IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Secure and Privacy-Preserving Cloud Computing Presents Technical, Legal, and Administrative Challenges

Mr. Kandunuri Rama Krishna[1], Mr. Mohammed Yesuf Mohammed[2], Mr. Abdulahi Mahammed Adem[3], Mr. Suleyman Yimer Abebe[4]

Assistant Professor, Department of Computer Science & Engineering, Samara University, Semara, Ethiopia[1]

Lecturer, Department of Computer Science & Engineering, Samara University, Semara, Ethiopia[2,3,4]

Abstract: In this paper, in this Project We Proposed Securely encryption schemes have proven to offer a high level of security, but they require lengthy computations; more efficient and scalable security solutions are thus needed. Traditional distributed architectures uphold trust by enforcing security policies. However, in cloud deployment models, data and application control is delegated; hence traditional policy-based enforcement presents a number of challenges. Reliable enforcement is a critical aspect of cloud service dependability. A trusted third party within a cloud environment is often used together with cryptographic methods to ensure the integrity, authenticity, and confidentiality of both data and communication. Protecting a user's account from misuse is an important part of the larger problem of controlling access to cloud-based resources (such as objects, memory, devices, and soft ware). Cryptographic authentication solutions can help facilitate secure resource utilization. Secure and privacy-preserving cloud computing presents technical, legal, and administrative challenges. Our focus here is on the technical issues. The main aspects of security, confidentiality, integrity, and availability must be addressed at the client side, the connection, and the server side. The major issue is that all three operate in and are part of shared environments; hence their security and privacy requirements must be combined. The importance of cloud security has been widely acknowledged, and several organizations, such as the Cloud Security Alliance have been looking at it from different perspectives. Cloud services have three basic models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Although these models have major differences, they share many security- and privacy-related issues.

Keywords: network of nodes, Data Sanitization, Denial of Service, software as a service, data computation, infrastructure as a service, Securely encryption, Software metrics, platform as a service.

I. INTRODUCTION

Security of stored data, access management, data utilization management, and trust are among the primary security aspects in cloud computing. A particularly promising approach to improving security in cloud computing is the use of cryptographic methods. Because of limitations in computational efficiencies and associated constraints, traditional cryptographic techniques aren't yet widely used in cloud-based environments. Proposed Securley encryption schemes have proven to offer a high level of security, but they require lengthy computations; more efficient and scalable security solutions are thus needed.

Trustworthy cloud computing relies on two parties performing certain tasks in a dependable manner. Traditional distributed architectures uphold trust by enforcing security policies. However, in cloud deployment models, data and application control is delegated; hence traditional policy-based enforcement presents a number of challenges. Reliable enforcement is a critical aspect of cloud service dependability. A trusted third party within a cloud environment is often used together with cryptographic methods to ensure the integrity, authenticity, and confidentiality of both data and communication.

II. SYSTEM OVERVIEW

Secure and privacy-preserving cloud computing presents technical, legal, and administrative challenges. Our focus here is on the technical issues. The main aspects of security, confidentiality, integrity, and availability must be addressed at the client side, the connection, and the server side. The major issue is that all three operate in and are part of shared environments; hence their security and privacy requirements must be combined. The importance of cloud security has been widely acknowledged, and several organizations, such as the Cloud Security Alliance have been looking at it from

DOI10.17148/IJARCCE.2017.64161

different perspectives. Cloud services have three basic models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Although these models have major differences, they share many security- and privacy-related issues.
A major concern of cloud users is the potential for losing data privacy. Once the data has moved to the cloud. Customers need assurance that their data is well protected by cloud service providers. Encryption can alleviate this fear, but it also has drawbacks. To avoid time-consuming downloading and uploading of data for customers, the cloud provider can perform operations in the cloud. However, to manipulate encrypted data in the cloud, users must share their encryption/decryption keys with the cloud provider, effectively allowing them access to the data.

