Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Cloud Computing Security potential for migration from a single cloud to a Multi-Cloud Environment

B.Srinivasulu [#1] , S.V.SRIDHAR [#2,] U.Narasimhulu[#3,]K.Ramakrishna[#4]

Hyderabad(A.P),India

Abstract – this paper we propose and evaluate The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility ofdata. Ensuring the security of cloud computing is a major factor inthe cloud computing environment, asusers often store sensitive information with cloudstorage providers but these providers may beun trusted. Dealing with "single cloud" providers ispredicted to become less popular with customers dueto risks of service availability failure and thepossibility of malicious insiders in the single cloud. Amovement towards "multi-clouds", or in other words,"Inter clouds" or "cloud-of-clouds" has emergedrecently.This mainly focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid a untrusted cloudprovider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud Computingis surveyed.

Keywords:, Secret Shring Algoritham, Byzantine Protocol, Byzantinefault tolerance, Integrity Layer.

I. Introduction

The use of cloud computing has increased rapidly in many organizations Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi clouds", "inter cloud" or "cloud-of-clouds".

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid a un trusted cloud provider. Protecting private and important information, such as credit card details or a patient's medicalrecords from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed.

Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' serviceInfrastructure. A cloud provider offers many services that can benefit its customers such as fast access to their data from any location, scalability, pay-for-use, data storage, and data recovery, protection against hackers, on-demand security controls, and use of the network and infrastructure facilities

In this we are using "Secret Shring Algoritham "it is used how to store the data in different clouds. It is one type of crypto graphic algorithm and it is used in security purpose.

In this we are using "byzantine fault tolerance protocol" it is used check the traffic in to the clouds. In this using one formula' 3*f+1'in this 'f' means fault probability.

Background:

Cloud computing as "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". The cloud

Secret sharing algorithm:

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead.

They are algorithms that will share a secret between several parties, such that none of them can know the secret without the help of others. Either all or a subset of them will need to get together and put their parts together to obtain the original secret. A simplistic solution can be achieved by XORing the secret with a random number, then giving the result to one party and the random number to the other. Neither one can find out what the secret was without the other. To retrieve the secret they only need to XOR the two parts together again. This can be extended to any number of parties.

II. System Overview

Byzantine Protocol:

In cloud computing, any faults in software orhardware are known as Byzantine faults that usuallyrelate to inappropriate behavior and intrusion tolerance.In addition, it also includes arbitrary and crash faults .Much research has been dedicated to Byzantinefault tolerance (BFT) since its first introduction. Although BFT research has received a great dealof attention, it still suffers from the limitations of practical adoption and remains peripheral in distributed systems .The relationship between BFT and cloudcomputing has been investigated, and many argue thatin the last few years, it has been considered one of themajor roles of the distributed system agenda.Furthermore, many describe BFT as being of onlypurely academic interest" for a cloud service. Thislack of interest in BFT is quite different to the level ofinterest shown in the mechanisms for tolerating crashfaults that are used in large-scale systems. Reasons thatreduce the adoption of BFT are, for example, difficulties in design, implementation, or understanding of BFT protocols.

As mentioned earlier, BFT protocols are notsuitable forsingle clouds.One of the limitations of BFT for the inner-cloud is thatBFT requires a high level of failure independence, asdo all fault-tolerant protocols. If Byzantine failureoccurs to a particular node in the cloud, it is reasonable to have a different operating system, different implementation, and different hardware to ensure suchfailuredoes not spread to other nodes in the samecloud. In addition, if an attack happens to a particularcloud, this may allow the attacker to hijack theparticular inner-cloud infrastructure.

Security Risks in Cloud Computing:

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment. Users of online data sharing or network facilities are aware of the potential loss of privacy. According to a recent IDC survey, the top challenge for 74% of CIOs in relation to cloud computing is security. Protecting private and important information such as credit card details or patients' medical records from attackers or malicious insiders is of critical importance. Moving databases to a large data Centre involves many security challenges such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. , which are data storage security, application security, data transmission security, and security related to third-party resources.

In different cloud service models, the security responsibility between users and providers is different. According to their EC2 addresses security control in relation to physical, environmental, and virtualization security, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data.

The way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user's applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users' data. t the levels of security issues in IaaS are different. The impact of security issues in the public cloud is greater than the impact in the private cloud. For instance, any damage which occurs to the security of the physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems.

