ISSN No. 0976-5697

Volume 6, No. 1, Jan-Feb 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Protecting Healthcare Database by Access Control Method on Cloud Computing Technique - A Survey

A. Anusha Priya
Research scholar
Department of Computer Science
Karpagam University
Coimbatore Indore

Dr. S. Saravanan
Professor & Head
Department of EEE
Muthayammal Engineering College
Rasipuram, Namakkal (Dt) India

Abstract - A Wireless Sensor Network (WSN) has important applications such as remote environmental monitoring and target tracking. Sensors those are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. Cloud Computing is a computing paradigm, where large pools of systems are connected in Private or Public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. This paper explores the basics of Cloud Computing and its functionality of Cloud services. It provides security based on access control method, which is helps that identified and authenticated user is allowed to access information resources in a specific way. The Cloud application offers significant benefits to the healthcare sector which is explored in these surveys.

Keywords: Wireless Sensor Network, Cloud Computing, Access control method, Healthcare.

I. INTRODUCTION

A. *Wireless Sensor Network:*

Wireless Sensor Network is a collection of sensor nodes interconnected by wireless Communication channels. Each Sensor node is a small device that can collect data from its surrounding area, carry out simple computations, and communicate with other Sensors or with the Base Station (BS). Recent years have witnessed an increasing interest in using Wireless Sensor Networks (WSNs) in many applications, including environmental monitoring and military field surveillance. In these applications, tiny sensors are deployed and left unattended to continuously report parameters such as temperature, pressure, humidity, light, and chemical activity. Reports transmitted by these sensors are collected by observers (e.g., base stations).The dense deployment and unattended nature of WSNs makes it quite difficult to recharge node batteries. Therefore, energy efficiency is a major design goal in these networks. Several WSN applications require only an aggregate value to be reported to the observer. In this case, sensors in different regions of the field can collaborate to aggregate their data and provide more accurate reports about their local regions. For example, in a habitat monitoring application, the average reported humidity values may be sufficient for the observer. In military fields where chemical activity or radiation is measured, the maximum value may be required to alert the troops. In addition to improving the fidelity of the reported measurements, data aggregation reduces the communication overhead in the network, leading to significant energy savings [8] [11]. The concept of Wireless Sensor Networks is based on a simple equation:

Sensing + CPU + Radio = Thousands of potential applications

B. *Cloud Computing:*

Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The Cloud Computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud Computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

II. OVERVIEW OF CLOUD COMPUTING

A. *Characteristics:*

The characteristics of Cloud Computing include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self-service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or Private networks. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centres. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

The conceptual view of the architecture, shown in Fig 1, brings together three key Cloud perspectives - the Provider, Consumer, and the Broker.

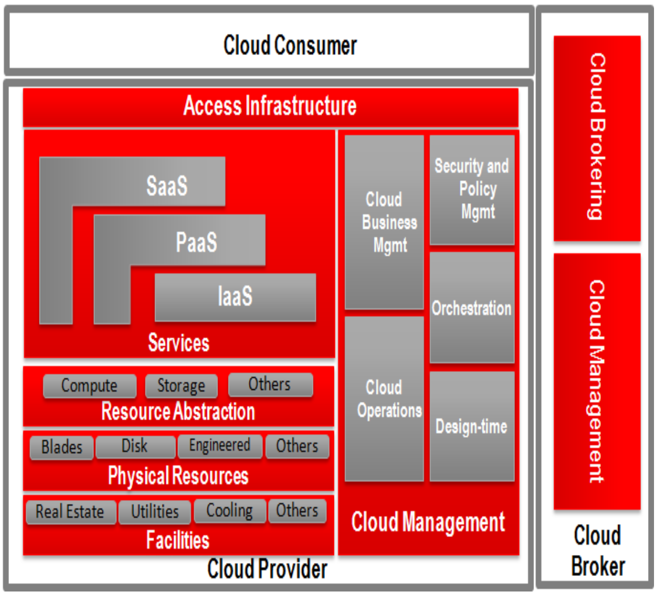


Figure 1. Conceptual view of Cloud Computing

The role of the Cloud provider is the most important and most complex of all. Infrastructure for the Cloud is usually of unprecedented scale and stringent requirements. Implementing the Cloud and maintaining it to satisfy the SLAs of the consumers requires extensive planning and precise execution.

