International Journal of Future Generation Communication and Networking
Vol. 11, No. 1 (2018), pp.23-36

Secured Identity Management System for Preserving Data Privacy and Transmission in Cloud Computing

Garima Rastogi[1*] and Rama Sushil[2]

[1*]*Computer Science and Engineering Department, DIT University, Dehradun INDIA*
[2]*Department of Information Technology, DIT University, Dehradun INDIA*
garimaverma.research@gmail.com
ramasushil@yahoo.co.in

Abstract

In this era of globalization, cloud computing is being preferred for management and maintenance of data and services across sectors such as health, banking, manufacturing, national security services etc. Therefore, it becomes extremely important to make ample provision for data confidentiality and privacy. In short, data security is a very important issue which needs to be addressed properly to enhance the usage of cloud computing. In this manuscript, some vulnerability issues have been identified in the conventional identity management (IDM) systems that are used currently. This paper proposes a novel identity management system for secure data transmission and preserving data privacy in cloud environment called (SIDM). The proposed system will overcomes issues such as network traffic interception, IDM compromise and replay attack. In comparison to general IDM, the proposed scheme has some additional features like human intervention procedures, different token distribution method, homomorphic encryption etc. to enhance the security and solve the mentioned issues. To confirm the same, an experiment has been conducted to evaluate the performance and security measures of proposed scheme.

Keywords: *Vulnerability, Security, Confidentiality, Identity management system*

1. Introduction

Cloud computing has been defined by five essential characteristics given by the National Institute of Standard and Technology (NIST), elasticity, a large pool of resources, broad network access, self-service and measured services [1]. The main features which attract and drive adoption of cloud computing are a small cost of initial investment, low maintenance cost, independence of location and resource allocation and de-allocation according to the dynamic change in needs. Cloud computing provides an environment to store data and information of various clients. It provides an environment for remote data management, *i.e.* the data are maintained by third parties which challenge security concern. The data servers which are available on a cloud can also be prone to the attacks [2, 3, 4]. Therefore, it is important that only authorized users access the services of the cloud. For this, there is a need to maintain the access control system so that only authorized user can have the access towards the services of the cloud. Access controlling is gaining importance day-by-day in social networking applications where users store and share their personal and professional information, pictures, video *etc*. It is not only enough to store information securely but also making sure that it is accessed by valid and authorized users only. It is a responsibility of cloud system that information stored in the cloud is secure, *i.e.* it is stored in such a way that it cannot be hacked easily [4]. All these preferences are generally managed by a chosen cloud identity management system which

Received (October 21, 2017), Review Result (December 19, 2017), Accepted (December 22, 2017)

ISSN: 2233-7857 IJFGCN

authorizes and authenticates a user for accessing the services on the cloud. However, most of the current identity management systems (IDMs) that are being used suffer from potential vulnerabilities such as network traffic interception, IDM compromise *etc*. [5]. Through various research, it is identified that it very easy to access data if a hacker can attack any of the entity used in the cloud management *i.e.* IDM server, CSP server or any communication link. It is important whenever any IDM scheme is designed the researcher should give the focus on these issues. Although we cannot claim for complete security with no loop holes we can enhance the security layers so that the hacker should have difficulty in hacking any system or link. To address the above issues, in this manuscript, a secured identity management system (SIDM) for preserving data privacy for cloud environment is proposed. The proposed methodology of secure IDM also evaluates the scheme for IDM attack, network traffic interception and overall performance on the basis of time and security.

The road map of this paper is as follows. Section 2 pinpoints about the related works. Section 3 provides the general cloud identity management (IDM) system and also elaborates the weaknesses of the general IDM system. Section 4 illustrates secure identity management system for preserving data privacy in cloud environment. Section 5 presents the measures used in proposed SIDM. Section 6 presents the experimental analysis followed by the Discussion in section 7 and conclusion of work as Section 8.

2. Related Work

Practitioners and researchers have designed and implemented various flavors of Identity Management Systems (IDMs) to provide security and privacy. In the work [6] the authors proposed a new scheme for secure IDM for secure mobile computing. They identified that if an attacker can compromise the communication between IDM and mobile client the whole system will become vulnerable.

The OAuth is a widely used IDM scheme for cloud computing. In OAuth the client gets a token from the authorization server, which is valid for a limited time and limited scope, to access the resource from resource owner that is handled by the resource server. After proper validation of a token by resource server, resource owner grants the access of requested resource to the client [7]. The authors also identified some attacks which are possible on OAuth such as server trust, poor session management, and timing attack. It can create problems if the communication channel of resource owner is compromised or the resource server itself is compromised. In the study [8] authors have explored that OAuth also grants access to resources to a third party on the behalf of the resource owner by using a system like OpenId. This facility is also called as single sign-on. Through literature, it has been identified that OpenId has many weaknesses and vulnerabilities. If any how an attacker succeeds to inject malicious code inside a server, then by using OpenId he can forward the client to a vague authentication page and ask for identity. Authors also emphasized that the security mechanisms provided by current IDM are not sufficient because if a hacker is able to hack credentials somehow, the whole data on a cloud can be at stake [6, 7, 8].