One of the top threats to cloud computing is malicious insiders. An insider can be a rogue administrator employed by a cloud service provider, an employee of the victim organization who exploits vulnerabilities to gain unauthorized access, or an attacker who uses cloud resources to launch attacks. The multitenant nature of the cloud computing environment makes it difficult to detect and prevent insider attacks. Securleyencryption allows computations to be carried out on encrypted data (also known as cipher text), thus generating an encrypted result, which, when decrypted, matches the result of the same operations performed on the original data (plaintext). This can be a major advantage for applications that outsource encrypted data to the cloud.
Securleyencryption is attractive for many applications, but it has a serious limitation: the Securleyproperty is typically restricted to one operation only, usually addition or multiplication.

III. THE WORKING PRINCIPLE

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantee:

1) Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users.

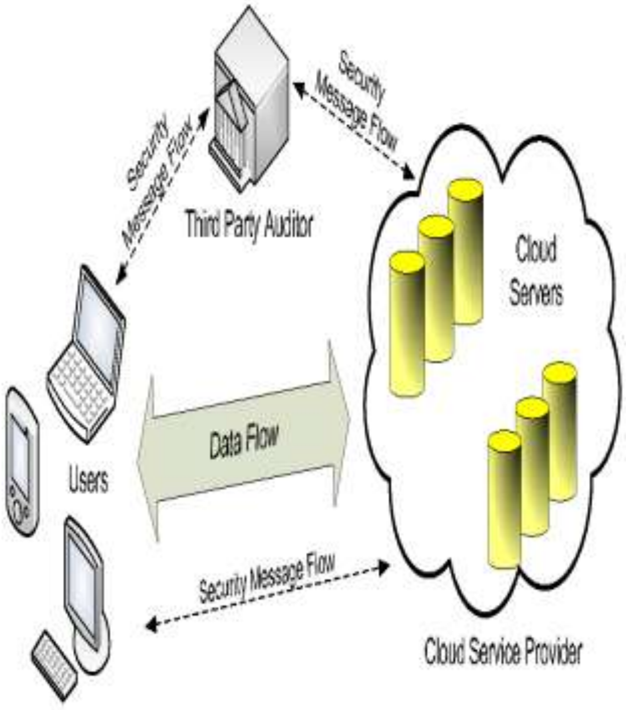


Fig. 1: The architecture of cloud data storage service

2) Storage correctness: to ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users' data intact.

DOI10.17148/IJARCCE.2017.64161

3) Privacy-preserving: to ensure that there exists no way for TPA to derive users' data content from the information collected during the auditing process.
4) Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.
5) Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead

3.1 FUNCTIONAL REQUIREMENTS

- Functional Requirements refer to very important system requirements in a software engineering process (or at micro level, a sub part of requirement engineering) such as technical specifications, system design parameters and guidelines, data manipulation, data processing and calculation modules etc.
- Functional Requirements are in contrast to other software design requirements referred to as Non-Functional Requirements which are primarily based on parameters of system performance, software quality attributes, reliability and security, cost, constraints in design/implementation etc.
- The key goal of determining "functional requirements" in a software product design and implementation is to capture the required behavior of a software system in terms of functionality and the technology implementation of the business processes.
- The Functional Requirement document (also called Functional Specifications or Functional Requirement Specifications), defines the capabilities and functions that a System must be able to perform successfully.
- Functional Requirements should include:
- Descriptions of data to be entered into the system
- Descriptions of operations performed by each screen
- Descriptions of work-flows performed by the system
- Descriptions of system reports or other outputs
- Who can enter the data into the system?
- How the system meets applicable regulatory requirements
- The functional specification is designed to be read by a general audience. Readers should understand the system, but no particular technical knowledge should be required to understand the document.
- Functional requirements should include functions performed by specific screens, outlines of work-flows performed by the system and other business or compliance requirements the system must meet.
- Interface requirements
- Field accepts numeric data entry
- The spreadsheet can secure data with electronic signatures
- Security Requirements
- Member of the Data Entry group can enter requests but not approve or delete requests
- Members of the Managers group can enter or approve a request, but not delete requests
- Members of the Administrators group cannot enter or approve requests, but can delete requests
- The functional specification describes what the system must do; how the system does it is described in the Design Specification.
- If a User Requirement Specification was written, all requirements outlined in the user requirement specification should be addressed in the functional requirements.

