Modeling Implementation of TBDSA-Token based Data Security Algorithm in Cloud Computing

Rimmy Chuchra
Department of Computer Science & Engg.
Sri Sai Institute of Engg and Technology,
Mannawala (Amritsar-Punjab)

R.K Seth
Department of Applied Sciences
Sri Sai University, HP (India)

ABSTRACT
Security during data transmission in cloud computing using TBDSA (Token Based Data Security Algorithm) along with its implementation is presented in this paper. The auto-generated token based certificate activation approach with SSL (Secure Socket Layer) provides the appropriate collaboration between the cloud client and the cloud service provider, so that user may become confident during data transfer by utilizing various cloud applications and services. The chances of attacks may be reduced by implementing this TBDSA. This designed algorithm takes less time to execute and increases the performance of the system.

Keywords
Security algorithm, digital signature, secure socket layer.

1. INTRODUCION
CLOUD stands for "common location independent only utility on demand" [16].It is an umbrella term used for internet based development and services [6]. The functioning of these services depends on deployment and delivery models that help to dynamically deliver a variety of things as a service over the internet based on demand of the consumer as an example network, storage, hardware as well as software [2] .Currently, crimes on internet are increasing and hackers are always ready to find number of different ways to steal information. Therefore the security becomes a mandatory issue [12].There are several types of attacks performed by the attackers on cloud and the most popular attacks are listed below:

- Social Engineering.
- Malware injection.
- XML.
- Signature wrapping.
- Account hijacking.
- Traffic flooding.
- Wireless LAN attack pose: Is a great risk to cloud computing systems [7].

For preventing confidential data from the attackers, the cloud service providers has duty to provide security at separate levels [8] as an example how to provide security on data and files in individual manner that sometimes becomes more difficult [5]. Therefore, they suggest to their customers who are cloud clients to use secure cloud services. The benefit to use such type of secure cloud services is to give secure treatments and calculations for data storage in the database [1]. Generally, whenever any cloud client send request to cloud service provider for accessing specific cloud service, then data will be stored on the cloud server that can be shown as in fig.1:

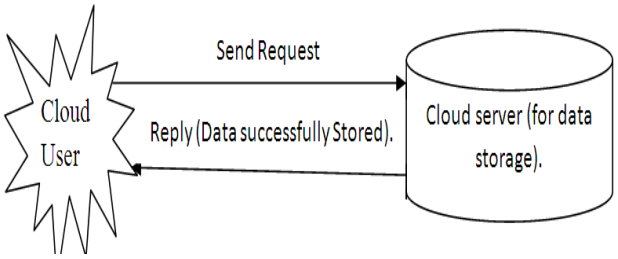

Fig 1: Overview: Data Store on cloud [13].

For analyzing cloud data security in depth, there is a need to study about various different parameters related to data security like data security risk, data security requirements, deployment of security functions and some processes through digital signature etc [9]. Besides there are number of positive and negative impacts of data security as given by cloud service providers where the positive impact is to provide the security of data during transmission and the negative impact is to put data on the server which is also a type of critical risk. Therefore risk management and risk assessment becomes crucial factors for any cloud service provider to handle [10].They also concentrates to provide security at exact location of data, access of data, SLA (Service level Agreement), authentication and authorization. The network and system administrator helps to implement various security policies in different cloud applications [4].There are number of methods that are available for providing security and the most common usable methods are listed below:

- Cryptography is one of the most efficient method for providing data security in cloud computing. It includes the design and implementation of encryption and decryption algorithms. In addition, It also helps to provide encryption at four separate levels which are listed below:
  - Full disk level.
  - Directory Level.
  - File Level.
  - Application Level.[11]
- By providing centralized access of data cloud service provider can improve the security [12].
- Other method is by exchanging session key frequently [14].