A Cloud provider can spread the costs of facilities, across consumers to achieve economies of scale. Facilities expense may include the cost of real estate, cooling, utilities, and rack space among other things. The physical infrastructure components may include blades, networks, engineered systems, and storage disks. These resources must be pooled and provisioned through grid technologies in order to support the elasticity and scalability demands of Cloud infrastructure.

The physical resources need to be logically partitioned and secured in order to support multi-tenancy. Rapid elasticity requires the resources to be quickly deployed and undeployed at granular levels. Traditional deployments require downtime for scaling and maintenance but Cloud infrastructure does not have that luxury. The approach is to create and deploy new instances on the fly to grow, shrink, or fix the existing deployments. The resource abstraction layer provides the capabilities to logically abstract the physical resources.

B. Cloud Computing models:

Enterprises can choose to deploy applications on Public, Private or Hybrid Clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization.

a. Public Cloud:

Public Clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public Cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

b. Private Cloud:

Private Clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a Public Cloud. There are two variations to a Private Cloud:

a) On-premise Private Cloud:

On-premise Private Clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security.

b) Externally hosted Private Cloud:

This type of Private Cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy. This is best suited for enterprises that don't prefer a Public cloud due to sharing of physical resources.

c. Hybrid Cloud:

Hybrid Clouds combine both Public and Private Cloud models. The service providers can utilize third party Cloud providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid Cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a Private cloud with the resources of a Public cloud can be used to manage any unexpected surges in workload.

d. Community Clouds

Typically cloud systems are restricted to the local infrastructure, i.e. providers of Public Clouds offer their own infrastructure to customers. Though the provider could actually resell the infrastructure of another provider, Clouds do not *aggregate* infrastructures to build up larger, cross-boundary structures. In particular smaller SMEs could profit from community clouds to which different entities contribute with their respective (smaller) infrastructure. Community Clouds can either aggregate Public Clouds or dedicated resource infrastructures. We may thereby distinguish between Private and Public community Clouds. For example smaller organizations may come together only to pool their resources for building a Private community Cloud. As opposed to this, resellers such as Zimory may pool cloud resources from different providers and resell them. Community Clouds as such are still just a vision, though there are already indicators for such development, e.g. through Zimory [6] and Right Scale [14].

C. Services of Cloud Computing:

Cloud providers offer services that can be grouped into three categories.

a. Software as a Service (SaaS):

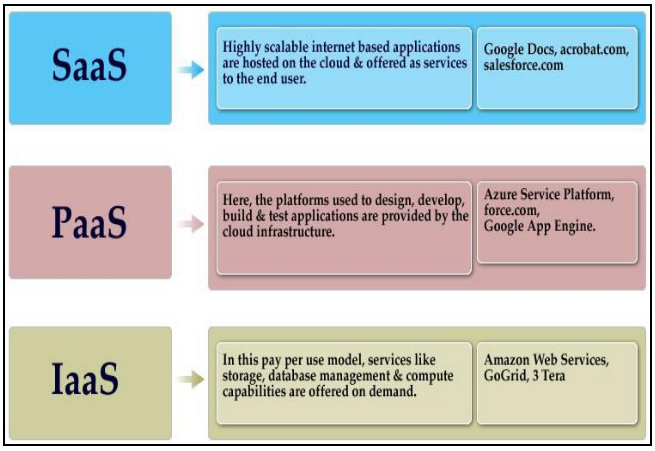
In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customer's side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

b. Platform as a Service (PaaS):

Here, a layer of software or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS (Operating System) and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Googles App Engine, Force.com, etc are some of the popular PaaS examples.

c. Infrastructure as a Service (IaaS):

IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc.