In the cloud environment, the physical infrastructure that is responsible for data processing and data storage can be affected by a security risk. The path for the transmitted data can be also affected, especially when the data is transmitted to many third-party infrastructure devices. As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the Internet; consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through networks which may be insecure. As a result, internet security problems will affect the cloud, with greater risks due to valuable resources stored within the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used in the Internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud. Data intrusion of the cloud through the Internet by hack cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients .

Current Solutions of Security Risks:

In order to reduce the risk in cloud storage, customers can use cryptographic methods to protect the stored data in the cloud. Using a hash function is a good solution for data integrity by keeping a short hash in local memory. In this way, authentication of the server responses is done by recalculating the hash of the received data which is compared with the local stored data. If the amount of data is large, then a hash tree is the solution. Many storage system prototypes have implemented hash tree functions; at this is an active area in research on cryptographic methods for stored data authentication. that although the previous methods allow consumers to ensure the integrity of their data which has been returned by servers, they do not guarantee that the server will answer a query without knowing what that

Query is and whether the data is stored correctly in the server or not. in cloud storage and running Byzantine-fault-tolerant protocols on them where each cloud maintains a single replica.

Analysis of Multi-Cloud Research:

Moving from single clouds or inner-clouds to multi clouds is reasonable and important for many reasons. "Services of single clouds are still subject to outage". In addition, showed that over 80% of company management "fear security threats and loss of control of data and systems" assumes that the main purpose of moving to inter clouds is to improve what was offered in single clouds by distributing reliability, trust, and security among multiple cloud providers. In addition, reliable distributed storage which utilizes a subset of BFT techniques was suggested to be used in multi-clouds. A number of recent studies in this area have built protocols for inter clouds, utilizes RAID-like techniques that are normally used by disks and file systems, but for multiple cloud storage. Assume that to avoid "vender lock-in", distributing a user's data among multiple clouds is a helpful solution. This replication also decreases the cost of switching providers and offers better fault tolerance. Therefore, the storage load will be spread among several providers as a result of the RACS .HAIL (High Availability and Integrity Layer) is another example of a protocol that controls multiple clouds. HAIL is a distributed cryptographic system that permits a set of servers to ensure that the client's stored data is retrievable and integral. HAIL provides a software layer to address availability and integrity of the stored data in an inter clouds

III. The Working Principle

Technical Background:

JSP:

Java server Pages is a simple, yet powerful technology for creating and maintaining dynamic-content web pages. Based on the Java programming language, Java Server Pages offers proven portability, open standards, and mature re-usable component model .The Java Server Pages architecture enables the separation of content generation from content presentation. This separation not eases maintenance headaches; it also allows web team members to focus on their areas of expertise. Now, web page designer can concentrate on layout, and web application designers on programming, with minimal concern about impacting each other's work.

Portability:

Java Server Pages files can be run on any web server or web-enabled application server that provides support for them. Dubbed the JSP engine, this support involves recognition, translation, and management of the Java Server Page lifecycle and its interaction components.

Components :

It was mentioned earlier that the Java Server Pages architecture can include reusable Java components. The architecture also allows for the embedding of a scripting language directly into the Java Server Pages file. The components current supported include Java Beans, and Servlets.

Processing

A Java Server Pages file is essentially an HTML document with JSP scripting or tags. The Java Server Pages file has a JSP extension to the server as a Java Server Pages file. Before the page is served, the Java Server Pages syntax is parsed and processed into a Servlet on the server side. The Servlet that is generated outputs real content in straight HTML for responding to the client.

Access Models:

A Java Server Pages file may be accessed in at least two different ways. A client's request comes directly into a Java Server Page. In this scenario, suppose the page accesses reusable Java Bean components that perform particular well-defined computations like accessing a database. The result of the Beans computations, called result sets is stored within the Bean as properties. The page uses such Beans to generate dynamic content and present it back to the client.

In both of the above cases, the page could also contain any valid Java code. Java Server Pages architecture encourages separation of content from presentation.

HTML:

HTML, an initialism of Hypertext Markup Language, is the predominant markup language for web pages. It provides a means to describe the structure of text-based information in a document by denoting certain text as headings, paragraphs, lists, and so on and to supplement that text with interactive forms, embedded images, and other objects. HTML is written in the form of labels (known as tags), surrounded by angle brackets. HTML can also describe, to some degree, the appearance and semantics of a document, and can include embedded scripting language code which can affect the behavior of web browsers and other HTML processors.HTML is also often used to refer to content of the MIME type text/html or even more broadly as a generic term for HTML whether in its XML-descended form (such as XHTML 1.0 and later) or its form descended directly from SGML

Hyper Text Markup Language

Hypertext Markup Language (HTML), the languages of the World Wide Web (WWW), allows users to produces Web pages that include text, graphics and pointer to other Web pages (Hyperlinks).

