principle is that these autonomous sensor nodes would be scattered over a certain geographic area. However, the lack of infrastructure imposes various difficulties in the design of networking protocols for WSNs. Possible methods of deployment for the motes could be from moving ground units. They have to be self-contained, battery operated, and able to gather data from the surrounding environment and forward it to a predetermined destination. The data gathering is to be done via on-board sensors. Furthermore, motes have to be fairly robust as they are envisioned to operate in potentially hostile and extreme environments. It is because of their fairly robust and autonomous nature that WSNs have been envisioned as an indispensable aid in several areas such as military. health care, industrial manufacturing, security, and agriculture.

1.1 CLOUD COMPUTING

Cloud computing is a colloquial expression used to describe a variety of different computing concepts that involve a large number of computers that are connected through a real-time communication network (typically the Internet).. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.



Layer	Cloud Computing Components
Five Characteristics	On-demand self-service Broad network access Resource pooling Rapid elasticity Measured Service
Three Delivery models	IaaS PaaS SaaS
Four Deployment models	Public Private Community Hybrid

Fig1: Cloud Environment Architecture

The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be un trusted. Dealing with “single cloud” providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards “multi-clouds”, or in other words, “inter clouds” or “cloud-of-clouds” has emerged recently.

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). End users access cloud based applications through a web browser or a lightweight desktop or mobile app while the business software and data are stored on servers at a remote location.

Cloud application providers strive to give the same or better service and performance than if the software programs were installed locally on end-user computers. At the foundation of cloud computing is the broader concept of infrastructure convergence and shared services. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability and less maintenance, and enables IT to more rapidly adjust IT resources (such as servers, storage, and networking) to meet fluctuating and unpredictable business demand The cloud computing model consists of five characteristics, three delivery models, and four deployment models.

The five key characteristics of cloud computing are: location-independent resource pooling, on demand self-service, rapid elasticity, broad network access, and measured service. These five characteristics represent the first layer in the cloud environment. The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking infrastructure facilities, data storage and computing services. In other words, it is the delivery of computer infrastructure as a service. An example of IaaS is the Amazon web service . In PaaS, the user runs custom applications using the service provides infrastructure and providing licensed applications to users to use services is known as SaaS. An example of SaaS is the Salesforce.com CRM application. This model represents the second layer in the cloud environment architecture.

Cloud deployment models include public, private and hybrid clouds. A cloud environment that is accessible for multi-tenants and is available to the public is called a public cloud. A private cloud is available for a particular group, while a community cloud is modified for a specific group of customers. Hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public cloud) . This model represents the third layer in the cloud environment architecture. The infrastructure that is owned and managed by users is in the private cloud. Data that is accessed and controlled by trusted users is in a safe and secure private cloud, whereas the infrastructure that is managed and controlled by the cloud service provider is in a public cloud. In particular this data is out of users control and is managed and shared with unsafe and un trusted servers.

Secure delivery of data to and from the cloud is however a serious issue that needs to be addressed.

WSN and cloud can be integrated through the use of PHP and MYSQL

1.2 SECURITY ISSUES IN CLOUD COMPUTING

Security has always been the main issue for IT Executives when it comes to cloud adoption. However, cloud computing is an agglomeration of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. For example, browser based attacks, denial of service attacks and network intrusion become carry over risks into cloud computing Organizations such as ISACA and Cloud Security Alliance publish guidelines and best practices to mitigate the security issues in the cloud. It includes certain algorithms like encryption and decryption algorithm.

II. CREATION OF CLOUD BASED ENVIRONMENT FOR WCSN

Wireless sensor network (WSN) is a self-organizing network consisting of a lot of sensor devices that connect to others through wireless communication channel in multi-hop manner. Sensors collect environment parameters and transmit sensing data back to a central management node (i.e., a sink node) for further processing. Nowadays, WSN has been applied in many fields, such as environment monitoring, military, surveillance, disaster rescue and healthcare etc., and it is more widely used in the Internet of things (IoT) era. However, sensors are usually low cost devices equipped with limited resources, e.g., processing power, memory, wireless bandwidth, and battery. The design of WSN must take care of these constrains, especially the battery limitation that determines the lifetime of a sensor and a sensor network. All layer protocols used in WSN are optimized to reduce energy consumption, including MAC layer, network layer (routing protocols), transport layer, and cross-layer approaches. Since transmitting operation consumes more energy comparing against sensing and processing operations, some other technologies have been proposed to save energy, e.g., in-network data processing, mobile sink for data collection, and topology reorganization.

Cloud computing is considered as a cost efficient way of IT resource provision manner . It offers a number of advantages such as scalability, agility and economy efficiency, in comparison of traditional IT infrastructure. The cloud computing technology invented by Google is suitable for big data storage and processing. The Hadoop, an open source implementation of Google's cloud by Apache, is widely adopted by many companies. In this paper, we propose a novel architecture based on cloud computing for wireless sensor network. In this architecture, a cloud acts as a virtual sink and collects sensing data in multiple points. Therefore, the WSN is naturally divided into units which we refer as "zones". Each node in the cloud is responsible for data collection of sensors in a zone. The sensors in a zone are organized as a local WSN in flat or hierarchy topology, and these local networks are integrated together by the cloud. As a result, the average end-to-end path length of packet transmission could be shortened, and the energy consumption would be reduced. The required bandwidth for data transmission is reduced as well. Moreover, data in cloud are stored and processed in distributed manner, thus complicated tasks could be completed timely, which would be preferred for large volume data process.

