THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Cloud Based Remote Access Controllability with Enhanced Push/Pull Subscriptions

Sudhakar Murugesan
Lecturer, Department of Information Technology
Valley View University, Techiman Campus, Ghana
Nivash Thirunavukarasu
Assistant Professor, Department of Computer Science
Lord Vengadeswara Engineering College, Tamil Nadu, India
Seenuvasan Arumugam
Assistant Professor, Department of Computer Science
Lord Vengadeswara Engineering College, Tamil Nadu, India

Abstract:
Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. It's a new paradigm for deploying services on rented remote machine. The security problem prevent the rapid development of cloud computing. In our project, we are trying to achieve a Trustworthy Service Oriented Architecture (TSOA) in the Cloud environment through enforcing stronger accountability. We are trying to implement a SAML based authentication which is evaluated by XSD and all the SAML alterations were validated and loaded by Janus back grounded SAML tracer. To avoid web bottling our project includes the customization of Anti-Spoof Captcha option in which the entire captcha will be dynamically constructed to enhance the highest security against spam bots. In cloud the documents will be stored in the format of File Stream Data type in a secure repository and the ease of tracking the documents with revoking versioning of the documents is one of the advanced accountability options designed in the system. The system is internally configured for Push and Pull Subscription methodologies, it is flexible to process on the log data and the data access will be driven by web services with an underlying SOAP protocol.

1. Introduction

Cloud computing can be considered a new computing paradigm with implications for greater flexibility and availability at lower cost. In Cloud computing customers plug into the cloud to access IT resources which are priced and provided on-demand. With Cloud service the users can access database resources remotely via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Cloud computing provides the facility to access shared resources and common infrastructure, offering services on demand over the network. There are number of notable commercial and individual cloud computing services, including Amazon, Google, Microsoft, Yahoo, and Sales force. It's a new paradigm for deploying services on rented remote machines. On the other hand, Service Oriented Architecture (SOA) has acquired wide adoption among various organizations due to the importance of collaborations and outsourcing. Cloud's enormous capacity with low cost makes it a platform for SOA deployment. On a whole, the correctness of the Service Oriented Architecture deployed in the Cloud environment depends on the correctness of all the individual participants. The security problem which prevents the growth of this new emerging technology. There are number of issues related to accountability, including the handling of personally identifiable information. The users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. So we are trying to achieve a Trustworthy Service Oriented Architecture (TSOA) in the Cloud environment through enforcing stronger accountability. Data handling in cloud is complex and user fear of losing control of their own data. We propose a novel approach, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and tractable. We are trying to implement a SAML based authentication which is evaluated by XSD combinational validations. Along with the changes, all the SAML alterations were validated and loaded by Janus back grounded SAML tracer which will track down the SAML contents. A multi level authentication and authorization is provided for accessing the data available in the cloud server. Customization of Anti-Spoof Captcha option is utilized to avoid web bottling happens on the system in which the entire captcha will be dynamically constructed by the user based on the options provided to enhance the highest security against spam bots. Our proposed CIA framework enforces access and usage control rules as needed. Associated with the accountability feature, we also develop two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers the user can retrieve the logs as needed. The owner will be getting a frequent updates about

the usage of their data. Once the owner logged into the system, he/she is enable to see the log data about the usage. The data access will be driven by web services with an underlying SOAP protocol. CIA framework presents challenges, including uniquely identifying CSPs, ensuring the reliability of the log, adapting to a highly decentralized infrastructure, etc.
The basic approach toward addressing these issues is to leverage and extend the programmable capability of JAR (Java Archives) files to automatically log the usage of the users' data by any entity in the cloud. Any access to the data will trigger an automated and authenticated logging mechanism local to the JARs. In order to ensure the integrity the documents will be stored in the format of File Stream Data type which is one of the special data type and load the data in a secure repository. The user document are traced so that versioning of the documents is revoked on needed basics of user is one of the advanced accountability options designed in the system. We also provide a detailed security analysis and discuss the reliability and strength of our architecture. We identify the common requirements and develop several guidelines to achieve data accountability in the cloud. A user, who subscribed to a certain cloud service, usually needs to send his/her data as well as associated access control policies (if any) to the service provider. After the data are received by the cloud service provider, the service provider will have granted access rights, such as read, write, and copy, on the data. Using conventional access control mechanisms, once the access rights are granted, the data will be fully available at the service provider. In order to track the actual usage of the data, we aim to develop novel logging and auditing techniques
We present an overview of the Cloud Information Accountability framework and discuss how the CIA framework meets the design requirements The Cloud Information Accountability framework proposed in this work conducts automated logging and distributed auditing of relevant access performed by any entity, carried out at any point of time at any cloud service provider.