HTML is not a programming language but it is an application of ISO Standard 8879, SGML (Standard Generalized Markup Language), but specialized to hypertext and adapted to the Web. The idea behind Hypertext is that instead of reading text in rigid linear structure, we can easily jump from one point to another point. We can navigate through the information based on our interest and preference. A markup language is simply a series of elements, each delimited with special characters that define how text or other items enclosed within the elements should be displayed. Hyperlinks are underlined or emphasized works that load to other documents or some portions of the same document.

HTML can be used to display any type of document on the host computer, which can be geographically at a different location. It is a versatile language and can be used on any platform or desktop.

HTML provides tags (special codes) to make the document look attractive. HTML tags are not case-sensitive. Using graphics, fonts, different sizes, color, etc., can enhance the presentation of the document. Anything that is not a tag is part of the document itself.

Basic HTML Tags:

<! -- -->	specifies comments
<A>……….</A>	Creates hypertext links
<B>……….</B>	Formats text as bold
<BIG>……….</BIG>	Formats text in large font.
<BODY>…</BODY>	Contains all tags and text in the HTML document
<CENTER>...</CENTER>	Creates text
<DD>…</DD>	Definition of a term
<DL>...</DL>	Creates definition list
<FONT>…</FONT>	Formats text with a particular font
<FORM>...</FORM>	Encloses a fill-out form
<FRAME>...</FRAME>	Defines a particular frame in a set of frames
<H#>…</H#>	Creates headings of different levels(1 – 6)
<HEAD>...</HEAD>	Contains tags that specify information about a document
<HR>...</HR>	Creates a horizontal rule
<HTML>…</HTML>	Contains all other HTML tags
<META>...</META>	Provides meta-information about a document
<SCRIPT>…</SCRIPT>	Contains client-side or server-side script
<TABLE>…</TABLE>	Creates a table

IV.Implementation Of System

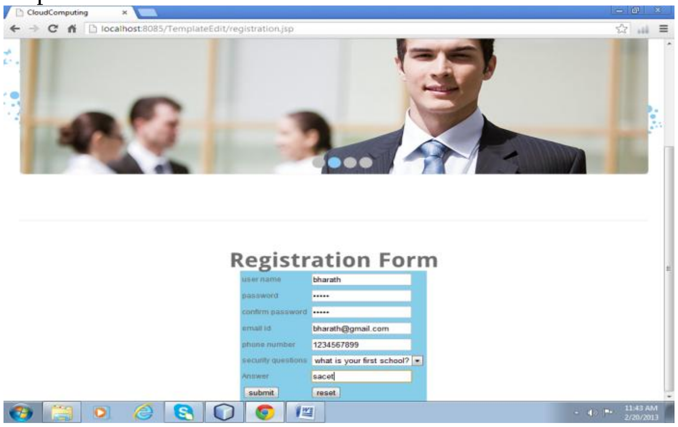
Uploading file:

```
<%@page import="java.util.Random"%>
<%
try
{
String name=session.getAttribute("admin").toString();
out.println("<font color='blue' size='6'>Welcome to "+name+"</font>");
%>
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<!DOCTYPE html>
<html>
<head>
<title>CloudComputing</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="css/style.css" rel="stylesheet" type="text/css" />
<link rel="stylesheet" type="text/css" href="css/coin-slider.css" />
<script type="text/javascript" src="js/cufon-yui.js"></script>
<script type="text/javascript" src="js/droid_sans_400-droid_sans_700.font.js"></script>
<script type="text/javascript" src="js/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="js/script.js"></script>
<script type="text/javascript" src="js/coin-slider.min.js"></script>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>JSP Page</title>
</head>
```

```
<body>
<div class="main">
<div class="header">

<div class="header_resize">
<div class="logo">
<h1><a href="index.html">ADMIN <span>HOME PAGE</span><small></small></a></h1>
</div>
<div class="clr"></div>
<div class="menu_nav">
<ul>
<li class="active"><a href="AdminHome.jsp"><span>HOME PAGE</span></a></li>

<li><a href="upload.jsp"><span>UPLOAD FILE</span></a></li>
<li><a href="viewusers.jsp"><span>VIEW USERS</span></a></li>
<li><a href="viewfeedback.jsp"><span>VIEW FEEDBACK</span></a></li>
<li><a href="index.html"><span>LOGOUT</span></a></li>

</ul>
</div>
<div class="clr"></div>
<div class="slider">
<div id="coin-slider"><a href="#"><img src="images/slide1.jpg" width="960" height="335"
alt="" /></a><a href="#"><img src="images/slide3.jpg" width="960" height="335" alt="" /></a><a href="#"><img
src="images/img1.jpg" width="960" height="335" alt="" /></a><a href="#"><img src="images/img2.jpg" width="960"
height="335" alt="" /></a></div>

<div class="clr"></div>
</div>
<div class="clr"></div>
</div>
</div>
<div class="content">
<div class="content_resize">
<div class="mainbar">
<div class="clr"></div>
</div>
</div>
</div>
<div class="clr"></div>
</div>
</div>
```