3.2 NON FUNCTIONAL REQUIREMENTS

- All the other requirements which do not form a part of the above specification are categorized as Non-Functional Requirements.
- A system may be required to present the user with a display of the number of records in a database. This is a functional requirement.
- How up-to-date this number needs to be is a non-functional requirement. If the number needs to be updated in real time, the system architects must ensure that the system is capable of updating the displayed record count within an acceptably short interval of the number of records changing.
- Sufficient network bandwidth may also be a non-functional requirement of a system.

A particularly promising approach to improving security in cloud computing is the use of cryptographic methods. Because of limitations in computational efficiencies and associated constraints, traditional cryptographic techniques aren't yet widely used in cloud-based environments.2 Proposed Securleyencryption schemes have proven to offer a high level of security, but they require lengthy computations; more efficient and scalable security solutions are thus needed.

DOI10.17148/IJARCCE.2017.64161

Trustworthy cloud computing relies on two parties performing certain tasks in a dependable manner. Traditional distributed architectures uphold trust by enforcing security policies. However, in cloud deployment models, data and application control is delegated; hence traditional policy-based enforcement presents a number of challenges. Reliable enforcement is a critical aspect of cloud service dependability. A trusted third party within a cloud environment is often used together with cryptographic methods to ensure the integrity, authenticity, and confidentiality of both data and communication.

IV. IMPLEMENTATION OF SYSTEM

4SYSTEM DESIGN: The Unified Modeling Language allows the software engineer to express an analysis model using the modeling notation that is governed by a set of syntactic semantic and pragmatic rules.A UML system is represented using five different views that describe the system from distinctly different perspective.

Class Diagram

Classes: These titled boxes represent the classes in the system and contain information about the name of the class, fields, methods and access specifies. Abstract roles of the Class in the system can also be indicated.
Interfaces: These titled boxes represent interfaces in the system and contain information about the name of the interface and its methods. Relationship Lines that model the relationships between classes and interfaces in the system.
Dependency: A dotted line with an open arrowhead that shows one entity depends on the behavior of another entity. Typical usages are to represent that one class instantiates another or that it uses the other as an input parameter
Aggregation: Represented by an association line with a hollow diamond at the tail end. An aggregation models the notion that one object uses another object without "owning" it and thus is not responsible for its creation or destruction.
Inheritance: A solid line with a solid arrowhead that points from a sub-class to a super class or from a sub-interface to its super-interface.
Implementation: A dotted line with a solid arrowhead that points from a class to the interface that it implement

V.SYSTEM IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.
The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

MODULES

1. Admin Module.
2. Access Control as a Value-Added-Service.
3. Reliable Credential Management.
4. User Module.

Module Description

1. Admin Module

In this module we find the correlation relationships among huge amounts of data and creating the buckets. This process analyzes users searching habits by finding associations between the different types of data that users place in their baskets.

2. Access Control as a Value-Added-Service

In this module for cloud-based utility service models, offering access control as a value added service. Achieving this requires devising sufficiently secure utility models. Solutions that perceive the concept of security as a value added service typically consider an overlay service.

3. Reliable Credential Management

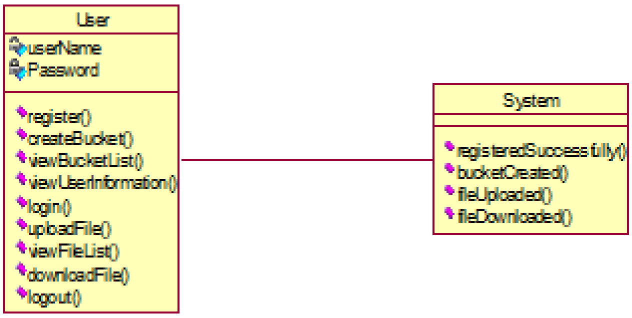
Robust authentication is vital in access control: authorizations are granted to authenticate users only. An important aspect of this is the management of identity credentials. Trustworthy identity management is essential to ensure reliable data utilization management. Useful trust evaluation metrics are proposed to estimate the reliability of security, and to be offered as a cloud utility service. The significance of trust evaluation is vital to ensure secure collaborative data sharing, data analytics, and data outsourcing.