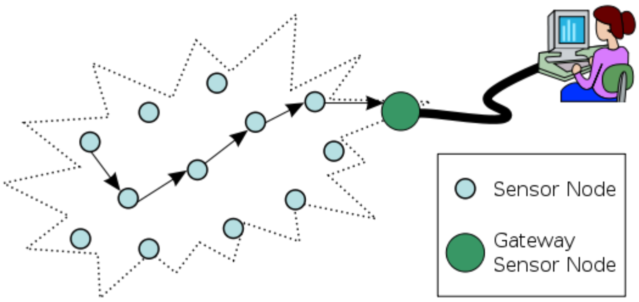


Fig 2:Typical multi-hop wireless sensor network architecture

III. DATA HANDLING OF WCSN

Wireless sensor networks of devices are already being deployed. Robust and efficient deployment of these networks will require as much hands-off configuration and management as possible as the size of these networks increase beyond trial dimensions. Incorporating intelligence in a low cost device is an important requirement if the limited resources of these networks are to be used effectively. This paper proposes a hybrid algorithm that is shown to fulfil some of the important requirements.

Efficient monitoring of environmental conditions over time and space is an important and developing field in it's own right, but also serves as a useful test case for more heterogeneous pervasive networks[5]. Mobile phones, laptops, pdas all have limited bandwidth and battery power but extensive functional capabilities, getting the most out of these devices in an increasingly networked society is a primary goal for ICT research.

A multi-layered algorithm is proposed that provides a scalable and adaptive method for handling data on a wireless sensor network. Statistical tests, local feedback and global genetic style material exchange ensure limited resources such as battery and bandwidth are used efficiently by manipulating data at the source and important features in the time series are not lost when compression needs to be made. The approach leads to a more 'hands off' implementation which is demonstrated by a real world oceanographic deployment of the system.

IV. DATA SECURITY METHODS & ALGORITHMS OVER CLOUD

The 'algorithm' is in fact a hybrid of several decision making and data handling systems. For the purposes of this paper we will assume that the data being handled has passed through some initial pre-processing. For example, tidal flow can be measured by averaging a number of tilt readings over time. Conventional measurement standards regarding the number of tilt readings that need to be gathered over a time period convert ‘tilt readings’ into a single ‘flow’ measurement.

There are therefore 3 decision making components:

1. Sliding Window averaging - We can scan a temporal ‘Sliding Window’ of readings for sufficient deletion conditions.
2. Local Rules - Internal condition monitoring that affects the frequency of some actions, using negative feedback to obtain a homeostatic behavior. A node may carry out none, one or many actions during a specific time period. Actions such as sensing, forwarding and queue management. Each action has a cost in terms of queue occupancy, battery usage and bandwidth usage. By monitoring the condition of these resources the probability of carrying out these actions can be modified. For instance, if the queue length is near it’s maximum it would prudent to take fewer readings and/or to do more forwarding or if the battery is being used at an unsustainable rate higher battery usage behaviors should be reduced and lower usage ones increased. We term this ‘local learning’.
3. Parameter Evolution - A genetic style transfer and fitness based evaluation of internal parameters can enable nodes that are performing well to share their configuration with nodes that are performing less well. Methods 1 and 2 both involve several parameters, values that effect the performance (e.g. Reading at T1 is deleted if + or – Z% of the average of Reading T0,T2. Sensing probability is reduced by X if queue is above Y). Effective values for these parameters are discovered in advance using multi-parameter optimization on a simulated environment. But this can only be as good as the simulated environment. By encoding these parameters in a genetic fashion the performance of the nodes can be evaluated and the genetic material for the ‘fittest’ nodes can be spread, while the genetic make up of the less fit nodes is modified or dies out

Cloud computing has transformed the way organizations approach IT, enabling them to become more agile, introduce new business models, provide more services, and reduce IT
costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches.

The cloud computing landscape continues to realize explosive growth. Specific security challenges pertain to each of the three cloud service models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

1. SaaS deploys the provider’s applications running on a cloud infrastructure; it offers anywhere access, bu-t also increases security risk. With this service model it’s essential to implement policies for identity management and access control to applications. For example, with Salesforce.com, only certain sales people may be authorized to access and download confidential customer sales information.
2. PaaS is a shared development environment, such as Microsoft™ Windows Azure, where the consumer controls deployed applications but does not manage the underlying cloud infrastructure. This cloud service model requires strong authentication to identify users, an audit trail, and the ability to support compliance regulations and privacy mandates.
3. IaaS lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications. As with Amazon Elastic Compute Cloud (EC2), the consumer does not manage or control the underlying cloud infrastructure. Data security is typically a shared respon¬sibility between the cloud service provider and the cloud consumer. Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data.

