ISSN:0975-9646

TBDS- A New Data Security Algorithm in Cloud Computing

R. K. Seth[1] and Rimmy Chuchra[2] and Simran[3]

[1] *Department of Applied Sciences, Sri Sai University, Palampur, Himachal Pradesh (India)*

[2] *Department of Computer Science and Engineering,*
Sri Sai College of Engineering and Technology, Manawala, Amritsar (India)

[3] *Department of Computer Science & Applications*
Kurukshetra University, Kurukshetra-136119

Abstract- Currently many organizations and companies are facing potential threats to their data management systems and these security concerns provide a basis to conduct research in this particular area. In this article, the authors are proposing an algorithm comprising digital signature with auto generated token ID allotted by the cloud service provider during registration of client for verification and authentication of the user. The methodology as described in this article provides data security during transmission so that any intruder/fake client may not be able to interfere till the data is received at the other end. The working of the methodology as designed is also discussed with procedure to be adopted. An appropriate collaboration between Cloud Client (CC) and Cloud Service Provider (CSP) would lead to provide data security in cloud computing so that user may become confident in utilizing cloud applications and services.

Keywords: Data mining, Security algorithm, digital signature.

1. INTRODUCTION

The aim of cloud computing is to reduce cost, access time and complexity of operating computers and networks. The other benefits to use this technology are scalability, efficiency and reliability [7]. This internet based computing helps for sharing of resources, information and software's to other computer devices and for their utilization on user demand [4]. Different types of models in cloud computing deals with a variety of security issues that need to be considered more importantly and the balance of responsibilities between the customer & cloud provider must be maintained for specific service models [5]. There are various types of services that are provided by different types of models which are shown in Table 1 has been incorporated in this part of forthcoming introductory part.

Table 1: Types of cloud services

Type	Consumer	Service Provider	Service Level Coverage
IaaS	Holds middleware and application support	Cloud Storage	Time taken by application coverage.
Paas	Application Owner	Runtime environment with application code	Environment availability and performance.
SaaS	End User(Client)	Finished applications	Application updates.
DaaS	Application Owner or Client	Data Center	Level of service access with shared or private mode.

The data stored in any remote customer location can be transferred to any location in the world [3]. The focus of cloud service provider view as extraneous hardware connected to support downtime on any device in the network, without changing user prospective [6]. The different or same types of services can be provided by different or same type of cloud providers. The selection of cloud service provider is based on the various parameters viz. time span of organization in the field, type of organization and support mechanism, resilience and the capability of organization in interpretation of real life business situation. The location of the data centre, area, and level of power can be taken into consideration. The selection of cloud service based upon above parameters may provide the continual service and that may avoid catastrophic disaster [18]. Even Cloud service providers are more concerned about their security and privacy issues concerning the availability, confidentiality, data integrity, control and audit of the service [2]. Sometimes Cloud Client and Cloud Service Provider both have equal responsibility to provide data security during transmission [10].It requires an effective & flexible dynamic security schemes to ensure the correctness of user data in cloud [1]. Security and confidentiality issues are more important for a critical intensive application in business transactions [8]. This paper discusses different types of data security issues which are discussed below:

Various Issues related with Data Security:

- **Data Integrity:** When data is on cloud then anyone can access from any location. But cloud cannot differentiate between the sensitive data with the normal common data and therefore enabling anyone to access those sensitive data that shows lack of data integrity.
- **Data Theft:** Data may be stolen from the external server by a malicious user.
- **Data Location:** User probably does not know exactly where your data is hosted, and in which country the data has been stored.
- **Data security on cloud Vendor Level:** Cloud Vendor makes sure that server will well secure from the external threads. Cloud may maintain its integrity when a good security would be provided by the vendor to the customers.

- **Data security on Client Level:** Even a security layer already provided by the cloud vendor, the responsibility of the client is to make sure about its own action that there should not be the loss and tampering of the data [9]. The issues related to data security may be visualized as shown in Figure 1.

