ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (119-126), Month: July - September 2016, Available at: www.researchpublish.com

Cloud Interrelated Service Oriented Audio Accepted By-Connections

Rethish Kumar S.[1], Dr. R. Vijayakumar[2]

[1]Lecturer, Dept. of Computer Science & Engineering, M.G. University College of Engineering, Thodupuzha, Kerala.
[2]Professor, School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala.

Abstract: **Cloud Computing presents a new approach to allow the development of dynamic, distributed and highly scalable software. For this purpose, Cloud Computing offers services, software and computing infrastructure independently through the network. To achieve a system that supports these characteristics, Service-Oriented Architectures (SOA) which provides tools for developing distributed systems that can be used for the establishment of Cloud Computing environments. This paper presents a CISAB (Cloud Computing Interface with Service Oriented Audio accepted By-Connections) architecture set on top of the platforms and frameworks by adding new layers for integrating a SOA and Cloud Computing approach and facilitating the distribution and management of functionalities. CISAB has been applied to the real case study consisting of the analysis of microarray data and has allowed the efficient management of the allocation of resources to the different system agents.**

Keywords: **Cloud Computing, SOA, Bioinformatics, Network Security, Distributed Computing & Micro-array Clustering of Voice signals.**

I. INTRODUCTION

Cloud Computing security (sometimes referred to simply as "cloud security") is an evolving sub- domain of computer security, network security, data mining and more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.
In connection with Cloud security architecture is only effective if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a Cloud security architecture, Correct security controls should be implemented according to asset, threat, and vulnerability risk assessment matrices. While cloud security concerns can be grouped into any number of dimensions (Gartner names seven while the Cloud Security Alliance identifies fourteen areas of concern) these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues. Eg. Of Cloud is AWS, IBM, and Google Drive etc.

II. EASE OF USE

Cloud computing is one of the most fascinating technologies which attract the users to outsource their data from local to remote Cloud servers using Internet. A large number of cryptographic schemes are available to encrypt the sensitive information and to protect data. Even though it protects the data but it limits the functionality of the cloud storage. This paper focuses on investigation of cloud data security and its issues. Cloud Computing is one of the most influential technology in the IT industry in recent years. In Cloud, the computing infrastructures (Hardware and Software) are provided as services over the internet in pay-as-you-use basis. The outsourced sensitive data cloud servers are not within

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (119-126), Month: July - September 2016, Available at: www.researchpublish.com

the same domain. For securing these sensitive user data in cloud server, at present many cryptographic solutions are available. However, these solutions have computation overhead, key distribution and data management for providing security and scalability in data access control of cloud computing. This paper presents the analysis on various cloud data security issues available.

(Architecture of Cloud Computing)

III. LITERATURE SURVEY

Cloud Security

Intelligent Security Model (ISM) means real cloud security. Blocking over 8 million attacks per month, the IMS stops hackers from wreaking havoc on your brand. Join FireHost and protect your customer data.

Secure Cloud

- Get a Custom Quote
- Enterprise Security
- Beyond Compliance
- High Performance
- Complete Service

Security

Fire Host's Intelligent Security Model™ provides multiple layers of protection from the physical data center all the way through to the database. Security is the core of FireHost's infrastructure, not something that's been bolted on Security Details.

Compliance

The FireHost infrastructure exceeds the compliance mandates for HIPAA and PCI DSS with a secure, validated cloud. This auditor friendly environment protects healthcare and payment businesses of all sizes from the risk of crippling cybercrime.

Performance

Only hardware, software, systems and configurations designed specifically for high performance, production workloads meet the entry criteria for FireHost's secure cloud. Secure servers are ranked #1 for performance in 3rd party benchmarks.

Service

Proactive support meets control and visibility. With over 24 distinct points of service, a robust API and a powerful portal, FireHost serves as an extension of any IT department. We take pride in providing automation with a human touch.

Security issues associated with the cloud.

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, and Hybrid). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-,

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (119-126), Month: July - September 2016, Available at: www.researchpublish.com

platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must ensure that the provider has taken the proper security measures to protect their information, and the user must take measures to use strong passwords and authentication measures.

(Properties of Cloud)

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole data enter to go down or be reconfigured to an attacker's liking.

IV. TOOLS AND METHODS

Cloud security controls

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls.

These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

(a). Deterrent controls

These controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, these controls do not reduce the actual vulnerability of a system.

(b). Preventative controls

These controls upgrade the strength of the system by managing the vulnerabilities. The preventative control will safeguard vulnerabilities of the system. If an attack were to occur, the preventative controls are in place to cover the attack and reduce the damage and violation to the system's security.

(c). Corrective controls

Corrective controls are used to reduce the effect of an attack. Unlike the preventative controls, the corrective controls take action as an attack is occurring.