V. SIMULATION OF PROTO TYPE FOR THIS PROPOSED ARCHITECTURE

A. Architecture

The architecture is shown in Fig 1. A number of special nodes (sink points) distributed across the WSN area constitute a cloud. We refer this type node as “cloud node”, which is equipped with more resources. Furthermore, a cloud node acts as a sink for sensors nearby. Therefore, the architecture is naturally cluster based. In order to differentiate from the term “cluster” in traditional WSN, we refer a cluster as a “zone” in this paper. These sensors in a zone are organized as independent local WSNs (LWSN), and all LWSN are integrated together by the cloud. The cloud can be viewed as a “virtual sink” for the whole sensor network.

B. Organizing Sensors in a Zone

We present a different way of heterogeneous sensors organization, as shown in Fig 2. The homogeneous sensors form a WSN (a different type sensor could be used as a software is deployed in the cloud. After processing data from all sensors, the cloud can designate sensors to perform properly through the accessed sink point. If the size of a zone is reasonable, the scheduling commands from the sink point could reach the destination sensor timely. This way of organization is different from the single-tier clustered architecture of WMSN. First, the independent WSN is built in a zone of which the size is smaller, instead of the whole sensor network. Second, the cloud can control activities of a sensor timely based on data collected from the whole WSN.

C. Organizing Cloud

As considering the organization of nodes to a cloud, the bandwidth is still one of the most important factors, especially when they communicate through wireless channel. In [17], Hadoop is adapted to the infrastructure built on smart phones, which has the similar requirements as here. In fact, Hadoop aims for big data storage and process, and data movement reduction is one of its design goals. One of its design criteria is “moving computation is easier than moving data.” We suggest the cloud is organized in the Hadoop way. Both of Hadoop’s storage system (Hadoop Distributed File System, HDFS) and data processing system (Map-Reduce framework) have a master/slave architecture, in which the master is responsible for storing file meta data or scheduling jobs, and slaves are responsible for storing file content or task execution (task is one piece of split job). The two masters could be deployed either in the same physical node or in different physical nodes. In its storage system, when a client accesses a file, it firstly contacts the master to retrieve the file’s meta data (file location, for example), then it directly retrieves the content from the slaves which store a part data of the file. In its data processing system, the code used is submitted to the master, and then the master distributes the code to the slaves which store the processed data, or to those slaves near by the slaves storing the processed data. As a result, the data is processed almost locally and the data movement (thus bandwidth requirement) is reduced. However, data movement cannot be avoided in distributed processing system. Hadoop supports data compression mechanism to reduce bandwidth cost as much as possible. Therefore, a master node should be introduced to build the cloud. The master node usually connects to the Internet and is the access point of the system.

VI. CONCLUSION

In this paper, we analyze the Cloud based Environment for Wireless Communication & Sensor Network Application along with the Security issues for Data Management. “Cloud” computing is based on technologies like virtualization, distributed computing, grid computing, utility computing, but also on networking, web and software services. The benefits of adopting this technology draw decision makers’ attention and now a days many companies are engaged in adopting or researching cloud adoption.

REFERENCES

[1] Virtualization Overview. White Paper. Vmware. Retrieved April 6, 2011.

[2] National Institute of Standards and Technology - Computer Security Division

[3] Bhaskar P., Admela J·, Dimitrios K·, Yves G.: Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. J. Grid Computing 9(1), 3-26 (2011)

[4] What the Hell is Cloud Computing. Retrieved April 6,2011.

[5] IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. Retrieved April 8, 2011

[6] New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved April 8, 2011

[7] LEMOS, R. 2009. Inside One Firm's Private Cloud Journey. Retrieved April 7, 2011.

[8] Boniface, M., Nasser, B., Papay, J., Phillips, S., Servin, A., Zlatev, Z., Yang, K. X., Katsaros, G., Konstanteli, K., Kousiouris, G., Menychtas, A., Kyriazis, D. and Gogouvitis, S., “Platform-as-a-Service Architecture for Real-time Quality of Service Management in Clouds”, Fifth International Conference on Internet and Web Applications and Services, ICIW 2010, May 2010, Barcelona

[9] Campbell , R. et al. Open Cirrus Cloud Computing Testbed: Federated Data Centers for Open Source Systems and Services Research. In Proc. HotCloud, 2009.

[10] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A Berkeley view of Cloud computing. Technical report UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, USA, February 2009.

[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control. In ACM Workshop on Cloud Computing Security, 2009

[12] Catteddu, D. and Hogben, G. Cloud Computing: benefits, risks and recommendations for information security. Technical Report. European Network and Information Security Agency, 2009.

[13] Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. White Paper. Information Systems Audit and Control Association, 2009.

[14] Brunette, G. and Mogull, R. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.Technical Report. Cloud Security Alliance, 2009.

[15] J. Brodkin. Gartner: Seven cloud-computing security risks. cloud-computing-security-risks-853, 2008.