Generally, cloud computing has several customers such as ordinary users, academia & enterprises who all have different motivation to move on the cloud [3].This paper discusses about those customers who are actually cloud clients & acts as an academia- that have find a way to combine security and performance. The security issues are directly related with

security architectures at different levels by using different security mechanisms as well as models [15]. There is number of security models available in market, but most of them failed to solve almost all security threads. Some security models provide an efficient way of communication, but these are not cost effective [5].

The TBDSA- is implemented by using the method of digital signature with SSL (Secure Socket Layer). But its working is different from the implementation of digital signature used in our daily life. The implementation of digital signature in MS-Word is shown in Fig.2.

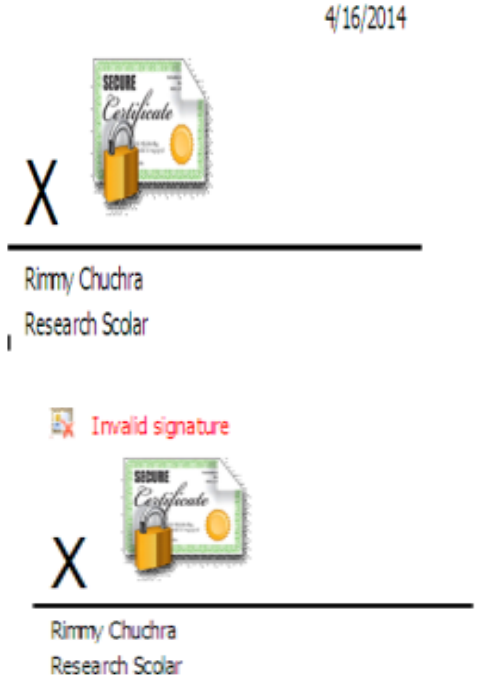

Fig 2: Implementation of valid & invalid Digital Signature: In MS-Word.

The use of digital signature in proposed algorithm is to verify the message intact from the claimed sender and provide security during data transmission so that any intruder or fake client may not be able to interfere till the data is received at other end and the client will become more confident while utilizing such type of cloud services in different applications during data transfer. The designed algorithm is implemented in NETBEANS JAVA Version 7.0 as front-end and DERBY Databases as back-end.

2. LITERATURE REVIEW

Chuchra et *al*., (2012), discussed about the problems occur when cloud client send data from one end to another end. There are number of attacks encountered to provide security from the attackers and that becomes mandatory task for any cloud service provider and also gave a methodology to provide security on the cloud at the client end. Here, cloud client and cloud service provider took a joint action for providing data security. The digital signature with auto-generated token-number by cloud service provider during membership on the cloud is used. The validity of digital signature can be checked as shown in Fig.3 [17].

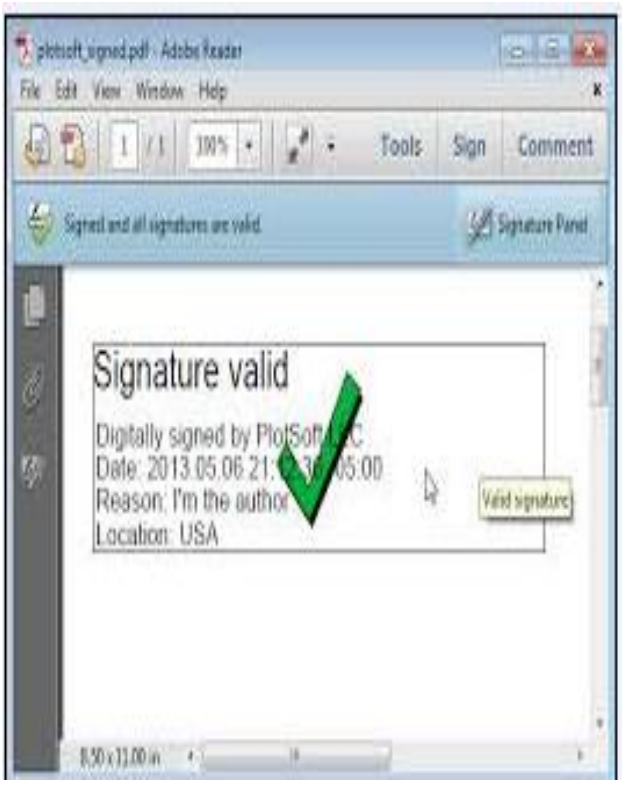

Fig 3: Verification of document by using Digital Signature.