In [4], the authors proposed the use of IDM without using the third party; it is able to provide good authorization but fails in proper authentication. In [9], the authors have done some analysis on various recent data security models. They also proposed cloud data security model based on business modeling notations. In [10], authors raised about stealing of digital data by the name of the third party. They also proposed a privacy preserving model to prevent the loss of digital data.

In [11], authors proposed a decentralized approach for IDM in which a group algorithm is used for deployment. The algorithm provided for authentication using single sign-on (SSO) is used by a group of services which are divided according to the type of relationship.

3. Preliminaries

3.1. Cloud Identity Management System

Despite many advantages of cloud, the rate of migration towards cloud is rather slow because of the security issues integrated with the technology. One of the issues which are gaining focus nowadays is identity management. It is required that cloud services are accessed by authorized users only. For that, cloud identity management systems (IDMs) are required to maintain updated information without any kind of conflicts caused by the dormant users [5, 12]. The main purpose of IDM system is to manage and store the important credentials of cloud service providers (CSPs) for authentication and authorizations. The life cycle of IDM is shown in Figure 1.

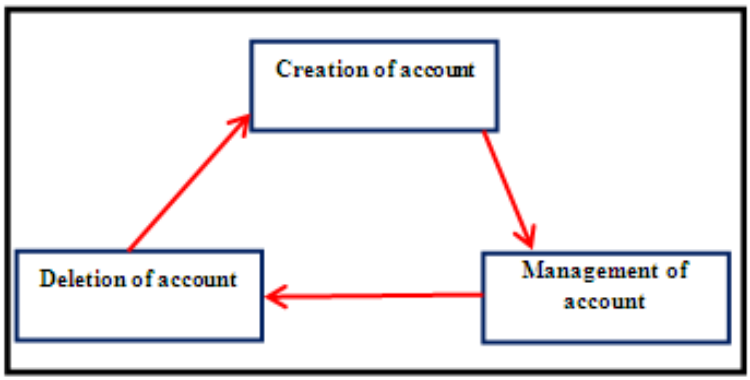

Figure 1. Life Cycle of IDM

IDM maintains the integrity of identities all over its life cycle to make related information updated and authenticated thus making it available for various services in a secure and protected manner [9, 13, 14]. IDMs can use one identification information for various organizations to access all different services within a trusted group of organizations across geographical borders. This IDM feature is called as a federation of identity. A general structure of IDM system in shown in Figure 2 which has CSP, IDM provider, and client/user.

As depicted in Figure 2, if the client tries to access the services of CSP, it asks for an access token. To get that token client needs to contact IDM, which verifies the identity of the client and if found valid, it generates the token and sends it to user and CSP simultaneously [6, 7]. When a client sends token to CSP, the CSP verifies it with token received from IDM. If both tokens are matched then CSP allows access of requested resource to the client.

3.2. Bottlenecks in Conventional IDM

There are various weaknesses identified in the current IDM system. First, vulnerability is possible if the cloud services are accessed by portable devices like mobile, laptop, palmtop *etc*. In case if the device theft or compromised by malicious code then it becomes a very severe threat. Any attacker can hack data or information from the device. Various practitioners and researchers have given different techniques to breach the security of mobile devices. In Georgia Tech cyber security summit 2014, practitioners showed how the malicious USB charger can be used to hack or infect Apple devices also they have shown the malicious app can be stored in the app store and whenever any user will install it the device will become vulnerable [15, 16]. In the 2015 summit, it is reported that mobile devices have enhanced the tendency through which more companies have access to detailed user data through the installation of apps on smart phones. The average

number of installed apps on Android smart phones, for example, has increased by approximate 57 percent over the past three years. Yet, less than approximate 45 percent of those apps are typically used on a monthly basis [17]. These apps are available with some offers like free recharge, trip offer *etc*. Some researchers briefed about the application installation procedure on Android and said that android system does not install any application on a device that is not signed. Further, they have shown the whole procedure, how the attacks can be done by inserting malicious code into the application without modifying its signature. Also, they have given some precautionary measures to save device from attacks. All the users now a day uses internet browsing, exchanging email, chatting, even virtual work environment all the time [6, 18]. If any time any user leave a virtual port open it can create serious issues. These virtual ports can be very easily accessed by hackers.

