Cloud deployment with Java implementation of Cloud data security algorithm

Dr. Sunil Kumar
Assistant Professor, School of IT
AURO University
Surat, Gujarat.

Dr. Jayant Shekhar
Professor, CSE
Adama Science and Technology University,
Euthopia

***Abstract*— Cloud computing is one of the major evolution of IT industry that not only gives economical benefits, but also gives the rapid scalability, on-demand universal accessibility and much more. All these features are the major attraction for the IT related organizations and users. But due to some data security issues, still many users are afraid from using the cloud computing services. In this paper, we implemented our already proposed data security algorithm, using Java programming language that is best suited for web application development and deployed on IBM Bluemix Cloud platform.**

Keywords—Encryption; Cloud data security; Encryption algorithm; Information security; Cloud computing; Cloud deployed security Algorithm.

I. INTRODUCTION

. When the computer has started or has been developed, we are very well associated with the computing term which is the process of utilizing computer technology to complete a task. Technology which help task to perform computing known as computing technology like mobile computing, grid computing or cloud computing. As we know that cloud is a mass of droplet in the sky or it is floating on our surface and attracted with gravity and in the form rain it comes to the earth so with this term cloud computing term has been developed in the IT industry. In the IT, cloud is the mass of infrastructures, high-end applications and services which are floated in the data centres similar to the original cloud that float in the sky. Here cloud is attracted by organizations and users for renting the services, applications or infrastructures from the data centers. So, cloud computing is a term through which we can hire the computing capabilities from the data centers, where mass of infrastructure or services are floated. Every big IT company is now joining their hand with the cloud computing because of the economical, pay-as-per-use and rapid scalability features. Some of them are Microsoft, IBM, Google, Amazon are Force.com that are adopting Cloud for expending their businesses. Cloud computing also affect the daily life of us, Kosie Eloff [1] has shown in his presentation that how the Dropbox, Google Drive, Apple icloud, SpiderOak for Linux and OneDrive of Microsoft are now replacing the physical flash drive for sharing the transporting our data from one place to another and it has taken a place on the desktop of our PC or laptop and mobiles to store a copy of our data on the cloud server freely and giving freedom of accessibility around the world with a single login facility using the internet. When lots of data is accessed from the data centres to cloud users and vice versa, some cyber attackers want to hack the session or remote server to stolen the data for their personal benefits. So, if security parameters are taken care properly, we can motivate more users (individual and organizations) to join the cloud revolution.

The paper is organized as follows. In Section 2, we discuss on the security requirement of cloud data. In Section 3, we describe the data security algorithm briefly. Whereas, in the Section 4, we highlight the overview of Java language, In Section 5, we show the deployment on IBM Bluemix cloud platform with Java implementation to evaluate the performance using 64-bit processor and in Section 6, we gives the conclusion of the paper with future work.

II. SECURITY REQUIREMENT OF CLOUD DATA

a	*s*	*d*	*f*
0	*011*	*1011*	*1100*

Every day, we listen a fresh news or read a blog about the security attack on the cloud related to availability, data security and many more, to aware us about the cloud computing security risks and threats. As Cloud computing required the internet connectivity, therefore it is always on the target of the hackers. Every cloud related services need techniques for identity management, authentication, authorization, and auditing (IAAA). Most vulnerabilities associated with the IAAA component should be regarded as cloud-specific because they're ubiquitous in state-of-the-art cloud offerings [2]. Some of the vulnerabilities are as follows:

1. Unauthorized access to management interface.
2. Internet protocol vulnerabilities.
3. Data recovery vulnerabilities.
4. Metering and billing evasion.
5. SQL injection.
6. Denial of service by account lockout.
7. Insufficient or faulty authorization checks.
8. Coarse authorization control.

III. OVERVIEW OF SECURITY ALGORITH

In the May month of 2015, JP. Singh et al[3] proposed an authentication and encryption technique for cloud computing. Later on December 2015 S. Kumar et al [4] proposed an improved find and remove the limitation and proposed an improved version of data security and encryption algorithm for cloud computing environment to provide privacy and security to our dynamic cloud data. According to them, they depicts a binary tree to store alphanumeric characters and special characters on each node and associate a binary value (0 or 1) on the link in the tree. To convert given input to encrypted text or ciphertext, each input string is broken into individual character, then a binary value is assigned according to the proposed binary tree. For example, input text is ***asdf***. In the Step 1, a binary value will be assigned to each character, following the binary tree as given in Fig.1.