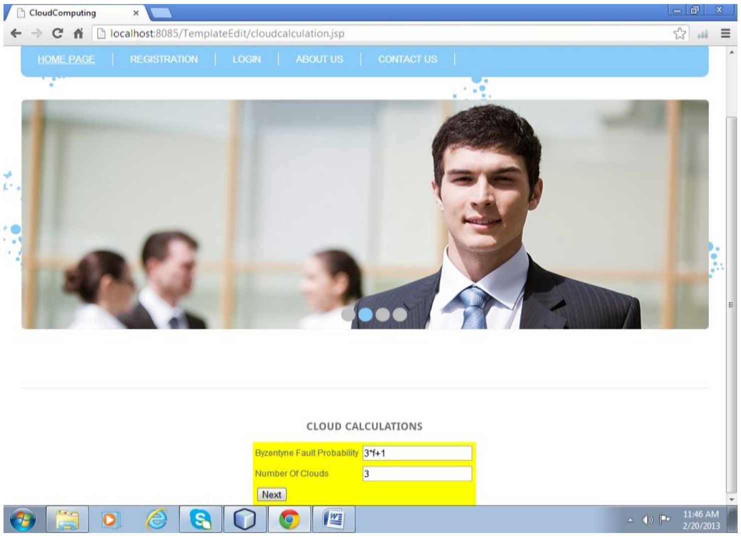
V.EXPERIMENTAL RESULTS

The concept of this paper is implemented and different results are shown below.



Registration Form

user name	bharath
password	•••••
confirm password	•••••
email id	bharath@gmail.com
phone number	1234567899
security questions	what is your first school?
Answer	sacet
submit	reset

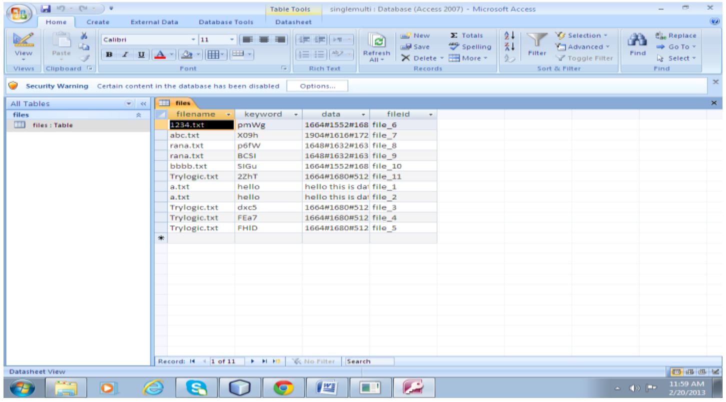

CloudComputing
localhost:8085/TemplateEdit/cloudcalculation.jsp
HOME PAGE | REGISTRATION | LOGIN | ABOUT US | CONTACT US
11:46 AM
2/20/2013