SaaS	Highly scalable internet based applications are hosted on the cloud & offered as services to the end user.	Google Docs, acrobat.com, salesforce.com
PaaS	Here, the platforms used to design, develop, build & test applications are provided by the cloud infrastructure.	Azure Service Platform, force.com, Google App Engine.
IaaS	In this pay per use model, services like storage, database management & compute capabilities are offered on demand.	Amazon Web Services, GoGrid, 3 Tera

Figure 2. Cloud Computing services

D. Cloud Computing Benefits:

Enterprises would need to align their applications, so as to exploit the architecture models that Cloud Computing offers. Some of the typical benefits are listed below:

a. Reduced Cost:

There are number of reasons to attribute based Cloud technology [7] with lower costs. The billing model is pay as per usage, the infrastructure is not purchased thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing.

b. Increased Storage:

With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently, since the cloud can scale dynamically.

c. Flexibility:

This is an extremely important characteristic. With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

d. Data Recovery and Availability:

All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support

(a). Appropriate clustering and Fail over

(b). Data Replication

(c). System monitoring (Transactions monitoring, logs monitoring and others)

(d). Maintenance (Runtime Governance)

(e). Disaster recovery

(f). Capacity and performance management

If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe.

e. Management Capabilities:

Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like "Auto-scaling" is a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

f. Regulatory and Compliance Restrictions:

In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

With Cloud Computing, the action moves to the interface that is, to the interface between service suppliers and multiple groups of service consumers. Cloud services will demand expertise in distributed services, procurement, risk assessment and service negotiation areas that many enterprises are only modestly equipped to handle.

III. ACCESS CONTROL BASED SECURITY

Access control [15] is generally a policy or procedure that allows, denies or restricts access to a system. It may monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Various access control models are in use, including the most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These access control methods are effective in unchangeable distributed system, where there are only aset of Users with a known set of services

A. Authentication:

Authentication is the process of establishing confidence in user identities. Authentication assurance levels should be appropriate for the sensitivity of the application and information assets accessed and the risk involved. A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange information between cooperating domains [1]. Also strong authentication should be used, i.e. two-factor authentication as is normal, for example, in online banking. Any network access should, in principle, be made secure by strong authentication. These strict requirements apply particularly to the CSP’s staff. They, too, should only gain access to the IT resources being administered via strong authentication, i.e. for example via a hardware-based authentication system using chip cards or USB sticks or via one-time passwords that can also be generated by hardware devices. This is absolutely indispensable for access via the Internet. The user obtains a certificate proving his identity signed by the Certification Authority (CA). This is the basis of every trust relationship among the participants, so a strict procedure has been set up for the connection between two principals. Once the trust relationship has been established via a trusted set of Certification Authorities, participants can use this to mutually authenticate each other in a connection [3]. There are various authentication methods and techniques that organizations can choose it such as follows:

a. User Password Authentication:

It is the most common form of providing identification. When user accesses the resource, access control framework asks for the user name password provided to the user. The credentials are validated against the one stored in the system’s repository.

b. Windows user based authentication:

Usually, organizations have a list of users stored in the windows active directory. Access control framework should be able to provide authentication for the user of the Primary Domain Controller (PDC).

c. Directory based authentication:

With the rising volume of business over the web, millions of users often try to access the resource simultaneously. In such a scenario, the authentication framework should be able to provide for faster authentication. One such technique is Directory Based Authentication where user credentials are validated against the one which is stored in the LDAP Directory.

d. Certificate based authentication:

This is probably one of the strongest authentication techniques where the user is asked to provide his/her digital ID. This digital ID, known as digital certificate, is validated against the trusted authority that issued the digital ID. There are various other parameters that are checked to ensure the identification of the user.

e. Smart card based authentication:

This is also used as a second factor authentication [13]. Smart cards are small devices containing co-processors to process cryptographic data.

f. Biometrics:

This is the strongest authentication. Known as third factor authentication [9], it is based on something the user is. It works after the users have provided something they know (User name password) and something they own (either a grid or token) or something they are (retina-scan, thumbprint or thermal scan). It is required in cases where data is top confidential, such as in Military/Defense.

g. Grid based Authentication:

This is used as a second factor authentication. It authenticates the user based on something he knows (User name password authentication) and then asks for something he owns (grid card information). Entrust Identity Guard provides such an authentication.

h. Knowledge-based authentication:

One of the simplest mechanisms for gaining additional confidence in a user's identity is to challenge the user to provide information that an attacker [2] is unlikely to be able to provide. Based on "shared secrets", this allows for the organization to question the user, when appropriate, to confirm information that is already known about the user through a registration process, or from previous transactions.

