I. J. Computer Network and Information Security, **2017, 3, 45-53**
Published Online March 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.03.06

Evaluation of Secure Cloud Transmission Protocol

Dinesha H.A
SGBIT/CSE, Belagavi, 590010, India
E-mail: sridini@gmail.com

Dr.D.H.Rao
SGBIT/CSE, Belagavi, 590010, India
E-mail: dr.raodh@gmail.com

Abstract**—**Authentication, Authorization, integrity, availability and confidentiality are important aspects in cloud computing services. Cloud services market demands can be increased by enhancing the authentication, data confidentiality and customer trust. To achieve strong authentication, security and to earn customer trust, we had proposed and published secure cloud transmission protocol (SecCTP) which describes SecCTP techniques in detail. In this paper, we evaluated the SecCTP and presented the GUI implementation. We discuss the applicability, usefulness and advantages of SecCTP techniques i.e. multi-dimensional password generation and multi-level authentication in comparison with existing cloud authentication and confidentiality techniques. We describe how SecCTP improves the identity, access management, integrity and confidentiality in existing cloud service access. We evaluated SecCTP resistance in multiple attacks.

Index Terms**—**Authentication, Access Control, Cloud computing, Confidentiality, Security.

I. Introduction

Cloud computing services are being used worldwide over internet to enhance business infrastructure and to fulfill on demand VMS, storages, platforms and software requirements. These services can be implemented in public, private, community and hybrid models. These services market has to prove its identity, access control, integrity, confidentiality and trust every time. Cloud service demands can be increased by achieving customer trust, Authentication, Authorization/Access control (AA), confidentiality and security. Cloud Service Providers(CSP) demonstration on strong authentication, integrity, confidentiality and secure channel, penalty on security break and CSP service level agreements are the main aspects to earn customer faith and to attract more customers.

Literature reports many authentication, access control, integrity, and confidentiality issues of cloud services [1]-[6]. These issues motivate us to look into multi-level, multi-dimensional way of accessing the cloud IaaS services. How good these structure help in checking privileges and access controls while accessing cloud services are described. Defence, Military and universities and similar organizations are working in hierarchical structure with different working powers/privileges and security in mind. Higher the level, more the power/privilege is. This inspires us to map multi-level structures with cloud AA, Confidentiality and security. Literature reports AA, confidentiality and security issues on cloud services [1]-[6].

Table 1 describes literature reported issues and proposed solution [7]-[26]. Literature study and demerits about cloud identity and access control issues, confidentiality issues, proposed solutions for existing problems and its demerits motivate us to take objectives of cloud strong authentication and secure channel to achieve customer trust, privacy, integrity, confidentiality and security.

We applied SecCTP techniques for accessing cloud services, to assure strong authentication and to achieve confidentiality in secure channel. SecCTP can be a solution for the issues reported in literature, such as:

i) Identity issues, authenticated Access based on user types (privileged access rights)
ii) Data Confidentiality and Integrity
iii) Poor identity and access management procedures and Implementation of poor access control and procedures.

Proposed SecCTP [27][28] has Multi-Dimensional Password (MDP) system [29], Multi-level Authentication (MLA) technique [30] and Multi-level Cryptography (MLC) system [31] to fix the identity, access control and confidentiality issues reported in literature.

This paper is organized as follows, Section 2, evaluated SecCTP techniques and describes its resistance against different attacks, compares the SecCTP techniques over existing cloud authentication and confidentiality techniques. It also describes usefulness and requirement of this protocol in different cloud services. Section 3, describes the SecCTP GUI implementation. Section 4, concludes the paper with future enhancements.

