Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Third Party Auditor Cloud Computing, Mobile Health (MH) Cloud Computing: A Research

Vijayaraghavan.U[1*],
1, Asst. Professor,Dept of CSE,
RVS College of Engineering& Technology,
Karaikal, Pondicherry University,
Pondicherry, India

Dr.Kumar.A[2],
2. Associate Professor, Dept of CSE,
Perunthalaivar Kamarajar
Institute of Engineering & Technology Karaikal,
Puducherry, India

Palanisamy.S[3]
3. Asst. Professor, Dept of IT,
RVS College of Engineering& Technology,
karaikal, Pondicherry University, India.

Abstract: Cloud computing is to implement the security level and Mobile Health (MH) data base function, to identify the error problem. This paper existing process function, unsecurity process, loss increase production management and unless secure database (file). The propose work is, to solve the Error file, secure data base and to create the high level secure process to using Third Party Auditor (TPA-Cloud Computing).

Key Words: Cloud Computing, Mobile Health Database-MHD, Message Authentication code and Third Party Auditor (TPA).

1. INTRODUCTION

1.1Cloud Computing

Cloud computing, or the cloud, is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network.

1.2 Cloud Characteristics

1.2.1 Application programming Interface:

(API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates interaction between humans and computers. Cloud computing systems typically use Representational State Transfer (REST)-based APIs.

1.2.2 Provide Security Services

Sherif et.al [4] The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics".

A. On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

B. Broad network access.

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

C. Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

E. Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

F. Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

A model for enabling convenient, on –Demand network access to a shared pool of configuration computing resources(e.g., Networks,Server,application services ,Third Party Auditor and security services)that can be rapidly provisioned and released with minimal management effort or services provider interaction. According to this definition, cloud computing has the following management supporting characteristics.

1. 3 On-Demand Self Services

A Consumer can unilaterally have provision of computing capabilities, such as server time and network storage, as needed automatically without human interaction with each service provider.

1.4 Broad Network Access

Capabilities are available over the network and accessed through standard mechanisms that promote use of heterogeneous thin or thick client platform (E.g.: Mobile Phone, Laptops and PDAs).

1.5 Resource pooling

The Provider is computing resources are pooled to serve multiple consumers request using a multivendor model, with different physical and virtual resources, dynamically assignment and reassigned according to consumer demand.

2. EXISTING SYSTEM

There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (Low Cost, Security Awareness and loss of Production management). Kangchan Lee [3].Key functions of a cloud management system are divided into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer.

Each layer includes a set of functions:

- The Resources & Network Layer manages the physical and virtual resources.
- The Services Layer includes the main categories of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.
- The Access Layer includes API termination function, and Inter-Cloud peering and federation function.
- The User Layer includes End-user function, Partner function and Administration function.

Other functions like Management, Security & Privacy, etc. are considered as cross-layer functions that covers all the layers. The main principle of this architecture is that all these layers are supposed to be optional. This means that a cloud provider who wants to use the reference architecture may select and implement only a subset of these layers.

2.1 Service Provider Lock-in

A consequence of the loss of governance could be a lack of freedom regarding how to replace a cloud provider by another. This could be the case if a cloud provider relies on non-standard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.

2.2 Unsecure Cloud Service User Access

As most of the resource deliveries are through remote connection, non-protected APIs, (mostly management APIs and PaaS services is one of the easiest attack vector). Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

2.3 Lack of Information/Asset Management

When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), countermeasures for BCP and Disaster Recovery and so on. Furthermore, the cloud service users also have important concerns on exposure of data to foreign government and on compliance with privacy law such as EU data protection directive.