R.K. Seth and R. Chuchra *et al.*,(May-June 2014) had been proposed a new procedure termed as "Token Based Data Security Algorithm" that helps to collaborate the cloud client and cloud service provider to achieve a joint action for providing data security [18].

Table 1.Nomenclature For TBDS Algorithm.

CC	Cloud Client.
CSP	Cloud Service Provider.
CS	Cloud Space.
MEM CON	Membership Confirmed.
T	Time.
TID	Token_ID.
AC	Authenticated User.
IDR	Intruder (Fake Client).
REQ	Request.
ACK	Acknowledgement.
CE	Client End.
CSPE	Cloud service Provider End.
DS	Digital Signature.

3. DESIGNING METHODOLOGY

3.1 Existing Design Procedure

A general client-server communication between the cloud client and cloud service provider is shown in Fig. 4.

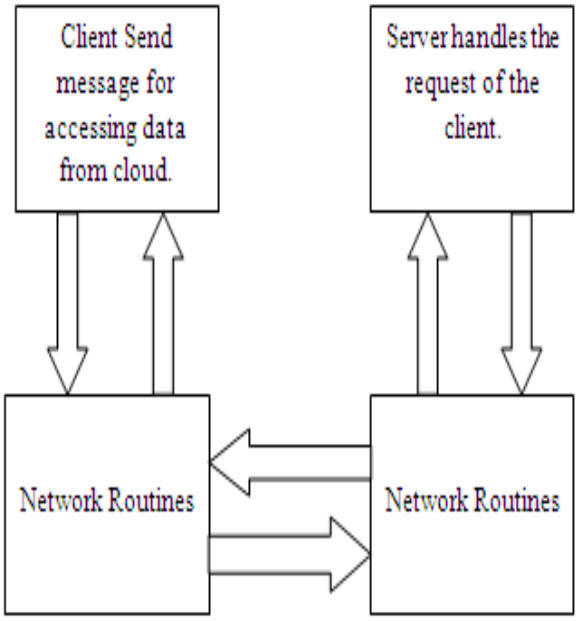

Fig 4: Existing work plan: Shows Communication between CC & CSP.

3.2 Proposed work plan

The proposed work plan shows the use of TBDSA with SSL after certificate activation during client/server communication that can be shown in Fig.5.

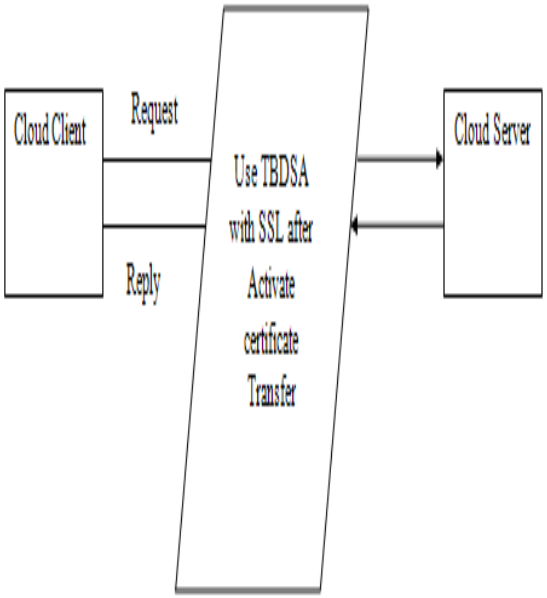

Fig 5: Proposed work plan: Shows Communication between CC & CSP.

4. ROAD MAP FOR DATA SECURITY PROCESS

A Road map for data security process can be shown as in Fig.6.