Table 1. Lliterature Reported Issues and Proposed Solution

Ref. No	Cloud Computing Services	Reported Cloud Computing Authentication and Confidentiality Issues[1]-[6]
	Sources of Information	
1	TCS Innovation Labs: Cloud Security Alliance (CSA), DMTF, SNIA, OGF, OCC,OASIS, ITU,ETSI,OMG, ARTS, IEEE, ATIS, IETF[1] {2009-2011 Reports}	Reported issues on poor identity and access management Procedures. Existing implementation of poor access control procedures creates many threat opportunities, for example that disgruntled ex-employees of cloud provider organizations maintain remote access to administer customer cloud services, and can cause intentional damage to their data sources [1]. Authentication and authorization issues reported in [1] which was 2009 to 2011 consolidated Survey of NIST Cloud Standards, Cloud Security Alliance (CSA), Distributed Management Task Force (DMTF), Storage Networking Industry Association (SNIA), Open Grid Forum (OGF), Open Cloud Consortium (OCC), Organization for the Advancement of Structured Information Standards (OASIS), TM Forum, International Telecommunication Union (ITU), The European Telecommunications Standards Institute (ETSI), Object Management Group (OMG), Association for Retail Technology Standards (ARTS), Institute of Electrical and Electronics Engineers (IEEE), Alliance for Telecommunications Industry Solutions (ATIS), Internet Engineering Task Force (IETF) [1].
2	HP Labs in year 2011[2]	Reported demerits on Lack of User Control, Unauthorized Secondary Usage, Access, Audit, Lack of Customer Trust[2]
3	Accenture Lab in 2011 [3]	Reported the concern around cloud access (authentication, authorization and access control or AAA), encrypted data communication, and user identity management [3]. 1) C31: How do I ensure that there is no unauthorized access to my cloud by a disgruntled employee, who has left the organization or by an identity thief? 2) C32: How to ensure proper levels of authentication to cloud services? How do I manage multi-device access? 3) C33: In multi-cloud scenario, how do I ensure that I provide / delegate access to users to different security domains so that the end-to-end workflow is seamless? Similarly, in hybrid cloud, how do I create a minimum common access control and identity structure? [3]. Demerits of: LDAP and Active Directory for providing organizational role-based access to a cloud PaaS or SaaS provider. Demerits of x.509 certificate, Security Assertion Markup Language and etc [3]
4	CA Technologies 2012-13[4]	Reported hybrid identity and access management in the cloud identify and authenticate user survey calculation before granting access to information or infrastructure. The ability to control strong authentication prior to accessing data and applications in the cloud environment [4].
5	Journal of Cloud computing Springer-2012[5]	Reported security domain as identity and access management, enabling authentication for cloud solutions while maintaining security levels and availability for customers and organizations; Reports user access, authentication and privacy as a novel concerns [5].
6	Cloud Authentication Protocol ieee [6]	Kerberos protocol: One flaw with Kerberos is that the replay attack [6] is still feasible. The OpenID authentication protocol was designed in 2005 which is prone to phishing vulnerabilities. OAuth Protocol: The protocol similar to Kerberos in several aspects and thus has comparable advantages and drawbacks. All of above rely on user's memorable passwords. A zero knowledge authentication protocol, sedici 2.0 protocol t uses third party authentication and solves phishing attacks reasonably but again it depends on textual passwords leads to vulnerability [6].
7	Cloud Gossip Protocol for Dynamic Resource Management[7]	It addresses the problem of dynamic resource management for a large-scale cloud environment. Research contribution including outlining distributed middleware architecture and presenting one of its key elements: a gossip protocol that ensures fair resource allocation among sites/applications, dynamically adapts the allocation to load changes and scales both in the number of physical machines and sites/applications [7].
8	IEEE Transaction on Parallel Distributed Systems[8]	The authors proposed a dynamic auditing protocol that can support the dynamic operations of the data on the cloud servers. Disadvantage of this method may leak the data content to the auditor because it requires the server to send the linear combinations of data blocks to the auditor [8].
9	IEEE Transaction on Parallel Distributed Systems[8]	Proposed an efficient and inherently secure dynamic auditing protocol. It protects the data privacy against the auditor by combining the cryptography method with the bilinearity property of bilinear paring, rather than using the mask technique [8].
10	IEEE conf Access Protocols-2013 [9]	Developed nearby share retrieval protocols for single-version systems to improve the read access latency [9]. Cloud Fault Tolerance Protocol [10] Proposes a collaborative fault-tolerant transfer protocol for replicated data available on the Cloud and the Grid during exceptional faults [10].
11	Agent-Based User Authentication and Access Control-2013 [11]	The proposed model was named ACUA (Access Control and User Authentication) model that contains appropriate tools for validating user legal identities and acquiring their access control privileges for the resources according to the role information. Limited to some platform, Compatibility issue [11].
12	IEEE Infocom [12][13]	The authors extended their dynamic auditing scheme to be privacy preserving and support the batch auditing for multiple owners. However, due to the large number of data tags, their auditing protocols will incur a heavy storage overhead on the server[12][13]
13	IaaS Authentication [14]	Presents a full system architecture allowing the authentication and secured execution of binary files using hardware-assisted on-the-fly memory encryption/decryption. In a context of general blurring of the physical relationship between a user and the computer which it eventually interacts, this architecture has been thought so as to achieve a certain degree of robustness against corruptions in a cloud computing[14]
8	Password Authentication [15]-[18]	A secure authentication mechanism using graphical password should be proposed in this paper for improving traditional authentication mechanism and let users access cloud services securely [15]. It is breakable by shoulder surfing attack. Secured Biometric Authentication [16], Biometric Authentication [17], RFID based authentication [18] and Eid Authentication [19] has its own drawbacks.
14	Authentication Protocol[20]	Reported issues and proposed brief solutions on privileged access, authenticated access user types bug, vulnerability of platforms. Multi-tenanted application isolation, authentication privileges to particular user Data Protection, Integrity, vulnerability Physical security, Privileged access rights, control and monitoring maintaining infrastructure, communication channel security, intruder detection[20] .

15	Authentication Protocol in 2015 [21]	Can achieve privacy-preserving access authority sharing; User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires [21].
16	IEEE transaction, Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs-TCBI in 2015[22]	Proposed to solve the open problem of resisting layer-adding attack by outsourcing the privacy-preserving aggregated transmission evidence generation for multiple resource-constrained vehicles to the cloud side from performing any one-way trapdoor function only once [22]. PSMA in 2015 describes the multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed [23].
17	A secure user authentication protocol in 2015 [24]	It was applied in sensor network for sensor data capturing [24]. An Efficient and Secure Dynamic Auditing Protocol [25] ensures the integrity of the outsourced data but active adversary issue [25]. On the Security of an Efficient Dynamic 2014[26] demonstrated that an active adversary can modify the auditing proof to fool the auditor and the owner that the remote cloud files are pristine, while the files have been corrupted [26].