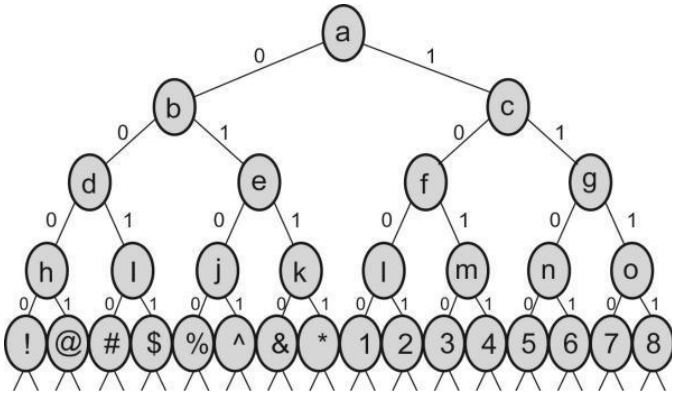

Fig. 1. A Binary Tree along with alpha-numeric values[4] In the Step 2, odd and even position characters are segregated and placed aside to form new string.

a	***d***	***s***	***f***
0	1011	011	1100

In the Step 3, some redundant bits (as a key) are added to each individual character to more secure and hard to break.

a		**d**	**s**	**f**
0	+ 111	1011+111	011+111	1100+111

In the Step 4, a compression technique is applied to make it compact in size to store on the cloud server, from the client or sender side as encrypted text.

Whereas, on the receiver or server side, a decryption algorithm work as follows:

In the Step 1, Un-compress the received compress data from the server. In Step 2, detect and remove the redundancy bit from the uncompressed data.

In Step 3, assign the text value to each binary value, according to the depicted tree. Whereas in the last Step, rearrange the odd and even position binary value to their original position.

A. Advantage of this algorithm

It gives more security with the facility of authentication without remembering lengthy passwords and

numeric values representation also improve the throughput

minimizing the calculation time to generating the encrypted data easily. As we know that authentication is used to identify the user and establishment of assurance of confidentiality.

IV. Overview of Java

Java is an object-oriented, platform independent, robust, secure and multi-threaded programming language was developed by James Gosling and officially launched by Sun Microsystems in 1995. Later in January 2010, Oracle corporation acquire the Sun Microsystems completely[5]. According to Oracle corp.[6], there are 3 billions Mobile devices are running Java and more than 9 millions Java developers are exist. Current version of Java is 8, officially launched in November, 2015[7] that enhanced support for cryptography, stronger algorithms for password-based encryption and much more on Kerberos 5, client-side TLS and SSL/TLS also [8]. In Java, security is available under the two components: first is JCA (Java Cryptography Architecture), provides the support in digital signature and Message digests and second is JCE (Java Cryptography Extension) that deals in the key generation, message authentication and encryption.

V. Deployment on IBM Bluemix Cloud platform

There are many Cloud vendors, who provide platform-as-a-service to deploy user-created application like Google, Microsoft, Amazon, OpenStack and IBM, based on their supported languages environments such as Java, Phython, C# etc. We selected IBM Open Cloud Architecture that is worldwide known as Bluemix, to deploy our Java implemented data security algorithm. Bluemix is the latest cloud product of IBM, which facilitate organizations and developers to access the cloud service for creating, deploying, and managing applications rapidly. We can easily combine enterprise-level services with our cloud applications without the knowledge of installation or configuration. Bluemix implementation is based on open source Platform as a Service (PaaS) known as Cloud Foundry that provide the facility to deploy and manage of the server by

developers cloud apps in easy way. It provides a list of services to that includes: providing additional frameworks and services, Bluemix provides a dashboard for you to create, view, and manage your applications and services as well as monitor your application's resource usage. The Bluemix dashboard also provides the ability to manage organizations, spaces, and user access.

Bluemix offers wide variety of services that can be easily integrated into our own developed application. Cloud Foundry and other tools that are delivered from IBM and third party, are used to provide these services.

IBM free offers for 30 days as a trail to deploy user-created Java-based application on its Bluemix platform[9], Fig.2 depicted the welcome page of IBM offered Cloud computing Bluemix service. Anyone can easily register using his/her e-mail and get started to use IBM cloud platform-as-a-service(PaaS) freely for a month, Fig. 3 show the single-sign-on login page that required registered email as a IBM id and a password to access the Bluemix numerous services like dashboard, UI and data-store etc.