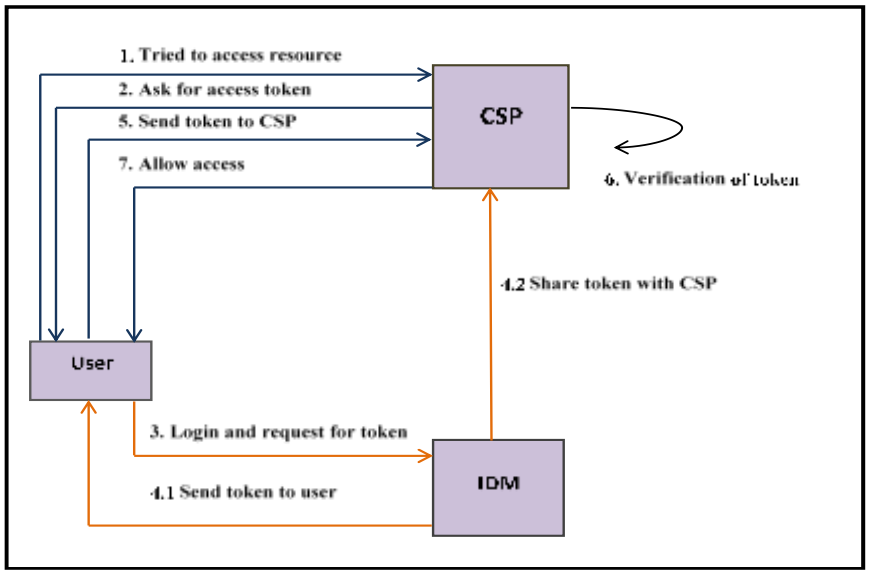

Figure 2. General Structure of Conventional IDM

The second vulnerability is possible if the IDM server gets compromised. Although it is very difficult to access IDM server because of physical and logical security around the IDM server like activity monitoring, audit logs, firewalls, *etc*. but an IDM server can be compromised despite all the measures. The recent attack is reported in 2013, in which hacker intruded Adobe's network and stolen approximate 38 million customer details [18]. In 2014 yahoo has also disclosed that 500 million users account were stolen.

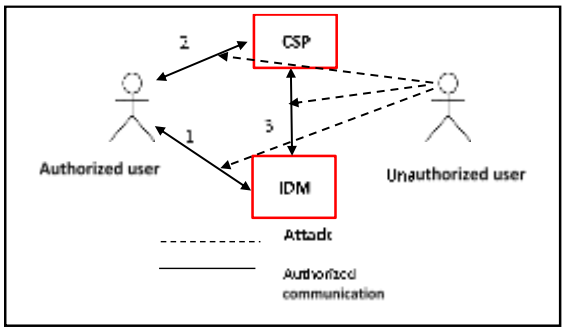

Figure 3. Possibility of Communication Path Compromise in Conventional IDM

Another vulnerability, which is possible, is hacking messages while IDM is communicating with the user or CSP while establishing trust management or information transfer. If any how an attacker can hack traffic between users and IDM, he can get the credentials of the user and he can gain access to IDM server and cloud services [19, 20, 21]. Although it is not possible to save all the communication paths every time, yes, we can increase the difficulty level for attacker which can reduce the possibilities of attacks. In Figure 3, possible attacks that happen in the conventional IDM on communication path are shown. If there is an attack on path 1 the attacker can easily grab token sent by IDM to the user. Similarly, on path 2 and 3, the token can be acquired while it is being sent from IDM to CSP or user to CSP.

4. Proposed SIDM System for Preserving Data Privacy and Transmission

In this section, the proposed methodology of secure IDM is illustrated. To make the security concern more appropriate the below-mentioned functionalities have been considered. Assumptions - IDM server has all the user login and passwords in the encrypted form [22, 23]. The user will use user login in plain text, but IDM will match it through stored encrypted login.

1. The client generates a key (symmetric) K and C by encrypting ID of the user, ID of CSP and random nonce using K.
2. After login to IDM, the user sends Cuser=E(C, K) to IDM and request for access token for CSP.
3. The IDM after decryption of Cuser verifies the user and generates random token and Cidm by encrypting C and token using the private key of IDM and sends Cidm to the respective CSP.
4. User will encrypt C by using KPub (public key of CSP) for generating Ccsp and send it to CSP for granting permission of requested resources.
5. The CSP has now Cidm and Ccsp and it will decrypt both. After decryption of Cidm the CSP will get C and access token. From decryption of Ccsp only C will be generated. The CSP server will compare both values of C. If both have same information then it grants access to the user.