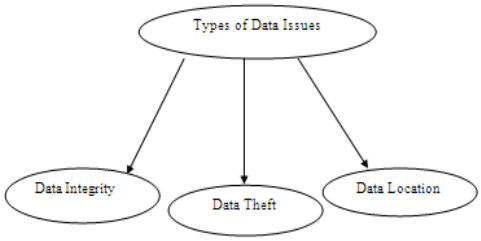

Fig 1: Data Security Issues.

This paper proposes a new algorithmic approach named as ***"TBDS"- Token Based Data Security*** that helps to provide data security during data transmission. A collaboration between cloud client and cloud service provider leads to achieve a joint action for performing data security in cloud computing.

2. DESIGN METHODOLOGY

For providing data security during online data transmission between the cloud client and cloud service provider in suitable manner, this paper proposes a algorithm that helps data will be accessed by the authenticated client without interference of INTRUDER. Figure 2 shows the systematic diagram of communication for performing the tasks on data.

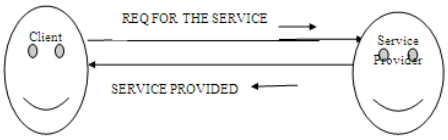

Fig 2: Communication between the CC and CSP.

2.1 Procedure

The Table 2 shows the nomenclature to be used in the paper for TDBS 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.

Table 2: Nomenclature for TBDS Algorithm.

After the nomenclature as tabulated, the steps in the procedure to be followed are as under:

Step 1) When CC SEND REQ: = CS, THEN NEW ACCOUNT CREATED & CLIENT REGISTERED.
Step 2) IF MEM: = CONFIRMED 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) IF Token_ID does not MATCH with the database entry for specific cloud service that indicated presence of INTRUDER AND REPEAT STEP 1 TO 4.OTHERWISE Data transferred through Secure Channel and RECEIVE ACK.

2.2 Working

In first step, when cloud client (CC) will send request for the cloud space from cloud service provider then client must have to register first and create a new account for accessing any service on cloud. After, registration cloud client will move to second step, to confirm his/her own registration. Once registration is confirmed then CC becomes member of cloud and cloud service provider assigned auto-generated Unique Token_ID for future communication. In third step, for future communication when cloud vendor send request for data transfer then it first verifies the assigned token_ID for specific type of cloud service, and if the allotted token_ID will match, then data will be transferred or fetched from one end to another end failing which INTRUDER may enters and the fake client may try to steal your data or access your data due to channel insecurity. The client has to send request once again and then REPEAT STEP 1 to 4.

3. METHODOLOGY FLOWCHART

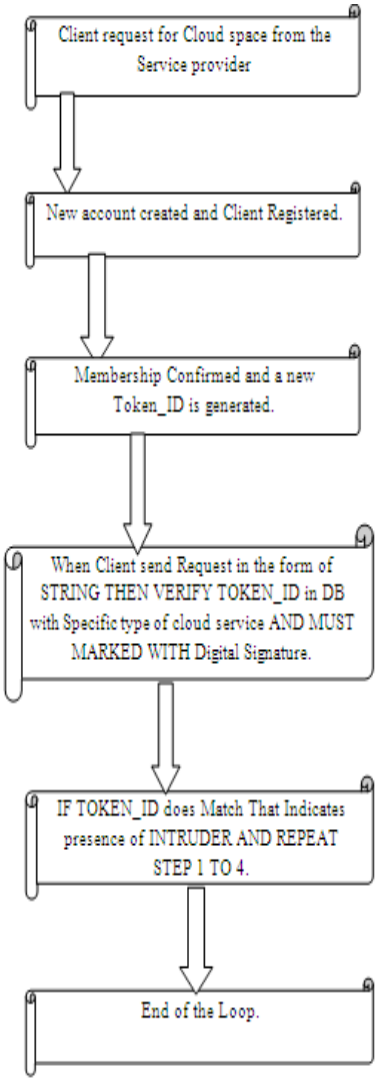

Fig 3: Working of TBDS.