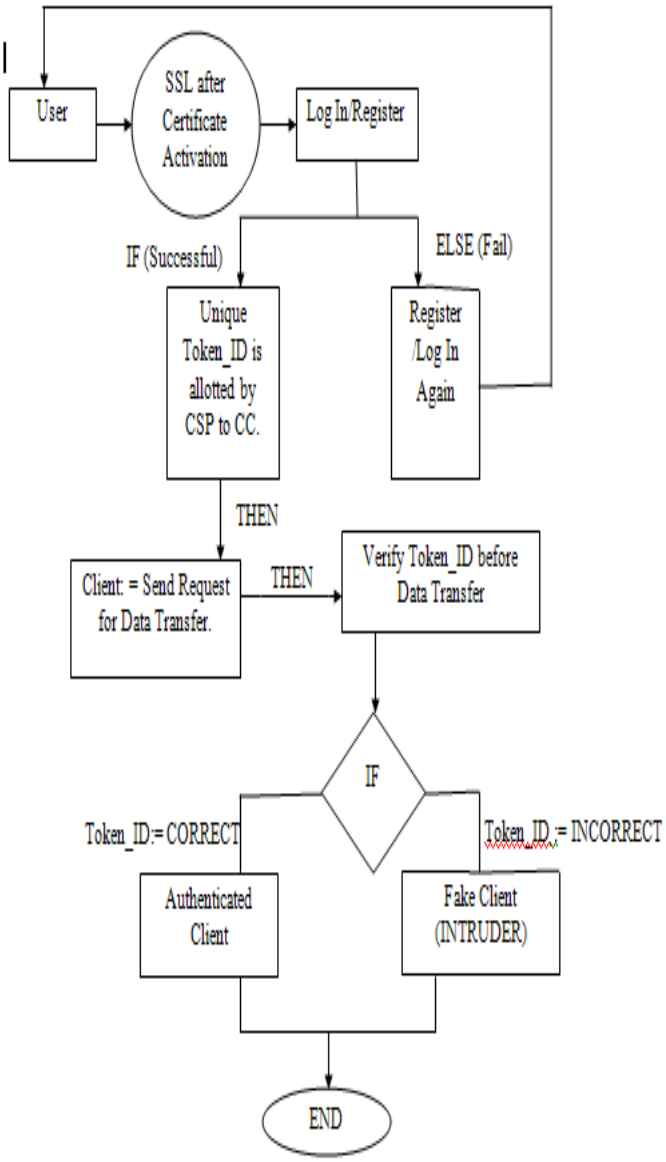

Fig 6: A Roadmap: For Data Security Process.

Software/Hardware Requirements for implementing TBDSA are as follows:

Front-End: NETBEANS JAVA VERSION 7.0.

Back-End: DERBY Databases.

5. DATABASE DESIGN

Table 2: Cloud Client Space Registration.

Column_Name	Data_Type
User_ID	Varchar(20)
PASSWORD(*)	Varchar(20)

Table 3: Cloud Service Provider Details.

Column_Name	Data_Type
Token_ID	Primary Key Int
Type_of_Cloud_Service(Saas,PaaS,IaaS)	Varchar(20)

The steps in the procedure to be followed under TBDSA are given as follows:

Step 1) When CC SEND REQ: = CS, THEN NEW ACCOUNT CREATED & CLIENT REGISTERED.

Step 2) IF MEM: = CON THEN UNIQUE TOKEN_ID is generated on that 'T' FOR SPECIFIC CLOUD SERVICE.

Steps 3) THEN CC SEND REQ: = STRING THEN CHECK FOR THE MARKED/VERIFIED TOKEN_ID with DS.

Step 4) IF (T_ID:= CORRECT)

{

Authenticated Client.

}

ELSE

{

Intruder (Fake Client).

}

Step 5) IFToken_ID does not MATCH with the database entry for specific cloud service that indicated presence of INTRUDER AND REPEATSTEP 1 TO 4.OTHERWISE Data transferred through Secure Channel and RECEIVE ACK. *[9]*.