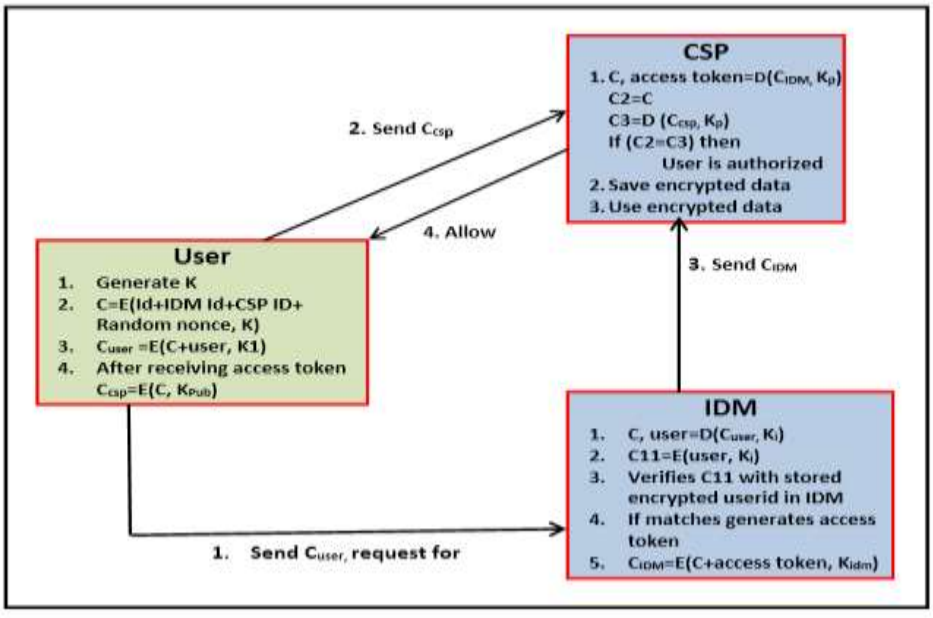

Figure 4. Flow Chart of SIDM

As depicted in Figure 4, a flow chart of the SIDM, the algorithm proposes some human interventions of extra security for dealing with the loss or compromise of the device in case of mobile, laptop *etc*. The proposed pseudo code for each module is shown below.

Algorithm$_1$: **(For User)**

Generate_Csp(userid, password)
  Generate K
  C=Enc (id+IDM id+CSP id+random nonce, K)
  C_{user} = Enc (C, K)
  T=AccesstokenIDM(C_{user})
  Ccsp = Enc(C+T, Kpub)
  Per=GrantCSP(Ccsp)
  If *Per=true then*
    Resource can be accessed
  Else
    Resources cannot be accessed
  End
End

Algorithm$_2$: **(For IDM)**

AccesstokenIDM(C_{user})
  C, userid=Dec(C_{user}, K)
  C11=Enc (userid, K_{idm})
  If *EncIDM(userid)=C11* ***then***
    Generate T
    C_{IDM}=Enc(C+T, K_{idm})
    GrantCSP(C_{IDM})
  End
End

Algorithm$_3$: (**For CSP)**

GrantCSP(C_{IDM})
  C, T=Dec(C_{IDM}, Kp)
  C2=C
  C3=Dec(C_{csp}, Kp)
  If *C2=C3* ***then***
    Return true
  Else
    Return false
  End
End

The main reason for adding human intervention is that most of the time users prefer to store ID and password locally on the device or cookies or in applications itself. To verify this, a survey has been conducted from different places and different type of users such as students, teachers, office executives, and doctors. Figure 5 shows the results of a survey which says that more than 45% percent of students and 65 % office executives, store passwords in cookies while approximate 53% teachers store the password in applications and 35% doctors preferred to save the password in a text file. Anytime, if the device is lost hacker can have access to all stored ID and passwords and use them for their own benefit. For minimizing these kinds of incidents, the algorithm has some more verification apart from Ccsp by asking some personal information from the user like date of birth, anniversary date, subjects of graduation, the percentage of 10th, first pet name, *etc*. This

verification is termed as security questions. The number of attempts to answer the questions is only two after that the user-declared as unauthorized and again he needs to take grant for an access token from SIDM server. This idea has been implemented by various applications like most of the banking services have this facility of human intervention.

The proposed algorithm saves from the hacking of information if the IDM server is compromised. In a general IDM case, if the IDM server is compromised the hacker will get the token and can send it to CSP on behalf of the legal user. The CSP will verify the token and grant the access of resources. But, in case of SIDM the algorithm, can reject granting of resources. There are various reasons for the same such as the algorithm is saving all the user and password information in encrypted form. Therefore, it will not be easy to access them easily. The algorithm is sending Ccsp from a user and Cidm from IDM server. When both values are founded by the CSP then only it starts verification and if matched it declares a user as authorized and grants permission to access resources. Through this algorithm created some more difficulty level for the attacker because now the access to CSP depends on more than one conditions. The CSP is accessible after getting two information which is related but coming from two different places. As well as after verification of Ccsp and Cidm the CSP server will ask for some security questions. SIDM is shown in Figure 6.