(d). Detective controls

Detective controls are used to detect any attacks that may be occurring to the system. In the event of an attack, the detective control will signal the preventative or corrective controls to address the issue.

Dimensions of Cloud security

Correct security controls should be implemented according to asset, threat, and vulnerability risk assessment matrices. While cloud security concerns can be grouped into any number of dimensions (Gartner names seven while the Cloud Security Alliance identifies fourteen areas of concern) these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues.

Security and Privacy

(a). Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or provide an identity management solution of their own.

(b). Physical and personnel security

Providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented.

(c). Availability

Cloud providers assure customers that they will have regular and predictable access to their data and applications.

(d). Application security

Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures be in place in the production environment.

(e). Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted (even better) and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

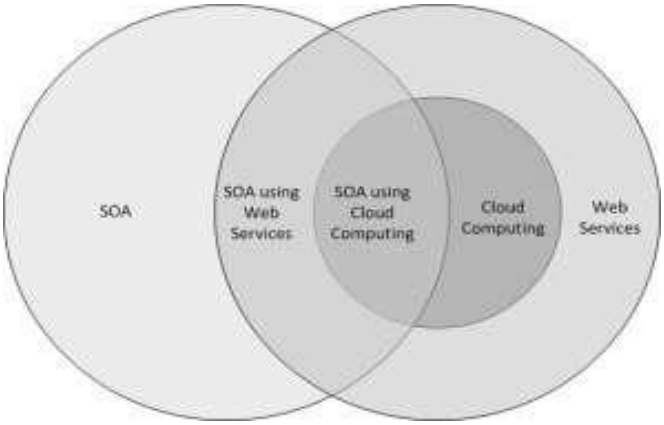
V. PROBLEM DEFINITION

Currently we are used smart phones with Android OS. Whenever we are taken a "Selfy", within seconds it is available in our Gmail account. The smart phones are always configured with Gmail/Google account. However, we are unaware about whether it is secured or not. Our private pics are protected or it has any security strategies or our selfies are how many are watching etc.

The main drawback of Cloud Computing platform is the Security challenges. Here any third party wants data which is located at Cloud, first authenticate whom the data is needed and which purpose the date is taken. Someone needs it for healthy purposes and perhaps another is an intruder. So first we find out who are intruders and second to eliminate these intruders from scale and secure data at Cloud.

Prevent unauthorized access to cloud computing infrastructure resources. This includes implementing security domains that have a logical separation between computing resources (e.g., logical separation of Postal Service workloads running on the same physical server by virtual machine (VM) monitors [hypervisors] in a multitenant environment) and using default to no-access configurations.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (119-126), Month: July - September 2016, Available at: www.researchpublish.com



(Service Oriented Cloud Computing)

Protect Internet browsers from attacks to mitigate end-user security vulnerabilities. This includes taking measures to protect Internet- connected personal computing devices by applying security software, personal firewalls, and patches on a regular maintenance schedule.

Deploy access control and intrusion-detection technologies at the CP and conduct an independent assessment to verify that they are in place. This includes, but does not rely on, traditional perimeter security measures in combination with the domain security model. Traditional perimeter security includes: restricting physical access to network and devices; protecting individual components from exploitation through security patch deployment; setting as the default the most secure configurations; disabling all unused ports and services; using role-based access control; monitoring audit trails; minimizing the use of privilege; using antivirus software; and encrypting communications.

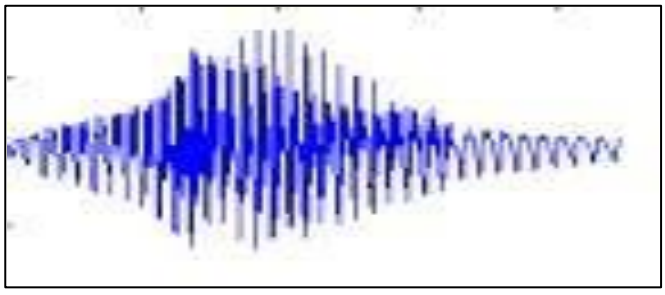
Support portability such that the Postal Service can take action to change CPs when needed to satisfy availability, confidentiality, and integrity requirements. This includes the ability to close an account on a particular date and time and to copy data from one CP to another.