6. IMPLEMENTATION OF TBDSA IN JAVA

Starting from registration, the allocation of Token ID and its verification has been has been implemented using JAVA and pictures for the same are shown as follows:

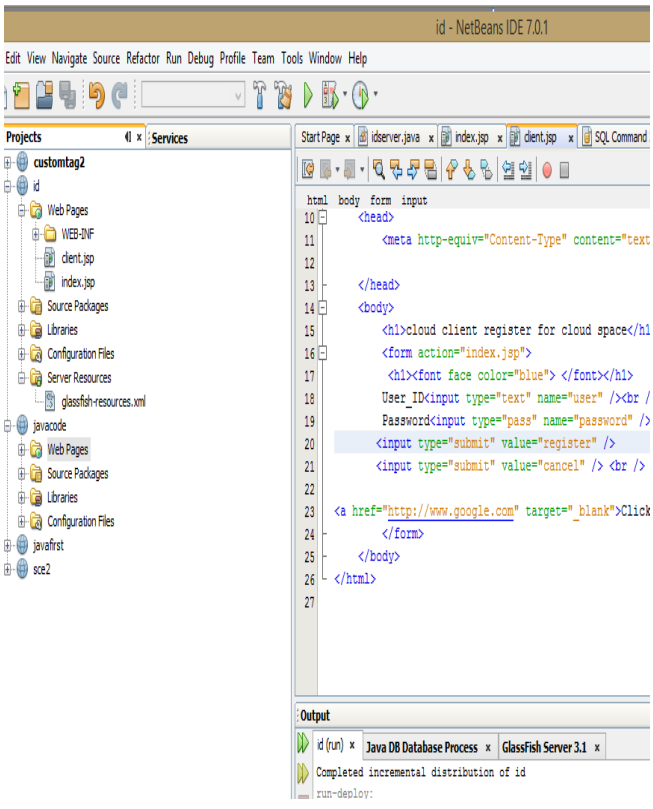

Fig 7: Registration form: For cloud space.

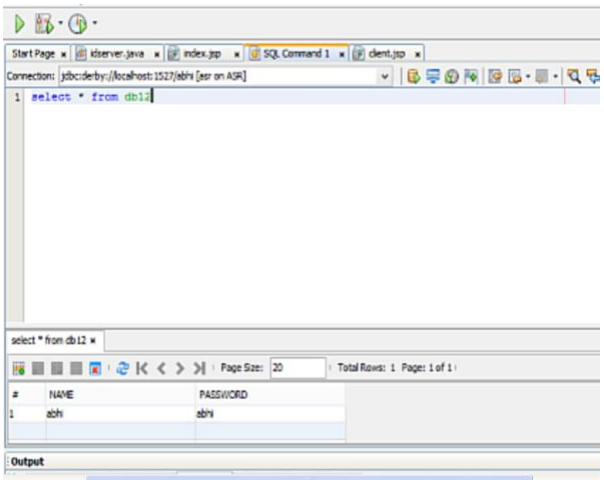

Fig 8: Client details saved successfully in DERBY Databases.