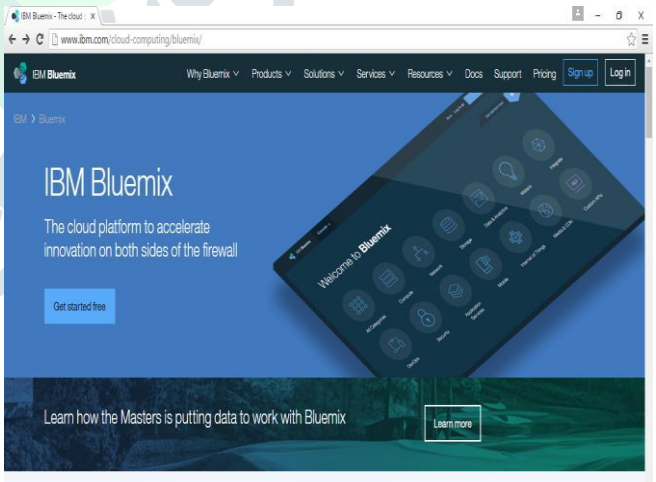

Fig.2: IBM Bluemix Cloud platform welcome page (http://www.ibm.com/cloud-computing/bluemix/).

Developer can easily deploy his own created Java application in the Bluemix user interface using Cloud Foundary services following the documentation steps[10]. Bluemix provide an integrated environment to user-created apps with built-in database support on a single dashboard.

Developer need not to worry about app related services after deployement.

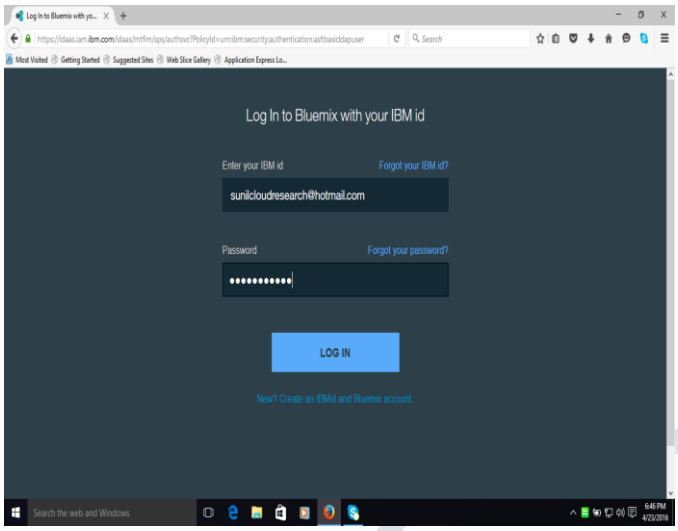

Fig.3: IBM Bluemix Login Panel with IBM Id and password.

Bluemix also facilitate developers to more optimize the time, which they spend in creating cloud application. Developers no longer have to be concerned about installing software or having to deal with virtual machine images or hardware. After few clicks or keystrokes, developers can easily provision instances of their applications with the required services to carry them. Below show the HTML code and snapshot of running page.

```
<!DOCTYPE html>
<html>
<head>
<meta charset="ISO-8859-1">
<title>Welcome in Sunil Encryption Algorithm. </title>
</head>
<body bgcolor="pink">
<h1><font color="blue">Welcome in My Data Security
Encryption Algorithm for Cloud Computing.</font></h1>
<form action="login.jsp" method=post>
Enter some input <input type=text name="inputval">
<input type=submit value="Encrypt">
</form>
<br>
<p>Designed and Developed by:
<hr>
<br><font face="times new roman" size=15
color="blue">Sunil Kumar, Ph.D-Research Scholar
<br>Guided by: Dr. Jayant Shekhar
<br>Swami Vivekanand Subharti University, Meerut,
India</font>
</body>
</html>
```