4. User Module

To enter into this module the user must be first registered, after login using user name, password he/she can upload files, view files and download files.

DOI10.17148/IJARCCE.2017.64161

This module is used for only authorized persons, if unauthorized person login error message is wrong user name and password.



Sample source code:
Login.jsp

```
<% String msg=request.getParameter("msg");%>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Security and Privacy in Cloud Computing</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="stylesheet" href="css/style.css" type="text/css" media="screen, projection, tv" />
<link rel="stylesheet" href="css/style-print.css" type="text/css" media="print" />
</head>
<body>
<BR><BR><BR><div>
<img src="img/title.png" width="1335" height="102" />
</div>
<hr class="noscreen" />
<BR><BR><div>
<div>
<ul class="menu">
<li><a href="index.html" class="active"> <img src="img/Home.png width="139" height="58"
/></a>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;
<a href="Reg.jsp"><img src="img/Reg.png" width="227" height="58" /></a>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;
<!--<li><a href="#">Portfolio</a></li>-->
<a href="Login.jsp"><img src="img/Login.png" width="227" height="58"
/></a></li>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;
</ul>
</div>
<div id="skip-menu"></div>
<div class="column-right">
<div class="box">
<div class="box-top"></div>
<div class="box-in">
<h2>Login</h2>
<!--<p>Introducing Privacy Preserving of your files</p>
<p>We provide privacy to your files in cload storage. With high security by using encryption and decryption technique to your private data. We also store publice and sharable data in the cloud.</p>
<br /> -->
<center> <%if(msg!=null){%>
<h2><font color="red"><%=msg%></font></h2>
<%}%></center>
<center/>
        <form name="f2" action="Login1.jsp" method="post">
```

DOI10.17148/IJARCCE.2017.64161

```
<table cellspacing="10" >
<tr><td>Username</td><td><input type="text" name="username"></td></tr>
<tr><td>password</td><td><input type="password" name="psw"></td></tr>
<tr><td><input type="submit" value="Login"></td><td><input type="reset" value="Reset"></td></tr>
</table>
</center>
</div>
</div>
<!--<div class="box-bottom">
<hr class="noscreen" />
<div class="footer-info-left"><a href="http://all-free-download.com/free-website-templates/">My personal
website</a>, 2008. All rights reserved.</div>
<div class="footer-info-right"><a href="http://www.mantisatemplates.com/">Mantis-a templates</a></div>
</div>
</div>-->
<div class="cleaner">&nbsp;</div>
</div>
</div>
<!--<div align=center>This template  downloaded form <a href='http://all-free-download.com/free-website-
templates/'>free website templates</a></div>-->
</body>
</html>
```

Privateupload.jsp

```
<%@page import="java.sql.*"%>
<%
        String username=(String)session.getAttribute("username");
        session.setAttribute("username",username);
        String email="";
        try
        {
        Class.forName("com.mysql.jdbc.Driver");
        Connection con=DriverManager.getConnection("jdbc:mysql://localhost:3306/privacy","root","root");
        Statement st=con.createStatement();
        ResultSet rs=st.executeQuery("select email from reg where username='"+username+"'");
        if(rs.next())
                {
                email=rs.getString(1);
                }
        }
        catch(Exception e)
        {
        System.out.println(e);
        }
%>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Security and Privacy in Cloud Computing</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="stylesheet" href="css/style.css" type="text/css" media="screen, projection, tv" />
```

VI. CONCLUSION AND FUTURE ENHANCEMENTS

In the recent past, cryptographic solutions have been increasingly popular as viable solutions to secure Data storage and access control. Some of the cryptographic techniques are attractive in terms of security, efficiency, and scalability. Advanced encryption schemes such as Securleyencryption ensure strong security at the expense of heavy computational overheads. Improving efficiency and scalability with respect to cloud deployment models and application-specific demands requires more research effort. Required and the period of key update for practical deployment.