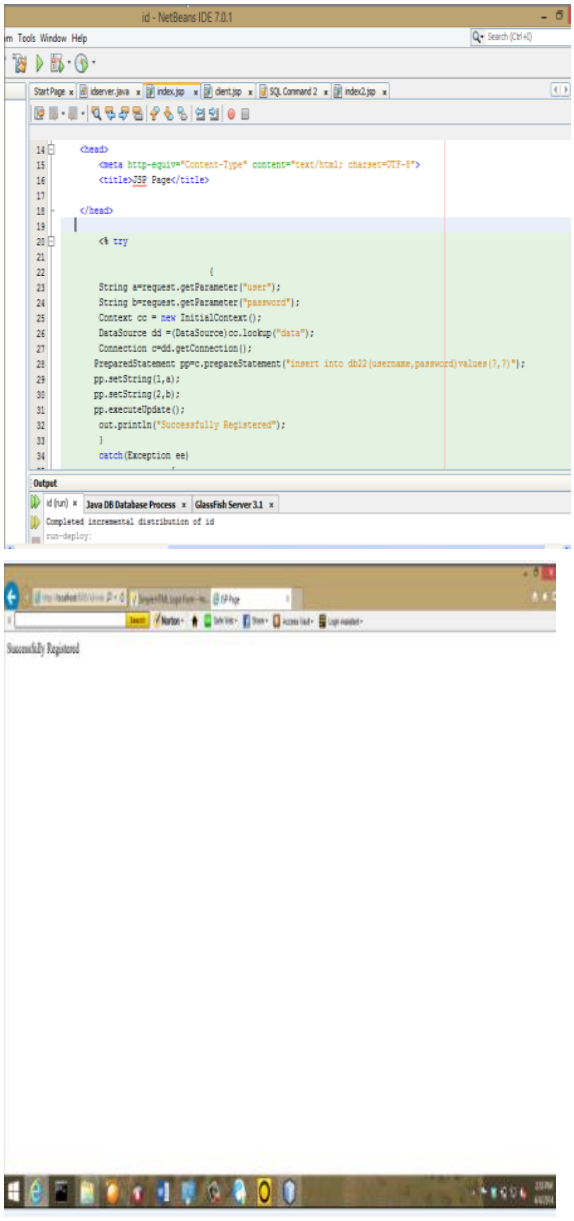

Fig 9: The Client Successfully Register.

Fig 10: After Clicking on CLICK HERE button: Shows Confirmed registration of client.

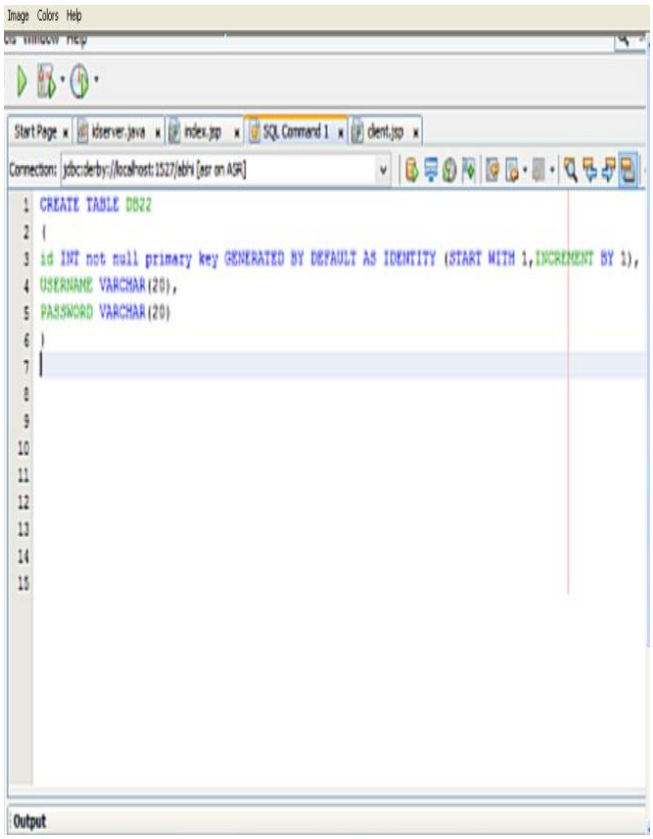

Fig 11: After Confirmation: A unique Token_ID is generated.

Fig 12: Verification of Token_ID and digital signature is marked showing data confidentiality.

7. WORKING

Starting with a request by cloud client to cloud service provider for getting cloud space through registration, the client got registered indicating that the account has been created successfully on the cloud. After confirmation of registration, a unique Token_ID is generated for specific cloud service in the database. In the next step, when cloud client wants to use that specific service in future, then at first the client will enter the already allotted Token_ID by the cloud service provider for specific service and after matching of Token_ID with the pre-generated ID that would

automatically marked the digital signature and will display the access is enabled to the authenticated client otherwise display will show the access is not enabled indicating the client is fake.