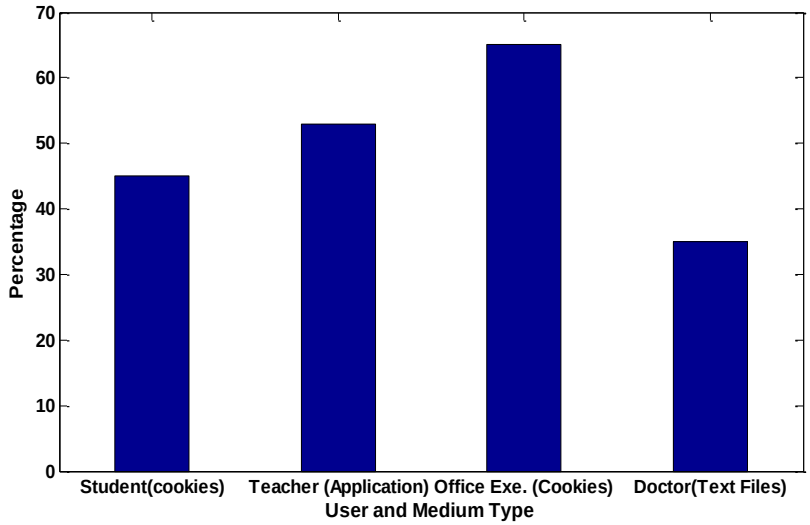

Figure 5. Plot of Percentage between User and Medium Type vs. Percentage

Now if the hacker tries to hack data while transferring from any of the links, then he will also find it difficult because the algorithm is transferring data from one place to another only in encrypted form whether it is user-id, password, token or any message. The random nonce that is added to C will protect from a replay attack. Also, the CSP will give access to resources only if it finds two values *i.e.* Ccsp and Cidm. Further, if the hacker tries to compromise CSP then it will also be difficult for him because according to the algorithm the CSP save and use all kinds of data only in encrypted form.

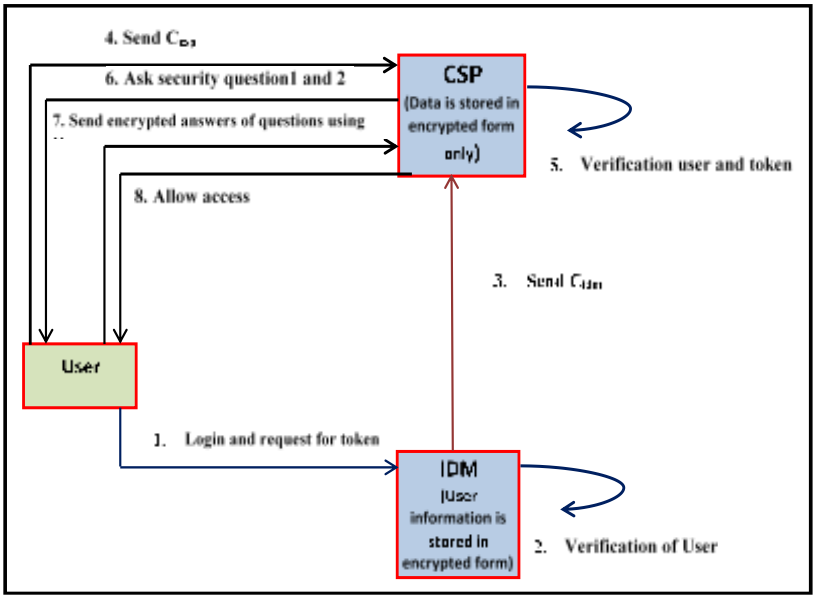

Figure 6. Secure IDM System (SIDM) with Security Questions

5. Measures Used in SIDM

5.1. Stolen or Device Compromised

When a cloud client stores its useful credentials in a device in the form of text file or cookies or any other form, the unauthorized user can easily hack the credentials by compromising it using malicious code insertion or by stealing it. After accessing the credentials, the unauthorized user can very easily communicate with IDM server and access the token in conventional IDM system. To overcome this vulnerability, SIDM involves human intervention before access is granted in CSP.

5.2. IDM Server Compromised

When IDM server is compromised by inserting malicious code or illegal access, the unauthorized user can access the credentials of all users and token information. By using the information, unauthorized user can use the services of CSP. To check this problem, SIDM has following measures:-

- Separation of information –The token is divided into two parts of information. One part is provided by SIDM server to CSP and other part is generated and provided by the user.
- The credentials in SIDM server related to user and CSP are stored in the form of encrypted data.

5.3. Network Traffic Interception

While transferring credentials for verification, if an unauthorized user is able to interrupt the communication between two parties *i.e.* between IDM server and use or user and CSP server or IDM server and CSP server, then intruder can access the token or credential information and get the unauthorized access of services from CSP. To overcome this, SIDM has following measures-

- CSP server stores all data in encrypted form and all the operations are performed on encrypted data only by using partial homomorphic algorithm RSA. RSA can be used as multiplicative homomorphic encryption due to its multiplicative property.

$$\text{Encrypt}(P1 \otimes P2) = \text{Encrypt}(P1) \otimes \text{Encrypt}(P2) \quad (1)$$

5.4. RSA Algorithm as Multiplication Homomorphic Encryption

Begin
1. Select p and q large prime numbers
2. n= p * q
3. phi(n)= (p-1) * (q-1)
4. select e where 1<e<phi(n) and e,n are co-primes
5. (d * e) mod (phi(n)) =1
6. public key (e,n), private key (d,n)
7. C=P mod(n)
8. P=C mod(n)
9. encrypt (P1) * encrypt(P2) =encrypt(P1 x P2)

End

- The data which is transmitting on any channel is encrypted.
- Human interventions in the form of security questions.

6. Experimental Work

To verify all the discussed security capabilities of SIDM, three experiments have been conducted. A symmetric key is used for generating data encryption algorithm (DES) and for RSA, asymmetric encryption, is used. RSA is also used for homomorphic encryption in CSP. The results of the experiments are shown in Table 1. The mode of experiment contains three parts: device is stolen or compromised, malicious code is inserted in the IDM server and SIDM server and CSP is compromised. For conducting experiment, java language has been used and database has been maintained using oracle server. The system has been then tested for attacks from laptop as well as mobile phone clients. Two virtual hosts were deployed on Amazon EC2 with the specification - 12 GB RAM 2TB hard disk. One host has been used for CSP as storage server and whereas other has been used for IDM/SIDM.