REFERENCES

1. S. Yu et al., "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE Conf. Computer Comm.(INFOCOM 10), 2010, pp. 1–9; doi:10.1109/INFCOM.2010.5462174.
2. Y. Tang et al., "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 6, 2012, pp. 903–916.
3. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol.21, no. 2, 1978, pp. 120–126.
4. C. Gentry, "A Fully SecurleyEncryption Scheme," PhD dissertation, Dept. of Computer Science, Stanford Univ., 2009.
5. C.H. Tai, P.S. Yu, and M.S. Chen, "k-Support Anonymity Based on Pseudo Taxonomy for Outsourcing Of Frequent Itemset Mining," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and DataMining (KDD),2010,pp.473–482.
6. F. Giannotti et al., "Privacy-Preserving Mining of Association Rules from Outsourced Transaction Databases,"IEEE Systems J., vol.7, no.3, 2013,pp. 385–395.
7. W.K. Wong et al., "Security of Outsourcing of Association Rule Mining," Proc. Int'l Conf. Very Large Databases (VLDB 07), 2007, pp. 111–122.
9. I. Molloy, N. Li, and T. Li, "On the (In)Security and (Im)Practicality of Outsourcing Precise Association Rule Mining," Proc. IEEE Conf. Data Mining (ICDM 09),2009, pp. 1–10.
10.IHS Technology, "Cloud-Related Spending by Businesses Triple from 2011 to 2017," http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011-2017.

BIOGRAPHIES

Mr. K. Ramakrishna, presently working as an assistant professor in computer science engineering and technology department, samara university, samara ,Ethiopia. Doing my Doctor of philosophy in computer science engineering in sri satyasai university of technology and medical sciences, sehore, India. He received the master of technology degree in VNR Vignana Jyothi Institute of Engineering and Technology- Jawaharlal Nehru Technological University Hyderabad, India . He received the bachelor of technology degree in The Vazir Sultan College of Engineering And technology, Kakatiya University, Warangal, India. He Has 8+ Years Teaching Experience, His Research Interests Include mobile ad-hoc networks , Data Mining, Information Security, Software Testing, mobile communication and cloud computing.

Mr. Mohammed Yesuf Mohammed, presently working as a lecturer in computer science department, samara university, semara ,Ethiopia..He received the Master of Science in Hawassa University, Hawassa ,Ethiopia in 2015. He received the bachelor of science degree in Wollo university,Dessie ,Ethiopia,2010. He Has 4+ Years Teaching Experience, His Research Interests Include mobile ad-hoc networks , Data Mining, Information Security, Software Testing, mobile communication, cloud computing and Green technology.

Mr.Abdulahi Mahammed Adem, presently working as a lecturer in computer science department, samara university, semara ,Ethiopia..He received the Master of Computer Application (MCA) in Andhra University, Andhra Pradesh ,INDIA in 2015. He received the bachelor of science degree in Mekelle university,Mekelle,Ethiopia,2010. He Has 4+ Years Teaching Experience, His Research Interests Include Computer Security, mobile ad-hoc networks , Data Mining, Information Security, Software Testing, mobile communication, cloud computing and Green technology.

Mr Suleyman Yimer Abebe presently working as a lecturer in computer science department, samara university, semara, Ethiopia.. He received the Master of Computer Application (MCA) in Andhra University, Andhra Pradesh ,India in 2016.He received the bachelor of science degree in Arba Minch university, Arba Minch, Ethiopia, 2009. He Has 4+ Years Teaching Experience, His Research Interests Include mobile ad-hoc networks, Data Mining, Information Security, Software Testing, mobile communication, cloud computing and Green technology.

DOI10.17148/IJARCCE.2017.64161