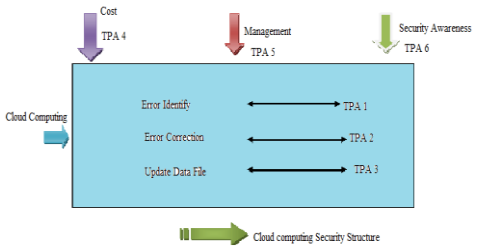


Fig: 1 Cloud Computing Security Structure

3. SURVEY WORK

Trust is the major concern of the consumer and provider of service that participant in a cloud computing environment. Depending on the services provider by the cloud, it is divided into main three categories.

Infrastructure as a Service (IaaS)

A service which provides an access to the hardware resources such as storage or computing hardware services.

Software as a Service (SaaS)

SaaS provides a software services to the end user. Web based email and google document are be example of this service .Refers to special purpose software made available through the Internet. (E.g.Security Process).

Platform as a Service (PaaS)

J.Ruiter et.al [6] This service provides a platform or an environment on which end user can develop his own application. User is transparent about the location of the platform whether it is hosted on cloud or (not).Google App engine is an example of PaaS.

3.1 Mobile Health (MH)

Abdal Nasir Kahan,et.al[5]The Purpose of applying MCC in Medical application is to minimize the limitation of traditional medical treatment (E.g., Small Physical Storage, Security and Privacy and Medical Errors).

Mobile Healthcare(MH) Provides mobiles user with convenient help to access resources e.g. Patient Health care record)easily and quickly besides ,MHealth Care offers hospital and health organizations a variety of on demand services on cloud rather than owning standard application an local servers.

There are a few schemes of MCC application in healthcare. The following five main mobile healthcare applications in the pervasive environment.

- **Comprehensive health Monitoring Services**

  Comprehensive health monitoring services enable patients to be monitoring at anytime and anywhere through broadband wireless communication.

- **Intelligent Emergency Management System**

  Intelligent emergency management system can manage and coordinate the fleet of emergency vehicles effectively and in time when receiving calls from accidents or incidents.

- **Health Aware Mobile devices detect Pulse**

  Rate, Blood Pressure and level of alcohol to alert healthcare emergency system.

- **Pervasive Access to Health Care Information**

  Allow Paintents or healthcare providers to access the current and past medical information.

- **Pervasive lifestyle incentive management**

  Pervasive life style incentive management can be used to pay Healthcare expenses and manage other related charges automatically.

3.2 Acronyms

AAA- Authentication, Authorization, Accounting.
APDU- Application Protocol Data Unit.
API - Application Programming Interface.
AV -Anti Virus.
B2B- Business to Business.
B2C- Business to Customer.
BTS- Base Transceiver Station.
CC- Cloud Computing.
CSP- Cloud Service Provider.
HA- Home Agent.
IaaS- Infrastructure as a Service.
IA- Integrated Authenticaticated.
ID-Identifier.
ISP-Internet Service Provider.
MC- Mobile Computing.
MSC- Mobile Service Cloud.
MCC- Mobile Cloud Computing.
PaaS –Platform as a Service
QoS- Quality of Service.

3.3 Third Party Auditor –TPA (Process)

A valid solution is to introduce a third party auditor (TPA) to do the job. On the other hand, this will introduce another issue related to data security, the data owner wants the TPA to Audit data and make sure everything is going according to plan, but the owner wants the TPA to do it without having access to the original data and without the need to have a local copy of the data. One of the solutions is that the data owner can encrypt their data and then generates message

authentication codes (MACs) for chunks of data, then the auditor can use these MACs to make sure that everything is going well. But this method will limit the operations over the data and add extra work needed by the user. Also any change to the data will requires a re-encryption and re-calculating of all MACs related the data change. MACs alone can give TPA some ideas about data and can interpret some knowledge about the original data, so to solve this and preserve privacy, a mask can be used with each MAC in order to completely hide the original data structure.

3.4 Proof Identify Process and Data Integrity

Vijayaraghavan U et.al [2] The TPA first selects fewer bits of the entire file and preprocesses the data. This fewer bits constitute metadata. This meta data is encrypted and appended to the file and sent to the cloud. Then whenever the client needs to verify the data correctness and availability it challenges the cloud through TPA and the data it got is correct, then integrity is ensured. This scheme can be extended for data updation, deletion and insertion at the client side. This involves modification of fewer bits at the client side.