i. Machine Authentication:

Machine authentication provides validation of the user's computer in a way that secures against a variety of threats in a zero touch fashion, reducing user impact. This is an especially effective method of user authentication where users typically access their accounts from a regular set of machines, allowing for stronger authentication to be performed without any significant impact on the user experience.

j. One Time Password (OTP):

A one-time password is dynamically generated and it is valid only for once. The advantage of one time password is that if an intruder hacks it, he cannot reuse it. There are two types of OTP token generators: synchronous and asynchronous. A synchronous token device synchronizes with the authentication service by using time or an event as the core piece of the authentication process. A token device, which is using an asynchronous token generating method, uses a challenge response scheme to authenticate the user.

B. Authorization:

Authorization is an important information security requirement in Cloud Computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud Computing. The rights management system must ensure that each role may only see the data (including meta-data) required to achieve the task. The access control should be role-based and the roles and authorizations set up should be reviewed regularly. In general, the least privilege model should be used, with users and CSP administrators only possessing the rights that they require to achieve their tasks [14].

a. Global Authorization:

In an access control decision there are several rules and policies to take into account global (e.g. organizational membership) and local (e.g. banned users). Both pieces of information have to be available in order to make the decision. Grid access is granted according to membership of Virtual Organizations. In the early versions of the Globus software, this membership information was recorded in a local grid mapfile. This required a user to have an account on all resources they wished to have access to, and their DN was mapped onto that account via the grid-mapfile [12].

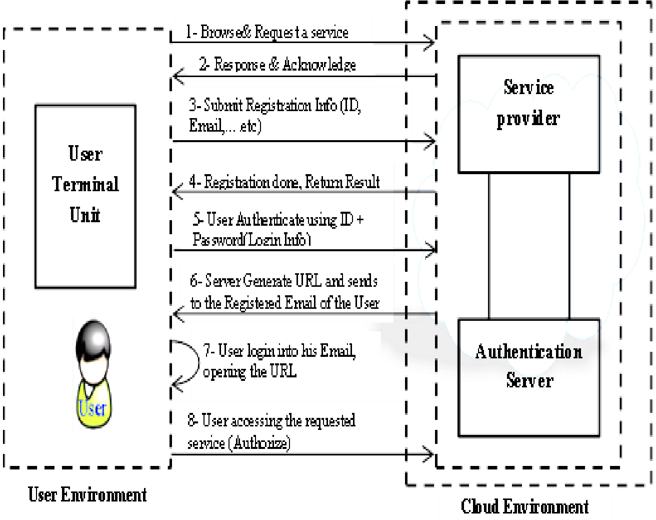

1- Browse& Request a service
2- Response & Acknowledge
3- Submit Registration Info (ID, Email,... etc)
4- Registration done, Return Result
5- User Authenticate using ID + Password(Login Info)
6- Server Generate URL and sends to the Registered Email of the User
7- User login into his Email, opening the URL
8- User accessing the requested service (Authorize)
User Terminal Unit
User
Service provider
Authentication Server
User Environment
Cloud Environment

Figure 3. Authentication and Authorization Process

From the above Fig. 3, it shows that the steps are marked in sequential order of their execution in the proposed scheme, as flow:

a) User browse and request for specific service from the cloud by enters URL of application.
b) The cloud system response and sends registration form to the user.
c) Upon receiving the registration form, the user fills and submits it to the cloud.
d) The Cloud checks and processes the registration from. If the details entered by the user are correct and satisfied to the condition terms, then they return information to the user of successful completion of the registration, otherwise the cloud denies.
e) The user authenticate into the cloud using registered information.
f) The cloud system after verifying the authentication of the user. They generate a dynamic link about specified service and send to the user of its registered Email-ID via text message, with notification about the process of replying.
g) The user login into his mail and enters that link received from cloud, within the threshold time, because after that the will expire and user has to login again.
h) After successful login the user is allowed and authorized to access the requested service in the cloud system, and the application is loaded.