6.1. Experiment 1: User Device is Compromised Or Stolen

In this experiment, a user stores all credentials in a device as a text file or cookies. One CSP is implemented from where the authorized user could access the list using a workstation. In this experiment, CSP uses IDM to authenticate the client. For checking conventional IDM and SIDM, two servers have been deployed. In normal conditions, when an authorized user accesses IDM servers (Conventional IDM and SIDM) without any compromise, the algorithm works perfectly to authenticate the user. In the next phase of the experiment, information stored in text files were accessed by an unauthorized user from a device. In case of IDM, the adversary may get the credential information of the user (user id and password). With this, an unauthorized user/an adversary can easily communicate with CSP. To verify this, IDM generates a single token which is not that much secure. However, in the case of the proposed SIDM, CSP requires Ccsp and two-way randomly generated security questions to be verified. Two attempts are allowed for a single user. When the user fails to give the correct answer in two attempts, the CSP declares the user as unauthorized and blocks the access from CSP. This experiment

clearly shows that SIDM is better in comparison to conventional IDM if the device is compromised.

6.2. Experiment 2: Malicious Code is Inserted

In this experiment, malicious code is inserted in the conventional IDM server and SIDM server. Since CSP only requires access token in case of general IDM, so the adversary/hacker is able to identify the token and ID of the IDM server. Further, the unauthorized user can use the same to access services of CSP acting as a legal user whereas. But in the case of SIDM, the CSP requires Ccsp, which is generated by Kpub and access token [26]. Anyhow, if the attacker is able to get Kpub and generate Ccsp, in this case, he/she also needs to give answers to two random questions. Therefore, it is not easy to get the access on SIDM because of the increased security walls.

6.3. Experiment 3: CSP is Compromised and Communication Path Interception

In this experiment, CSP is compromised. Once the attacker tries to access the data he/she gets encrypted data on CSP server, because in SIDM, the data in CSP is stored in the encrypted form. The RSA was used as a partial homomorphic algorithm to perform even operations on encrypted data, *i.e.* no decryption is required for performing operations on data [23, 24, 25].

In the next phase of this experiment, the attacker intercepts all the communication paths one by one. In case of conventional IDM, the attacker is able to access the token from any of the paths as the token was communicated on path 1 from IDM to the user, on path 2 users to the CSP and on path 3 from IDM to the CSP. Therefore, the unauthorized user uses the access on CSP once if he/she gets the token.

In SIDM, when the attacker hacks path 2, he gets Ccsp which contains C and T. Still he/she cannot access CSP because CSP needs CIDM to verify the user. When the attacker hacks path 3 gets CIDM, then he/she is not able to compromise CSP due to security questions which are not easy to answer till the time hacker knows the user very closely. Therefore, SIDM performs better in comparison to conventional IDM.

Table 1. Experimental Result of Different Algorithms

Algorithm	Success Device Stolen or Hacked	Success if Identity server compromised	Success if CSP server compromised
IDM	Yes	Yes	Yes
SIMD	No	No	No

6.4. Analysis of Communication Overhead

The communication overhead is the time when the system is busy to transfer data from one place to another instead of doing productive work. The communication overhead, while establishing the trust between the user, IDM and CSP, is the number of data bytes required for transferring. An experiment has been conducted to compare both the algorithms. For symmetric encryption, the DES algorithm is used. For asymmetric encryption, homomorphic encryption and RSA is used. The overhead in terms of communication is calculated with the below-mentioned parameters. Minimum packet size 40, user id and password (20 bytes), token size (44), a request to CSP (40), size of C (encrypted value) is 16.

1. According to the conventional IDM shown in Figure 2, the number of communications required between users and IDM are two, one for requesting token

and log in, other for granting access token. While in case of SIDM it is only one *i.e.* sending a request for token and login information to IDM server.

2. The number of communications required between IDM server and CSP in both cases is only one.
3. In case of general IDM, the number of communications between the CSP and user is four while in case of SIDM it is only two as shown in Figure 2 and Figure 4.

Table 2. Data Bytes Transfer at Each Link in Conventional IDM

Links	send	receive	Total
Path-1 (User and IDM) bytes	60	44	104
Path-2 (IDM and CSP) bytes	84	-	84
Path-3 (User and CSP) bytes	84	40	124

Table 3. Data Bytes Transfer at Each Link in Proposed SIDM

Links	send	receive	Total
Path-1 (User and IDM) bytes	56	44	100
Path-2 (IDM and CSP) bytes	56	-	56
Path-3 (User and CSP) bytes	56	40	96