4. SECURITY MEASURES IN CLOUD COMPUTING

The following security measures may be taken in view of the potential threats to the security in cloud computing:

- The cloud consumer privacy bill of rights with private protection is focused on the administration of personnel data and maintain its status of accuracy and its utilization on user demand basis [12]
- Need to design new data centers and sources, devices, services and applications for "THREAD DETECTION" related to outsourcing a top co-operate risk [11].
- Focus to design personal clouds that move gravity centre from application centric to personnel centric models so that users will retake the control over personal data. Wise Key Company launched these personal clouds on 24 February in Barcelona at mobile world congress and provides new Wise Key cloud applications that use online tools to empower the user by providing secure, authenticated, private digital identification & personal data storage on a secure vault on the cloud [15]
- Focus on mechanism based on the operational transparency rather than information technology. So that Internet crime decreases and security increases [13].
- Provide transparency towards data handling techniques by cloud service provider during internet monitoring and cloud service provider must use strong encryption algorithms with strong encryption keys like RC2, RC4, 128-bit RC4, DESX, 128-bit AES, 192-bit AES, and 256-bit AES [14].
- Need to reduce the CTERA-Bridges gap between cloud and the local storage in CTERA network that provide ONLINE CTERA solution portfolio & also manage service provider base in US [17].
- Replace all existing applications with the "CIPHERCLOUD" environment that helps to provide new interaction with cloud based security services & data loss prevention (DLP) environment so cloud service MONITORING will become easy [16].
- Need to design various new key cloud issues related to latency, bandwidth and various security standards [18].
- Challenge towards new designed methodologies based on data leakage, cloud credentials, snooping, key management and performance efficiency [19].
- Need to design a new procedure to secure dormant virtual machines in offline mode still available to any application that can access the virtual machine storage over the network & therefore susceptible to malware infection [20].

5. CONCLUSION

In view of the security issues in cloud computing and taking into account its significant concern in the data management systems along with its mobilization around the globe, an algorithm has been designed to protect the user does data comprise important information. The proposed methodology provides security by generating a comprehensive mechanism of digital signature with auto-generated TOKEN_ID for specific cloud service that may make the world of cloud computing more secure, reliable and admirable. The implementation of the procedure may reduce the security threats by limiting the access to original confidential data by authenticated client.

REFERENCES

[1]iaesjournal.com/online/index.php/IJCLOSER/article/view/Bharatividya peeth, % 20india.
[2] dl.acm.org/citation.cfm?id=1919665-2.
[3] www.csjournals.com/IJITKM/PDF-2/3-Sunita-Rani.pdf.
[4]libra.msra.Cn/Publication/51004520/Cloud-Computing-research-and-security-issues.
[5] Social.technetmicrosoft.Com/Wiki/Contents/articles13801.Cloud-Security-introduction.aspx.
[6]http://www.ijaiem.org/volume1Issue2/IJAIEM-2012-11-3-076.pdf.
[7]http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf.
[8]http://www.ojs.excelingtech.co.uk/index.php/IJCSET/article/viewFile/239/137.
[9]http://www.slideshare.net/ronak2454/issues-in-cloud-computing-9710875.
[10]www.iosjournals.org/iosr-Jce/Papers/Vol9-Issue1/D0911825.Pdf.
[11]www.computerweekly.com/opinion/security-Think-Tank-New-data-Source-are-2014-security-challange.
[12]www.theguardian.com/media-network/media-network-blog/2013/dec/16/data-Protection-cloud-computing-2014.

[13]www.oracle.com/US/Products/applications/10-questions-for-cloud-vendors-1639601.pdf.
[14] insights.wired.com/profiles blogs/what-will-2014-hold-for-cloud-data- security#aXZZ2Usk1ZguY.
[15] genevalaunch.Com/2014/02/25/2014-the-year-of-personal-cloud-security/.
[16]www.theregister.co.UK/2014/02/26/Ciphercloud-Launches/-.
[17]www.crn.com.au/News/373423,trackitonline-introduces-new-cloud-storage-solution-to-australia.aspx.
[18] Cloud computing intelligence.Com/index.php/resource-centre/articles /featured-articles/966-Predicting-the-cloud-in-2014.
[19]www.nasuni.Com/news/press-releases/26-top-5-security-challanges-of-cloud-storage.
[20] iosrjounals.org/iosr-Jce/papers/ICAET-2014/volume-5/7.pdf?id-7557.