There are two phases. One is Setup phase and the other is verification phase. Setup phase include generation of metadata and its encryption. Verification phase includes issuing a challenge to the third party auditor.

3.4.1 Deployment Models of Cloud Computing:

Fig.2 shows the types of cloud deployment models. There are describing in the following section.

A. Public Cloud

J.Ruiter, M.Warnier et.al [6] [7] In a public cloud the computing infrastructure is used by the organization or end user through clod service providers or venders. Public cloud are typically offered through virtualization and distributed among various physical machines.

B. Private Clod

In a private clod the computer infrastructure is dedicated to the particular organization and not shared with other organization. Private cloud are secure than public cloud.

C. Hybrid Cloud

J.Ruiter et.al [6] This is a Combination of the other two types of a cloud .In hybrid cloud organizations may host critical application on private clouds and applications which are having less security concerns hosted on public cloud .It is also known as cloud bursting.

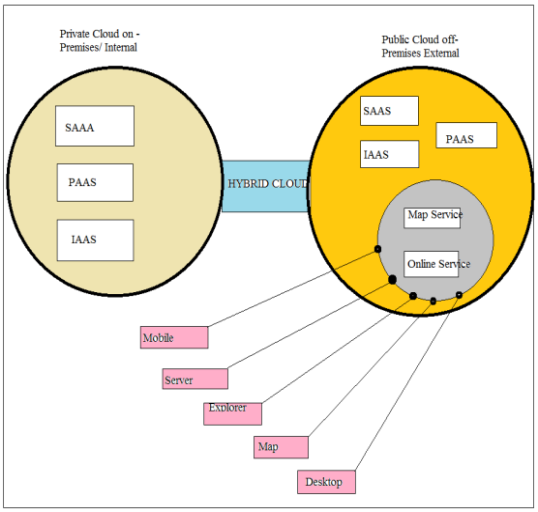


Fig: 2 Proof of Retrivability Architecture.

3.5 Message Authentication Code-MAC

Vijayaraghavan U et.al [1] suggests MAC is appended to a message .Our goal in this section is to define a cryptographic primitive that acts both as a MAC and an error correcting (or reassure) code. Moreover, we leverage the redundancy added by the error correction code for constructing the MAC. Such a primitive allows efficient checking of server response in our HAIL protocol.

MAC Procedure:

1. /* output F*/
F□---- (Input U1, Output V2)
2. /* Compute File Share */
Server □----- (S1, S2, S3)

3. /* generate nq challenge*/
For j=1 to no do
4. /* Challenge all servers
for a=1 to nq do
5. /* A responds for if j,f then Corrected
servers */
S corr ------S corr U (j)
6. /* Sj,S in correct replies blow q*/
if denote-F(output V2,Input U1)
7. /*F Error File can be recovered
else output 1
8. /* F is Corrupted*/.