IV. APPLICATIONS ON CLOUD

A. Cloud Computing for Healthcare:

Patient centricity has become the key trend in healthcare provisioning and is leading to the steady growth in adoption of Electronic Medical Records (EMR), Electronic Health Records (EHR), Personal Health Records (PHR), and technologies related to integrated care, patient safety, point of care access to demographic and clinical information, and clinical decision support. Availability of data, irrespective of the location of the patient and the clinician, has become the key to both patient satisfaction and improved clinical outcomes. Cloud technologies can significantly facilitate this trend. Cloud Computing offers significant benefits to the healthcare sector: doctor's clinics, hospitals, and health clinics require quick access to computing and large storage facilities which are not provided in the traditional settings.

a. Clinical Research:

Many pharmacology vendors are starting to tap the cloud to improve research and drug development. Currently, pharma firms do not have the capacity to run large datasets, especially DNA sequencing - as the size of the data can overwhelm their computers. Commercial cloud vendors have developed pharma-specific clinical research cloud offerings with the goal of lowering the cost and development of new drugs.

b. Electronic Medical Records:

Hospitals and physicians are starting to see cloud-based medical records and medical image archiving services coming on line. The objective is to offload a burdensome task from hospital IT departments and allow them to focus on supporting other imperatives such as EMR adoption and improved clinical support systems.

c. Collaboration solutions:

Early successes of cloud-based physician collaboration solutions such as remote video conference physician visits are being trailed. Extending such offerings to a mobile environment for rural Tele-health or disaster response is becoming more real with broader wireless broadband and smart phone adoption. Cloud Technology supports collaboration and team-based care delivery and the ability to use applications based on business model requirements and a common set of clinical information.

d. Telemedicine:

Increase in availability of mobile technologies and intelligent medical devices, telemedicine has grown to include not only Tele-consultations and Telesurgeries, but also health record exchange, video conferencing, and home monitoring. Cloud Computing and the related ease of services deployment and data storage is an enabler for telemedicine.

e. Big Data:

Healthcare organizations turn to Cloud Computing to save on the costs of storing hardware locally. The cloud holds big data sets for EHRs, radiology images and genomic data for clinical drug trials. Attempting to share EHRs among facilities in various geographic areas without the benefits of cloud storage could delay treatment of patients.

f. Health Information Exchange:

Health information exchanges help healthcare organizations to share data contained in largely proprietary EHR systems. CIOs may accelerate the deployment of HIE via a linkage to a strategic cloud implementation.

Healthcare organizations continue to depend on computer systems that are extremely vulnerable to data breaches caused by technology deficiencies, theft and insider misconduct. Cloud-Computing systems can be designed to be safer than traditional client-server systems against the prevailing causes of healthcare data breaches.

B. Future Research Areas:

Although much progress has already been made in Cloud Computing, we believe there are a number of research areas that still need to be explored. Issues of security [4], [10], reliability, and performance should be addressed to meet the specific requirements of different organizations, infrastructures, and functions. Security has different users to store more of their own data in a cloud, being able to ensure that one user's Private data is not accessible to other users who are not authorized to see it becomes more important. While virtualization technology offers one approach for improving security, a more fine-grained approach would be useful for many applications.

a. Reliability:

As more users come to depend on the services offered by a cloud, reliability becomes increasingly important, especially for long-running or mission critical applications. A cloud should be able to continue to run in the presence of hardware and software faults. Google has developed an approach that works well using commodity hardware and their own software. Other applications might require more stringent reliability that would be better served by a combination of more robust hardware and/or software-based fault-tolerance techniques.

b. Vulnerability to Attacks:

If a cloud is providing compute and storage services over the Internet such as the Amazon approach, security and reliability capabilities must be extended to deal with malicious attempts to access other users' files and/or to deny service to legitimate users. Being able to prevent, detect, and recover from such attacks will become increasingly important as more people and organizations use cloud Computing for critical applications.

c. Cluster Distribution:

Most of today's approaches to Cloud Computing are built on clusters running in a single data center. Some organizations have multiple clusters in multiple data centers, but these clusters typically operate as isolated systems. A cloud software architecture that could make multiple geographically distributed clusters appear to users as a single large cloud would provide opportunities to share data and perform even more complex computations than possible today.

d. Network Optimization:

Whether clouds consist of thousands of nodes in a computer room or hundreds of thousands of nodes across a continent, optimizing the underlying network to maximize cloud performance is critical. With the right kinds of routing algorithms and Layer 2 protocol optimizations, it may become possible for a network to adapt to the specific needs of the cloud application(s) running on it. If application level concepts such as locality of reference could be coupled with network-level concepts such as multicast or routing algorithms, clouds may be able to run applications substantially faster than they do today. By understanding how running cloud applications affects the underlying network, networks could be engineered to minimize or eliminate congestion and reduce latency that would degrade the performance of cloud-applications and non-cloud applications sharing the same network.

e. Interoperability:

Interoperability among different approaches to Cloud Computing is an equally important area to be studied. There are many cloud approaches being pursued right now and none of them are suitable for all applications. If every application were run on the most appropriate type of cloud, it would be useful to share data with other applications running on other types of clouds. Addressing this problem may require the development of interoperability standards. While standards may not be critical during the early evolution of Cloud Computing, they will become increasingly important as the field matures.

V. CONCLUSION

In this paper, we study about the concept of Wireless Sensor Network and Cloud Computing with its services. Cloud Computing offer benefits for organizations, individuals and security concerns, we have described a number of approaches to Cloud Computing in this survey and pointed out some of their strengths and applications. The approaches outlined in this paper along with other strategies, have already been applied successfully to a wide range of problems. As more experience is gained with Cloud Computing, the breadth and depth of cloud implementations and the range of application areas will continue to increase. We believe that Cloud Computing is poised to have a major impact on our society's data centric commercial and scientific actions. By enhancing the Cloud Computing architecture can improve security by access control method in healthcare database is our future work

VI. REFERENCE

[1] Abdelmajid Hassan Mansour Emam, "Additional Authentication and Authorization using Registered Email-ID for Cloud Computing", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013

[2] Ajey Singh, Dr. Maneesh Shrivastava, "Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume 1, Issue 4, pp. 321-323, April 2012.

[3] Abdul Raouf Khan, "ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT", Asian Research Publishing Network (ARPN), Journal of Engineering and Applied Sciences, ISSN 1819-6608, Vol. 7, NO. 5, pp. 613-615, MAY 2012.

[4] B.Meena, Krishnaveer Abhishek Challa, "Cloud Computing Security Issues with Possible Solutions", International Journal of Computer Science And Technology (IJCST), ISSN: 0976-8491 (Online) | ISSN : 2229-4333 (Print) Vol. 3, pp. 340-344, Issue 1, Jan. - March 2012.

[5] B.Prasanalakshmi, A.Kannammal, "Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics", International Journal of Computer Applications (0975 – 8887) Volume 53– No.18, pp. 13-19, September 2012.

[6] C.D. Plummer, T.J. Bittman, T. Austin, D.W. Cearley and D.M. Smith. Cloud Computing: Defining and Describing an Emerging. Phenomenon, 2008.

[7] Cha, J Seo and J. Kim. 2011. Design of AttributeBased Access Control in cloud computing. Proceedingof International conference on web service

[8] Heinzelman W. R, A. Chandrakasan, and H.Balkrishnan, "Energy-Efficient Communication Protocol for Wireless Micro sensor Networks", in Proceedings of 33rd Hawaii International Conference on System Science, Vol. 2, Jan. 2000, pp.1-10.

[9] Himabindu Vallabhu, R V Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, pp.163-165, September 2012.

[10] Jeon SeungHwan, Yvette E. Gelogo and Byungjoo Park, "Next Generation Cloud Computing Issues and Solutions", International Journal of Control and Automation Vol., No. 1, pp. 63-70, March, 2012.

[11] Lindsey S., C.S. Raghavendra, PEGASIS: power efficient gathering in sensor information systems, in: Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002.

[12] P. Bonatti and P. Samarati. 2002. A unifiedframework for regulating access and information release on the web.

[13] Pradnya B. Rane, Pallavi Kulkarni, SuchitaPatil, Dr.B.B.Meshram, "Authentication and Authorization: Tool for Ecommerce Security", IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No.1, pp. 150-157, 2012.

[14] Staten, J., Is Cloud Computing Ready For The Enterprise? 2008.

[15] Yuan and J. Tong. 2005. Attribute Based AccessControl (ABAS) for web Services. Proceeding of IEEE Conference on Web Service.