VI. PROPOSED METHOD

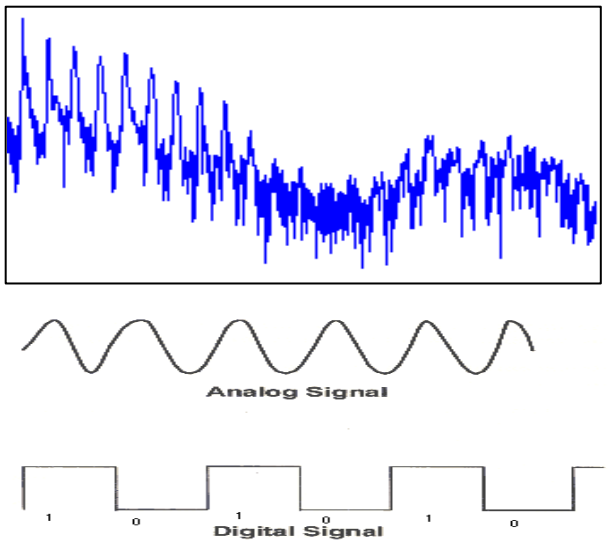
A variety of Biometric Cloud security is already existed. They are Fingerprints, IRIS, facial expressions, Agent types etc. are already live. Therefore, here we are adopted a new system of architecture that is used by voice or speech recognition.

In this paper a new technology adopted fro Cloud security that CISAB (Cloud Computing Interface with Service Oriented Audio accepted By- connections) Architecture is developed for attaining the Cloud security through Bio-Informatics. The audio (voice and speech) verified and after getting the authentication only the data provided for third party. Any one accessed for data on Cloud that first identified with speech recognition and if already given that is stored in micro-array chips.

In CISAB Architecture has been adapted to the analysis of microarray expression, since it has been necessary to include agents that simulate the behaviour of a laboratory and the necessary services in the Agent Platform in order to carry out analysis. As well as the predefined agents, the Agent Platform includes agents that simulate the roles associated with the case study. A Voice Recognition voiceprint is a spectrogram. A spectrogram is a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech creates different shapes on the graph. Spectrograms also use colour or shades of grey to represent the acoustical qualities of sound.



ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (119-126), Month: July - September 2016, Available at: www.researchpublish.com



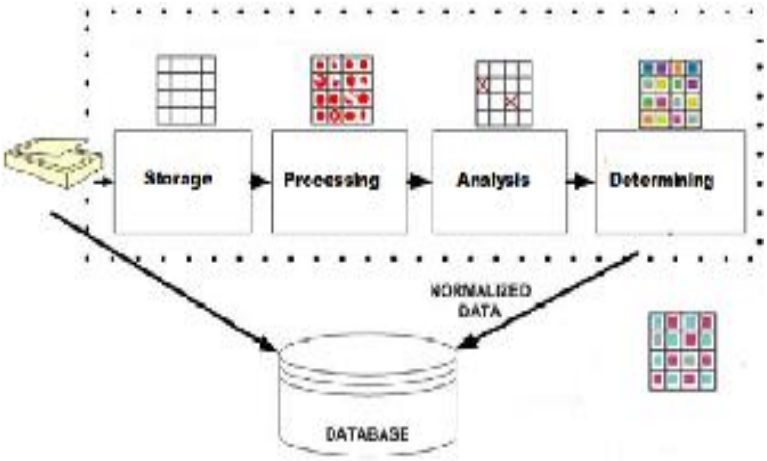
(Spectrum of vocal track sampling for authentication)

All of our voices are uniquely different (including twins) and cannot be exactly duplicated. Speech is made up of two components. A physiological component (the voice tract) and a behavioural component (the accent). Some companies use voice recognition so that people can gain access to information without being physically present, like in a phone call.

Unfortunately people can bypass this system by using a pre recorded voice from an authorized person. That's why some systems will use several randomly chosen voice passwords or use general voiceprints instead prints of specific words.

The voiceprint generated upon enrolment is characterised by the vocal tract and a cold does not affect the vocal tract. Only extreme vocal conditions such as laryngitis will prevent the system from proper voice recognition.

During enrolment, the user is prompted to repeat a short phrase or a sequence of numbers. Voice recognition can utilize various audio capture devices (microphones, telephones and PC microphones). The performance of voice recognition systems may vary depending on the quality of the audio signal. Random words and phrases are used so that no unauthorized use is suspected.



(Micro-array processing of audio signals)

The sampled voices are stored in the Micro-array in the Cloud or GRID platform. When a client approaches to the cloud first authenticate with the system that the incoming voice is matched with micro array stored voice. After the culturing it is found genuine that the person is authenticated and no problem for using the date at Cloud. Otherwise the incoming

voice date is mismatched, we assumed the person is intruder and the voice is fake and no authentication is provided for accessing of Cloud information.

Speech recognition is the computing task of validating a user's claimed identity by using characteristics extracted from their voice. Speaker recognition uses the acoustic features of speech that are different in all of us. These acoustic patterns reflect both anatomy (size and shape of mouth & throat) and learned behaviour patterns (voice pitch & speaking style), If a speaker claims to be of a certain identity and their speech is used to verify this claim. This is called verification or authentication. Identification is the task of determining an unknown speaker's identity.

Speech recognition can be divided into two methods. Text dependent and text independent methods. Text dependent relies on a person saying a pre-determined phrase whereas text independent can be any text or phrase. The methods can easily be deceived by someone playing a pre recorded phrase of a person who is authorized.