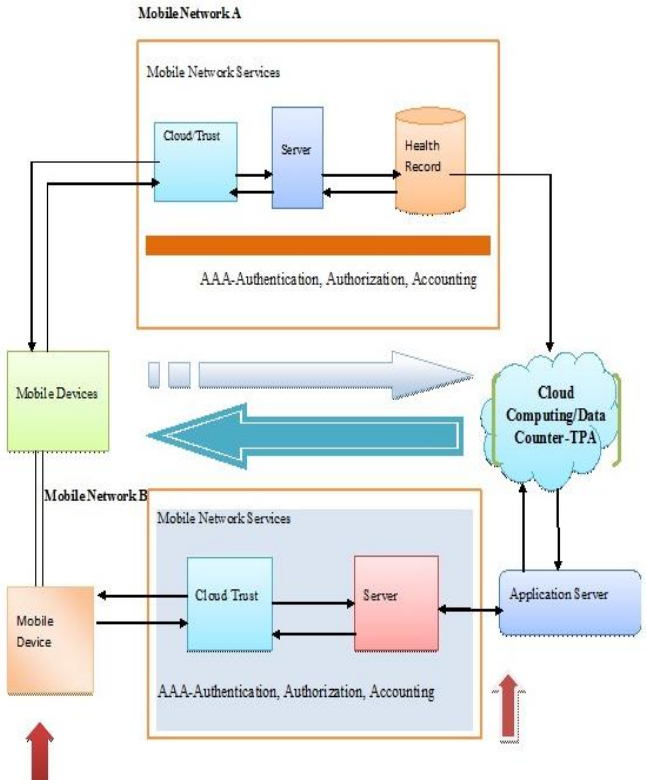


Fig: 3 Third Party Auditor and Mobile Computing Architecture

4. PROPOSE WORK

4.1 Data Location- Notation

F= Function Process.
S= Security Series.
1= Error Identify.
-1= Error Correction.
Find Series function f(x) is updated data file process. The input value f(1,-1) and output value (Error Location) Socket Process(x).
Security Series Location (**SSL**)

Proof: f(x) =1

Error Identify Process $f(x) = \int_{-1}^{1} f(x)\,dx$

$= 2\int_{0}^{1} f(x)\,dx$

$= 2\left[x^2/2 \right]_0^1$

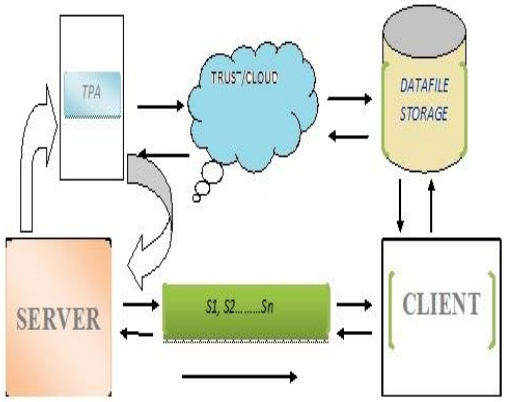
$= [2(1)/2-(2(0)/2]$

= 2/2
=1

Error Identify process f(x) =1.
The Proof is verified.

Error Identify Formula= $\sum$ **(Error Identify +Error Correction) / Update Data File (Security series location-SSL)**

4.2 Third Party Auditor Data File Process



Third Party Auditor Data File Process

Fig: 4 Third Party Auditor Data File Architecture

4.2.1 Error Identify and MHealth Process:

- **Error Identify S1**

The service providers an error identify the data error file (S1).

Error Correction S2

To service provider the third parity auditor (TPA) using the data error correction (S2).

Update File S3

To service provider the trust computing using an update file. In intimation to server message (S1+S2=S3) Services.

5. Flow Chart

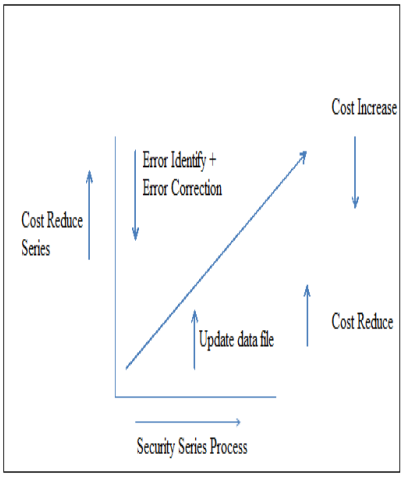


Fig: 5 Third Party Auditor and M-Health Flow Structure.