Fig. 4: Input HTML page of Data security Algorithm

Below given JSP code demonstrate the implementation code of our data security algorithm on IBM Bluemix platform.

```
<%@ page language="java" import="java.util.*;"
contentType="text/html; charset=ISO-8859-1"
   pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd"
>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=ISO-8859-1">
<title>Welcome in Sunil Encryption Algorithm. </title>
</head>
<body bgcolor="pink">
<h1><font color="blue">Welcome in My Data Security
Encryption Algorithm for Cloud Computing.</font></h1>
<%
String
input=request.getParameter("inputval");
String vals[];
char ctr[]=new char[20];
LinkedHashMap ht=new LinkedHashMap();
vals=new String[input.length()];
char[] cArray = input.toCharArray();

ht.put('a',"0"); ht.put('b',"00"); ht.put('c',"01");
ht.put('d',"000");ht.put('e',"001");ht.put('f',"010");
ht.put('g', "011"); ht.put('h',"0000");ht.put('i',
"0001"); ht.put('j',
"0010");ht.put('k',"0011");ht.put('l',"0100");
ht.put('m', "0101");ht.put('n', "0110");
ht.put('o', "0111");ht.put('p', "00000");
ht.put('q', "00001");ht.put('r', "00010");ht.put('s', "00011");
ht.put('t', "00100");ht.put('u', "00101"); ht.put('v',
```

```
"00110"); ht.put('w',"00111"); ht.put('x', "01000");
ht.put('y',"01001"); ht.put('z', "01010");
ht.put('@', "010100"); ht.put('#',"010101");
 {
  vals[i]=ht.get(cArray[i]).toString();
 }
 String bits="111";
 for(int j=0;j<vals.length;j++)
 {
 vals[j]=vals[j]+bits;
 }
 String newval[]=new String[vals.length];
 for(int k=0;k<vals.length;k++)
            newval[k]=vals[k];

 //Place the odd and even position chars in a group
 out.println("<br>Final encrypted text is ");
 for(String s:newval)        out.print(" "+s);
 final long duration = System.nanoTime() - startTime;
 out.println("<br> Execution Time :"+duration/100000+"
 Seconds");
 %>
 </body>
 </html>
```

This JSP code first convert input to encrypted text using our proposed data security algorithm and also calculate the execution time (in seconds).

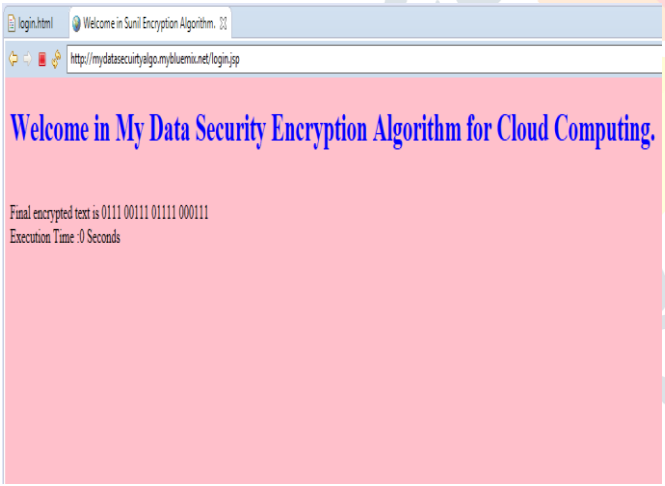

Fig. 5: Output JSP page of Data security Algorithm.

VI. Conclusions and Future works

In the paper, we implemented the data security algorithm on Java platform and deployed on the IBM Bluemix platform to find the time complexity. In future, we will deploy on the Mobile or other cloud platform like Google, Microsoft or Amazon to test its performance and try to make it more efficient.

```
final long startTime = System.nanoTime();
for(int i=0;i<cArray.length;i++)
```

References

[1] Kosie Eloff, "How will cloud computing affect my everyday life", June 5, 2012, ttps://saoug.files.wordpress.com/2012/.../cloudcomputing_kosieeloff.pdf

[2] Bernd Grobauer et al, "Understanding Cloud Computing Vulnerabilities", pp. 50-57, April 2011.

[3] JP Singh, Mamta and S. Kumar, "Authentication and encryption in cloud computing", In Proceedings of 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials(ICSTM), IEEE, 06-08 May,2015, Chennai. pp.216-219, ISBN: 978-1-4-4799-9854-8, DOI: 10.1109/ICSTM.2015.7225417.

[4] S. Kumar, J. Shekhar and JP. Singh, "Data security and encryption technique for cloud storage", In the Proceedings of CSI-2015 50th Golden Jubilee Annual Convention, 02-05 December 15, Springer(in press).

[5] Oracle Corp. Java Technology, 2013, https://www.java.com/en/about/.

[6] Oracle Corp. Oracle Completes Acauisition of Sun, 2010, http://www.oracle.com/us/corporate/press/044428

[7] Oracle Corp. Java Releases, 2015, https://www.java.com/en/download/faq/release_dates.xml

[8] Oracle Corp., What's new in JDK 8 secuirty, 2015, http://www.oracle.com/technetwork/java/javase/8-whats-new-2157071.html

[9] IBM Corp., IBM Bluemix, 2015, http://www.ibm.com/cloud-computing/bluemix/

[10] IBM Corp., Creating Cloud Foundary Apps, 2015 https://console.ng.bluemix.net/docs/cfapps/index.html.