A speech recognition system has two phases. Enrolment and verification. During enrolment, the speaker's voice is recorded and typically a number of features are extracted to form a voice print, template or model.

In the verification phase, a speech sample or utterance is compared against a previously created voiceprint. For identification systems, the utterance is compared against multiple voiceprints in order to determine the best match or matches, while verification systems compare an utterance against a single voiceprint. Because of this process, verification is faster than identification.

Voice/speech recognition systems are mostly used for telephone based applications. Voice verification is used in government offices, healthcare, call centres, financial services and customer authentication for service calls.

To find the best solution for voice and speech recognition systems, please check out our sponsors below.

VII. DISCUSSION

Layers

Organization- The organization agents run on the user devices or on servers. The agents installed on the user devices create a bridge between the devices and the system agents which perform data analysis.

Analysis- The agents in the analysis layer are responsible for selecting the configuration and the flow of services best suited to the problem that needs to be solved. On the other hand, the services necessary to carry out expression analysis must be implemented within SaaS (Software as a Service). These services are those used by agents from the analysis layer to carry out data analysis.

Pre-processing Service- This service implements the RMA (Robust Multiarray Average) algorithm which is frequently used for pre-processing Affymetrix microarray data.

Filtering Service- The filtering service eliminates variables that do not allow classification of patients by reducing the dimensionality of the data. Three services are used for filtering: Variability, Uniform Distribution and Correlations.

Clustering Service- It addresses both clustering and association of a new individual to the most appropriate group.

Security in the cloud is challenging, due to varied degrees of security features and management schemes within the cloud entities. In this connection one logical protocol base needs to evolve so that the entire gamut of components operates synchronously and securely.

Protect Postal Service data from unauthorized access, disclosure, modification, and monitoring. This includes supporting identity management such that the Postal Service has the capability to enforce identity and access control policies on authorized users accessing cloud services. This also includes the ability of the Postal Service to allow access to its data selectively available to other users.

Extraction- The knowledge extraction technique applied has been the CART (Classification and Regression Tree) algorithm. The agents at the organizational layer are CBP-BDI agents with the ability to generate plans automatically based on previously existing plans in the system. Each of the CBP-BDI agents handles its own case memory in which it stores past experiences related to the specific tasks assigned to the agent. As a result, each CBP-BDI agent manages its own case memory, which is updated each time a global plan is carried out.

VIII. CONCLUSION

CISAB facilitates the development of dynamic and intelligent multi-agent systems. Its model is based on a Cloud Computing approach where functionalities are implemented using Web Services. The architecture proposes an alternative where agents act as controllers and coordinators. CISAB takes advantage of the agents' characteristics to provide a robust, flexible, modular and adaptable solution that can cover most requirements of a wide diversity of distributed systems. One of the objectives of the research activity was testing the application of Cloud Computing and Cloud services to systems and platforms oriented to the analysis of large volumes of information. The architecture has enabled the quick and efficient integration of a case study and made the inclusion of new case studies possible with a simple rearrangement of the Agent Platform, based on the needs of the problem and the definition of new services where necessary.

IX. ACKNOWLEDGMENT

Authors would also like to thank my Supervising Teacher Dr.R.Vijayakumar, Professor at School of Computer Sciences, Mahatma Gandhi University, Dean, Faculty of Engg. & Technology, Chairman, BOS (PG), M.G. University) for his immense contribution for the development of Biometric Cloud Security model and he has done a vital role in the current information security scenario.

REFERENCES

[1] Cloud Computing: Virtual Cloud Security Concerns. Technet Magazine, Microsoft.

[2] Dark Cloud: Study finds security risks in virtualization. Government Security News.

[3] Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. p. 59. ISBN 978-1-59749-592-9.

[4] "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80.

[5] Cloud Computing Security Policies You Must Know". Cloud Computing Sec. 2011.

[6] "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02.

[7] Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance.

[8] How Stuff Works: "How Biometrics Works: Voiceprints". How Stuff Works & Diaphonics:"Faqs". Diaphonics Sound Security.

[9] Wikipedia:"Speech Recognition". Wikipedia, the free Encyclopaedia.

[10] Voice Vault:"How Voice Vault Works". Voice Vault.

[11] Classification and Regression Tree Construction, By Alin Dobra, Department of Computer Science, Cornell University, Ithaca NY, November 25, 2002.

[12] Attaining Pre-Eminent Cloud Security Using Intrusion Detection Systems by Jagadeeshraj.V., Lijoy C. George, Thenmozhi, Kalaignar Karunanidhi Institute of Tech., TN.

[13] http://www.cloudsecurityalliance.org/guidanc e/csaguide.v3.0.pdf

[14] http://www.gladnit.com

[15] http://www.box.net