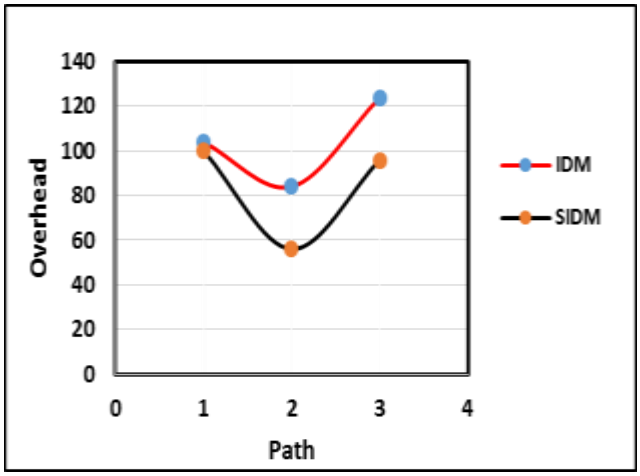

Figure 7. Comparison between General IDM Schemes and Total Overhead

Therefore, it can be seen from Table 2, 3, and Figure 7, that in case of general IDM, communication overhead is more in comparison to SIMD while trust management.

7. Discussion

In a study [26], authors have proposed an algorithm for privacy preserving Identity as a service (IDaaS). The main objective of this approach was to provide IDM without having access to user's information. But the algorithm is not able to protect data from malicious attacks. In [27], authors proposed an algorithm for privacy preserving identity and access management in Cloud called as PRIAM. The main purpose of the scheme is to maintain privacy and secure authentication. Keeping the above constraints, in this manuscript, we developed a novel scheme for enhancing security while data transmission in cloud environment. On the basis of literature, the current research evaluates some existing cloud IDMs to perform a comparative analysis. The purpose of the comparative analysis is to help cloud service centers and users to select most appropriate cloud IDMs according to

their requirements. Table 4 shows the detailed analysis of some cloud IDMs proposed by different researchers. The analysis table contains the reference of the scheme, type of the IDM, attacks which can be prevented by the proposed IDM and best practice used by the scheme for security.

Table 4. Analysis of some IDMs

Attacks Prevention	**[11]**	**[26]**	**[27]**	**SIDM**
Identity attack	**Yes**		**Yes**	**Yes**
Side channel attack	-	**Yes**	-	-
Man in middle attack	-	-	-	-
Malicious attack	-	**Yes**	-	**Yes**
Denial of service attack	-		-	-
Replay attack	-		-	**Yes**
Best Practices Used				
History Log	**Yes**	-	-	-
Single Sign on	**Yes**	-	-	-
SAML	-	**Yes**	-	-
Proxy	-	**Yes**	-	-
Blind signature chain	-		**Yes**	-
Encryption	**Yes**	**Yes**	-	**Yes**
Audit Log	-	-	-	**Yes**
Human Interventions	-	-	-	**Yes**
Homomorphic Encryption	-	-	-	**Yes**

As it is shown in Table 4, our proposed SIMD is able to handle more number of attacks and hence is a better alternative to existing IDMs being used.

8. Conclusion and Future Scope

IDM is a kind of authentication system which works on the behalf of service providers on the cloud to verify credentials of users who wants to access the resources of the cloud. The current IDM systems suffer from many security issues. In this paper, some vulnerabilities (device compromised, IDM compromised *etc.*) that are possible in a conventional IDM system have been identified. A secured IDM system (SIDM) algorithm has been developed for secure cloud computing with few new security parameters. The new algorithm proves to be a better option in two respects – first, it sends a token from IDM to CSP only and CSP does two types of verifications first, verifying Ccsp and Cidm received from users and IDM respectively. Second by asking two random security questions from a user before granting access to the resources. The experimental work and analysis of the algorithm have been done to overcome vulnerabilities of the general IDM systems.

As a future scope, this algorithm can be modified to make it decentralized so that a federation feature can be added in the algorithm. Also, RSA is a partial homomorphic algorithm which can be replaced by any full homomorphic algorithm to improve the performance of CSP.

References

[1] G. Rastogi and R. Sushil, “Cloud computing implementation: Key issues and solutions”, In IEEE Proc. of Computing for Sustainable Global Development (INDIACom), New Delhi, India, **(2015)**, pp. 320-324.

[2] R. L. Krutz and R. D.Vines, “Cloud Security: A comprehensive guide to secure cloud computing”,