2. Review of Literature

- **B. Chun et al. [1]** proposed in federated systems where remote resources can be acquired across multiple administrative domains and used in potentially undesirable ways. It addresses the concurrent problems of how to continuously monitor and manage trust relationships over time. It express, delegate, and verify trust relationships. Expressing and verifying trust in federated system is flexible, scalable, and accountable. It monitors trust relationships over time so that misuse of trust can be detected based on automatic detection. Misuse of resources also can be automatically detected.
- **Qianhui Liang et al. [2]** proposed a multi angled life cycle of the cloud is done in this project which includes policy planning, auditing, logging, safe looking of logs, auditing, optimizing and rectifying are some of the options specified in the system. Detective approach is proposed rather than preventive approaches to increasing accountability. Theoretical information about various techniques was specified to cover the overall trust on the service provider is created with all perceptional concepts. Clear information on the data security and accountability is discussed in this project. Detective controls are used to identify the occurrence of a privacy or security risk.
- **Q. Wang et al. [3]** proposed this paper to verify the integrity of the dynamic data stored in the cloud third party auditor (TPA) is introduced. The support for data dynamics via general forms of data operation, such as block modification, insertion and deletion. Ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations; this paper achieves both. The public auditing system of data storage security is done in Cloud Computing. Support scalable and efficient public auditing in Cloud Computing. TPA can perform multiple auditing tasks simultaneously. It explores the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud Computing.
- **P.T. Jaeger et al. [4]** proposed this paper to introduce the policy concerns, research areas, and potential solutions related to cloud computing. This paper explores the nature and potential of cloud computing , the policy issues raised, and research questions related to cloud computing and policy. It solve incredibly complicated scientific problems to using clouds to manage and provide access to medical records. Cloud computing raises a range of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others. This paper introduces and examines these issues individually.

3. System Design

System Design involves identification of classes their relationship as well as their collaboration. In objector, classes are divided into entity y classes and control classes. The Computer Aided Software Engineering (CASE) tools that are available commercially do not provide any assistance in this transition. CASE tools take advantage of Meta modeling that is helpful only after the construction of the class diagram. In the FUSION method some object-oriented approach likes Object Modeling Technique (OMT), Classes, and Responsibilities. Collaborators (CRC), etc, are used. Objector used the term "agents" to represent some of the hardware and software system. In Fusion method, there is no requirement phase, where a user will supply the initial requirement document. Any software project is worked out by both the analyst and the designer. The analyst creates the user case diagram. The designer creates the class diagram. But the designer can do this only after the analyst creates the use case diagram. Once the design is over, it is essential to decide which software is suitable for the application

3.1. Architectural Components

Architectural diagram that identifies the functions and their interactions for the corresponding system needs. A user who subscribed to a certain cloud service usually needs to send his/her data as well as associated access control policies to the service provider. After the data are received by the cloud service provider, the service provider will have granted access rights. Using conventional access control mechanisms, the data can be accessed from the Archive Repository based upon the access right. The data's are encrypted and stored in cloud server.

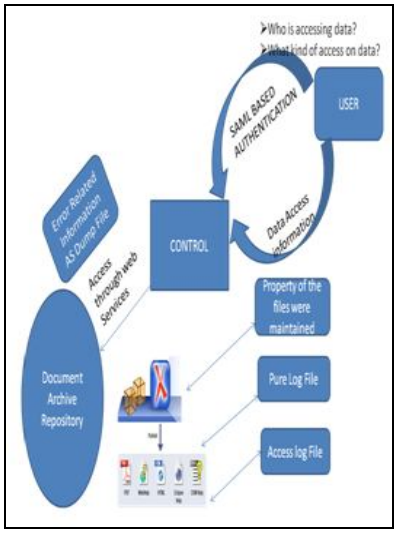

Figure 1: System Architecture

3.2. Module Description

- Captcha based Multi Angle Authentication Module
- User Document Upload Module/Object Access Specify Module

3.2.1. Captcha Based Multi Angle Authentication Module

In this module, the user will be provided a secure login to access our application. The authentication is based on the secure SAML based. The SAML is evaluated with the help of XSD and the valid SAML will be considered for login. Every changes happening on the SAML were traced with the help Janus SAML Tracer. Before hand, the user should have a valid credentials to enter into the system. The authentication is carried out through Web services which provides a secure way of entering into the system. To avoid automatic web crawling option on the web pages, the system is provided with the Anti Captcha facility on the web page. The captcha will be dynamically created based on the time nature of the server password changing, etc.

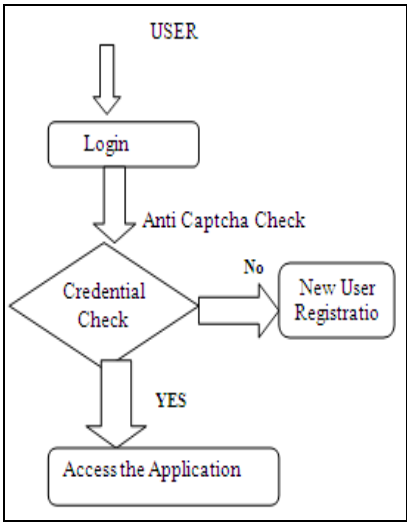

Figure 2: Captcha based multi angle authentication module

3.2.2. Document Navigation Track Module

In this module, the users were permitted to upload their documents. While uploading the document, the user is allowed to provide the access nature on the document. The documents will be archived with the help of rich streaming APIs which integrates the SQL Server Database Engine with an NTFS file system by storing varbinary (max) binary large object (BLOB) data as files on the file system. In addition, the user will be given the option of revoking the access at any time. Based on the access provided the documents will be accessed by the other users internally, the access details will be logged in the Access log file. User will be provided an option of selecting their own algorithm for encryption process.

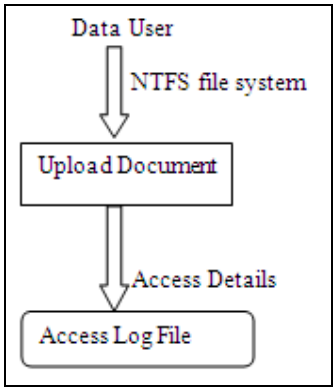

Figure 3: Documentation navigation track module

4. References

1. B. Chun and A.C. Bavier, (2007) "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS).
2. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.
3. E. Barka and A. Lakas, (2008) "Integrating Usage Control with SIP-Based Communications", J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8