8. CONCLUSION

This paper implemented Token Based Data Security Algorithm in NETBEANS JAVA version 7.0 as a frontend and DERBY databases as a backend. The results of this algorithm prove that TBDSA provide a high level security during data transmission. The authorized user (cloud space registered user) can access or exchange data by entering allotted TOKEN_ID by CSP at the time of cloud space registration.

9. FUTURE SCOPE

In future, security during data transmission in cloud computing will be enhanced by designing new algorithms that helps to identify attacker before launching any attack on the network by utilizing WIRESHARK tool. The use of this specific tool is to collect the complete information (say from entering to the leaving in the network) of the attacker from the network by utilizing different network parameters before launching any attack. WIRESHARK facilitates these new designed methodologies for the generation of warning message alerts for the users so that they will try to keep their data safe.

10. REFERENCES

[1] Rashminigoti and Dr. Shailendra singh, 2013. A survey of cryptographic algorithm for cloud computing, International journal of emerging trends and computer application systems.

[2] Leenakhanna and Dr. AmantJaiswal March-2013, Cloud computing: Security issues and description of encryption based algorithm to overcome them, International journal of advanced research in computer science and software engg.

[3] Manpreetkaur and Rajbir Singh May-2013, implementing encryption algorithm to enhance data security in cloud computing, International journal of computer application.

[4] M.Vijayapriya Sept-2013, Security algorithm in cloud computing: Overview, International journal of computer science and emerging technology.

[5] Dr. M.M andA.Hasham 2012.A new user authentication file encryption & distributed server based cloud computing security architecture, International journal of advanced computer science and applications.

[6] T.Sivasakthi and Dr.Prabakarn Feb-2014.Applying digital signature with encryption algorithm of user authentication for data security in cloud computing, International journal of innovative research in computer and communication engg.

[7] Chimerebarron and huimingYu WCE-2013. Cloud computing security case studies and research, proceeding of the world congress on engg,London, U.K.

[8] N.Saravanan andA.Mahendiran 2012.Implementation of RSA algorithm in google cloud using SQL cloud, Research journal of applied sciences, Engg. & technology.

[9] Nehajain and gurpreetkaur 2012.Implementing DES algorithm in cloud for data security, International journal of computer science and information technology.

[10] Sanjoli single and jasmeetsingh 2013.Implementing cloud data security by encryption using rijndaelalgorithm,Global journal of computer science and technology cloud and distributed.

[11] Prakash G.L and Dr.Manishparteek April-2013.Data encryption and decryption algorithm using key rotations for data security in cloud computing, International journal of engg. And computer science.

[12] Kevin Hamle, Murat kantarcioglu, Latifur khan and bhavanithuraisingham April-June-2010. Security issues for cloud computing, International journal of information security and privacy.

[13] Anjanachaudhry and ravinderthakur Dec-2013.A review: Data security approach in cloud computing by using RSA algorithm, International journal of advance research in computer science and management studies.

[14] V.S Rajudue,.N.Prasanthi and A.Jagadeesh Dec-2013.A study of algorithm used to secure data processing in cloud computing, International journal of computer science and technology.

[15] Kashifmunir and Dr. SellapanPalaniappan, April-2013, Framework for cloud computing, International journal on cloud computing: Services and architecture.

[16] P.Shubshri and A.Padmapriya July-2013.Implementation of reverse Caesar cipher algorithm for cloud computing, International journal of computer trends and technology.

[17] RimmyChuchra Oct-2012.Data security in cloud computing, International Journal of societal applications of computer science.

[18] R.K Seth and RimmyChuchra March-April-2014.TBDSA- A new data security algorithm in cloud computing, International journal of computer science and information technology.