Wiley Publishing, **(2010)**.
[3] A. Gopalakrishnan, "Cloud Computing Identity Management", SETLabs Briefings, vol. 7, **(2009)**, pp. 45–54.
[4] D. Zissis and D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer System, vol. 28, no. 3, **(2012)**, pp. 583–592.
[5] A. M. Lonea, H. Tianfield and D. E. Popescu, "Identity management for cloud computing", New concepts and applications in soft computing, vol. 417, **(2013)**, pp. 175-199.
[6] I. Khalil, A. Khreishah and M. Azeen, "Consolidated Identity Management System for Secure Mobile Cloud Computing", Computer Networks, vol. 65, **(2014)**, pp. 99-110.
[7] M. Jones and D. Hardt, The OAuth 2.0 authorization framework: Bearer token usage (No. RFC 6750), **(2012)**.
[8] R. Wang, S. Chen and X. F. Wang, "Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services", In IEEE Proc. of Symposium on Security and Privacy, Washington, DC, USA, **(2012)**, pp. 365–379.
[9] M. Ramachandran and V. Chang, "Towards performance evaluation of cloud service providers for cloud data security," International Journal of Information Management, vol. 36, no. 4, **(2016)**, pp. 618-625.
[10] D. Chandramohan, T. Vengattaraman and P. Dhavachelvan, "A secure data privacy preservation for on-demand cloud service", Journal of King Saud University-Engineering Sciences, vol. 29, no. 2, **(2017)**, pp. 144-150.
[11] J. Chen, X. Wu, S. Zhang, W. Zhang and Y. Niu (2012), "A decentralized approach for implementing identity management in cloud computing", In IEEE Proc. of second International conference on Cloud and Green Computing, Xiangtan, Chiana, **(2012)**, pp. 770 – 776.
[12] A. Benusi, "An Identity Management Survey on Cloud Computing", International Journal of Computing and Optimization, vol. 1, no. 2, **(2014)**, pp. 63-71.
[13] U. Habiba, R. Masood, M. A. Shibli and M. A. Niazi, "Cloud identity management security issues & solutions: a taxonomy", Complex Adaptive Systems Modeling, vol. 2, no. 1, **(2014)**, pp. 2-37.
[14] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability", Journal of Systems and Software, vol. 113, **(2016)**, pp. 130-139.
[15] "Anatomy of attack", A blog, RSA FraudAction Research Lab, **(2013)**. (Accessed on 10th May 2016). https://blogs.itb.ac.id/el5007s1t2014d201523214020luqmanzagi/
[16] "Emerging cyber threats", A report, Georgia tech cyber security summit 2013, The Georgia Tech information security center and Georgia tech research institute, **(2016)**. (Accessed on 10th May 2016).
[17] "Emerging cyber threats", A report, Georgia tech cyber security summit 2015, Institute for Information security and privacy, **(2015)**. (Accessed on 19th Oct. 2016),
http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf
[18] "Android master-key vulnerability", Application security resource of infosec institute, **(2013)**. (Accessed on 10th May 2016). http://resources.infosecinstitute.com/android-master-key-vulnerability-poc/#gref
[19] S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan and K. K. R. Choo, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service", Journal of Network and Computer Applications, vol. 74, **(2016)**, pp. 98-120.
[20] B. Bhargava, N. Singh and A. Sinclair, "Privacy in Cloud Computing through Identity Management, Defense technical information center", Purdue Univ. LAFAYETTE IN, **(2016)**. (Accessed on 10th May 2016). https://www.cs.purdue.edu/homes/bb/
[21] G. Rastogi and R. Sushil, "A Review Paper on Cloud Identity Management Systems", In Proc. of international conference on cloud computing and big data, Thailand, Phuket, **(2016)**, pp. 1-8.
[22] G. Verma and R. P. Arora, "Implementation of highly efficient Authentication and Transaction Security", International Journal of Computer Applications, vol. 21, no. 3, **(2011)**, pp. 43-49.
[23] G. Rastogi and R. Sushil, "Cloud Computing Security and Homomorphic Encryption", IUP Journal of Computer Sciences, vol. 9, no. 3, **(2015)**, pp. 48-59.
[24] S. Kumar, S. K. Singh, A. K. Singh, S. Tiwari and R. S. Singh, "Privacy preserving security using biometrics in cloud computing", Multimedia Tools and Applications, (1st Online), **(2017)**, pp. 1-23.
[25] Y. Yu, L. Xue, M. H. Au, W. Susilo, J. Ni, Y. Zhang, A. V. Vasilakos and J. Shen, "Cloud data integrity checking with an identity-based auditing mechanism from RSA", Future Generation Computer Systems, vol. 62, **(2016)**, pp. 85-91.
[26] D. Nunez and I. Agudo, "BlindIdM: A privacy-preserving approach for identity management as a service", International Journal of Information Security, vol. 13, no. 2, pp. 199-215, 2014.
[27] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li and J. Ma, "PRIAM: Privacy Preserving Identity and Access Management Scheme in Cloud", KSII Transactions on internet and information systems, vol. 8, no. 1, **(2014)**, pp. 282-304.

Authors

Garima Rastogi, she is a research scholar in DIT University Dehradun, Uttarakhand, (INDIA) attached to the Department of Computer Science and Engineering. She has completed M.Tech in Computer Science Engineering and pursuing a PhD in the field of Cloud Computing from DIT University, Dehradun. She has published 15 research papers in different reputed journals and national and international proceedings. She is a member of Computer Society of India. She has also qualified UGC Net in Computer Science.

Rama Sushil, she is currently working as prof and head, Department of Information Technology, DIT University, Dehradun. She has completed PhD from IIT Roorkee, Uttarakhand, (INDIA). She has guided various PhD students. She has also authored chapters in the books of IGI Global and published more than 40 research papers. Her research interests are Cloud Computing, Mobile Agents and Distributed Computing.