CLOUD CALCULATIONS

Byzentyne Fault Probability: 3*f+1

Number Of Clouds: 3

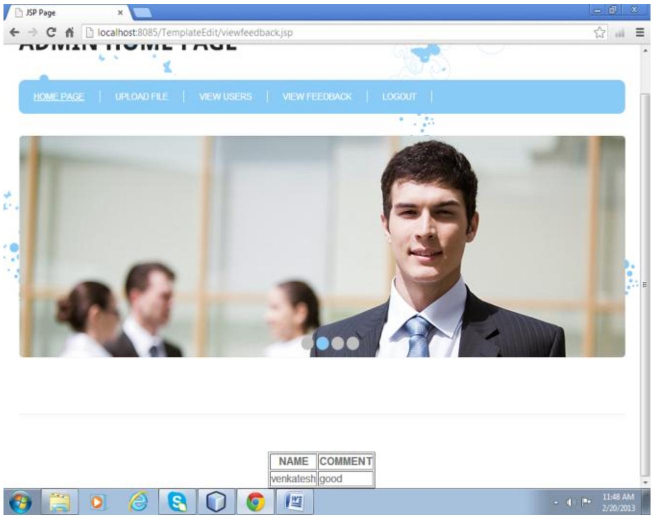
Next



Security Warning Certain content in the database has been disabled

files

filename	keyword	data	fileid
1234.txt	pmWg	1664#1552#168	file_6
abc.txt	X09h	1904#1616#172	file_7
rana.txt	p6fW	1648#1632#163	file_8
rana.txt	BCSI	1648#1632#163	file_9
bbbb.txt	SIGu	1664#1552#168	file_10
Trylogic.txt	2ZhT	1664#1680#512	file_11
a.txt	hello	hello this is dat	file_1
a.txt	hello	hello this is dat	file_2
Trylogic.txt	dxc5	1664#1680#512	file_3
Trylogic.txt	FEa7	1664#1680#512	file_4
Trylogic.txt	FHID	1664#1680#512	file_5


JSP Page
localhost:8085/TemplateEdit/viewfeedback.jsp
ADMIN HOME PAGE
HOME PAGE | UPLOAD FILE | VIEW USERS | VIEW FEEDBACK | LOGOUT
11:48 AM
2/20/2013

NAME	COMMENT
venkatesh	good

VI.Conclusion

It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multiclouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

VI. Future Enhancements

For future work, we aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity.

In relation to data intrusion and data integrity, assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder. This depends on Shamir's secret sharing algorithm with a polynomial function technique which claims that even with full knowledge of (k – 1) clouds, the service provider will not have any knowledge of vs (vs is the secret value) . We have used this technique in previous databases-as-a-serves research . In other words, hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud. Therefore, if the attacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider (in the case where k = 3) to know the secret which is the worst case scenario.

References

1. (NIST), http://www.nist.gov/itl/cloud/ . [2] I. Abraham, G. Chockler, I. Keidar and D. Malkhi,
2. "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.
3. H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1 ACM symposium on Cloud computing, 2010, pp. 229-240.
4. D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25 Intl. Conf. on Data Engineering, 2009, pp. 1709-1716.
6. Amazon, Amazon Web Services. Web services licensing agreement, October3,2006.
7. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM 54985498 Conf. on Computer and communications security, 2007, pp. 598-609.
8. A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6 Conf. on Computer systems, 2011, pp. 31-46.

Authors:

Mr B.Srinivasulu, Post Graduated in CSE(M.Tech) From JNTUH, 2010, and graduated in Computer Science & Engineering (B.TECH) From JNTU Hyderabad, 2008. He is working presently as Asst.Professor in Department of Computer Science & Engineering in HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE (HITS), R.R.Dist, A.P, INDIA.He Is Has 2+ Years Experience,His Research Interests Include Data Warehousing & Data Mining and Cloud Computing and mobile communication.

Mr.S.V.SRIDHAR, Presently working as: an Associate Professor in CSE in Holy Mary Institute of Technology & Science (College Of Engineering), Bogaram (V), Keesara (M), R.R. Dist,,QUALIFICATIONS: M.Tech (CSE) in IETE, M.C.A , M.Sc (Electronics). His research interests include Data Warehousing & Data Mining and Cloud Computing.

Mr.U.Narasimhulu, graduated in Computer Science & Engineering B.Tech(CSE) from JNTUA,and is Post Graduated in M.Tech(CSE) JNTUA A.P,India.He Is Working presently as Assistant Professor In Department of Computer Science And engineering in Avanthi scientific technology & research academy,His research interests include Data Mining and Cloud Computing.

Mr K.Ramakrishna, Post Graduated in CSE(M.Tech) From JNTUH, 2010, and graduated in Information Technology& Engineering (B.TECH) From K.U.He is working presently as Asst.Professor in Department of Computer Science & Engineering in HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE (HITS), INDIA.He Is Has 3+ Years Experience,His Research Interests Include Data Warehousing & Data Mining and Cloud Computing and mobile communication