Acknowledgements

I Wish to express my warmest, sincerest thanks and deepest gratitude to my Research advisor,Prof.Dr.P.THAMBIDURAI,M.E.,Ph.D., Principal of PKIET Engineering College,Karaikal,Puducherry ,India., for his impeccable guidance, numerous opportunities and valuable suggestion for my research work. I would like to thank my Prof.Dr.V.Arumugham, M.Tech.,Ph.D., Principal of RVS College of Engineering and Technology,Karaikal,Puducherry,India.

5 Conclusion

Cloud computing today is the starting of "Highly network based computing" over internet on power. It is the technology of the decade and is the enabling element of two totally new computing models (Third Party Auditor and M-Health), the client cloud computing and the terminal cloud computing. The data storage security is of the critical important so that users can resort to an external third party auditor using identify the error file. Third Party Auditor solving the Error file and cost reduce the database management.

Future Work

The future work focus, the Cloud computing highly level Security tools and different the pointer security algorithms to create the efficient security process (Cloud-TPA).

References

[1] Vijayaraghavan U, Madonna Arieth, R and R.Anand Babu "A Survey of the Research on Future an Error Identify and Error Correction" International Journal of Advanced Information Science and Technology (IJAIST) Vol.12.No.12, ISSN: 2319-2682.

[2] Vijayaraghavan U,Madonna Arieth,R and Geethanjali " Proof of Retrivability : A Third Party Auditor Using Cloud Computing" International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013).

[3]. Kangchan Lee "Security threat in cloud computing Environments" International Journal of Security and its Applications Vol.6, No.4, October, 2012.

[4]. Sherif Sakr Anna Liu, Daniel M. Batista, and Mohammad Alomari "A Suvey of Large Scale Data Management Approaches in Cloud Environments", IEEE Communications survey & Tutorials, Vol.13, No.13, Third Quarter 2011.

[5]. Abdul Nasir Khana,∗, M.L. Mat Kiah a, Samee U. Khanb, Sajjad A. Madanic "Towards secure mobile cloud computing: A survey", 2012 Elsevier,Accept 11 Auguest 2012.

[6] J.Ruiter and M.Warnier, Privacy regulation for cloud computing,compliance and implementation in theory and Pratice ,article.

[7] P.Metri and G.Sarote "Privacy Issues and Challenges in cloud computing", International Journal of Advanced Engineering Science and Technology, 5, Issue No.1, 001-006.

AUTHOR"S PROFILE

Mr.U.Vijayaraghavan received the B.Tech degree in information &Technology from the Lord Venkateshwarra Engineering College, Kanchipuram (Anna University Chennai), Tamil nadu, South India. He earned M.E (Computer Science &Engineering) in Academic Campus Anna University, Coimbatore, India. He is a member of IAENG. He delivered his papers in three national conferences and in one international conference. He delivered his papers in IJAIST and IJETAE. He was worked as Lecturer in Dept of Information Technology, Lord Venkateshwaraa Engineering College Kanchipuram. Currently he is working as an Assistant Professor in the Department of Computer Science and Engineering, RVS College of Engineering & Technology, karaikal, Puducherry, India. His Research area of interest is Cloud Computing, Grid Computing and Optical Networks.

Dr. A. Kumar M.Sc., M.Phil, .M.Tech. Ph.D. is working as Associate Professor in Perunthalaivar Kamarajar Insititute of Engineering and Technology, Nedungadu, Karaikal, India. He has completed his Ph.D in Sathayabama University, Chennai, India. His Area of Specialization is Data Mining, Database Systems. He has published articles in two International Journals and in One National Journal. He has 25 years working experience in teaching field.

Mr.S.Palanisamy received the B.Tech degree in Information Technology from Arulmigu Kalasalingam College of Engineering, Srivillipudur (Anna University, Chennai),TamilNadu, South India. He earned M.Tech (Information Technology) in Kalasalingam University, TamilNadu, India. He delivered his papers in two International Conferences and one national Conference .Currently he is working as Asst.Professor in RVS College of Engineering &Technology, Karaikal, India. His Research area of Interest is Grid Computing and Cloud Computing.