II. SEC CTP TECHNIQUES EVALUATION

This section presents the evaluation of MLA_MDP and MLC. It compares i) multi-level authentication with single level authentication, ii) password authentication with existing textual, graphical, 3d, biometric, RFID and 2- factor authentications and iii) describes how MLA_MDP and MLC suites in cloud computing service access.

A. Multi-level Authentication and Multi-dimensional Password System

Refer to Fig. 3 to 7 in section 3 describes SecCTP MLA _MDP define phase, MLA_MDP generation phase, and MLC Operations phase though RDP/SSH/Telnet/VDI to access cloud service. MLA_MDP define phase, defines number of levels L1,L2..Ln, Number of confidential MDP Inputs in each level L, i.e. Confidential images I1,I2…In and Confidential texts T1,T2…Tn used to generated multi-dimensional Password M.

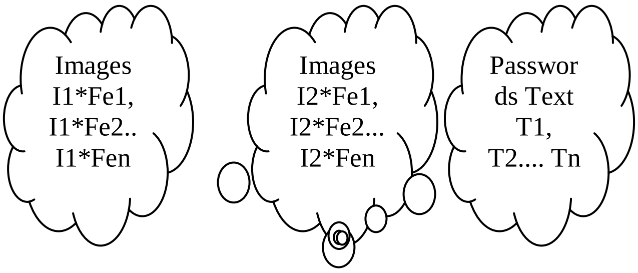


Fig.1. Images and Texts Group

As shown in fig.1, confidential Images are unique in its features Fe1,Fe2…Fen. This unique images features combined with Confidential texts generate M. M in its Level L binds with set of privileges S contains privileges access P1,P2…Pn. First level M used for cloud authentication, second level for Cloud Service CS and third level onwards for a cloud authorization Ca.

Hence Cloud authentication

$$CA= L1 <=M1<=(Rnd(I1(Fe1,Fe2..Fen)*I2(Fe1,Fe2..Fen)*In(Fe1,Fe2..Fen))||Rnd(T1*T2*..Tn)) \quad (1)$$

Generated MD Password M is Combined random images features data and random password text. Assuming two images and two password texts, possible MDP pattern will be Random featured image data with text password in regular expression is

$$M=[Ii+(Fej+)],Tk+ \quad (2)$$

Where, i, j, k lies in 1,2…N i.e. One or more features Fe of one or more images I combined with one or more texts T.

Table 2. Symbols and Notations

Symbols	Description
U	Cloud authenticated User
M	Multi-dimensional password generated using confidential inputs
P	User authorized Privileges on particular cloud service access
S	Privileges Set contains P's to work on particular cloud service by U
Ln	Nth Level, Leaf level in Multi-level authentication
I	Confidential Images which are unique in their features
T	Confidential Text which is a secret code decided by U
Fe	Confidential Image I Features such as RGB, Pixel, Brightness and etc
Pt	Password in Textual format
C	Complexities in breaking the proposed system
N	Last limit in Number. Last digit in range.
CSP	Cloud Service provider
CS	Cloud Service offered by CSP to U
||	Concatenation of previous level password
K	Key
Md	Metadata operation for rearrangement of data
Mdf	Metadata file contains rearrangement information
E(F)	Encryption of file plaintext contents
D(F)	Decryption of file cipher text contents
~Md	Reverse Metadata operation to get original data in right pattern
F	File contains plaintext/cipher text
Lk	Lock operation on encrypted file
Ul	Unlock operation to file received from CSP DSaaS service
Hk	Attacker/Hacker
CA	Cloud Authentication to prove customer authentication with CSP
Ca	Cloud Authorization to prove access rights/ privileges at customer's place
Rnd	Random selection of texts/image features
⊕	Xor Operation to be performed while generating MDP
G	Group contains the possible items
B	Brute force attack
r	Random generation
e	Error on operations
A	Admin who controls the CS

Hence Cloud Authorization for user U2 at Level 2, M1 will be:

$$Ca (U2, L2) = L1||M2 \quad (3)$$

Where, M2 =<=(Rnd(I1(Fe1, Fe2..Fen)*I2 (Fe1,Fe2..Fen) *In(Fe1,Fe2..Fen))||Rnd(T1*T2*..Tn))

Cloud authorization for User 3 at Level 3 will be

$$Ca(U3, L3) = L2||M3 \tag{4}$$

Where, M3 <=(Rnd(I1(Fe1, Fe2..Fen)*I2(Fe1,Fe2..Fen) *In(Fe1,Fe2..Fen)) ||Rnd(T1*T2*..Tn))

Derived authorization formula for User Un1 at Level Ln2 is

$$Ca(Un1,Ln2)= Ln2-1||Mn1 \tag{5}$$

Where, Mn1<=(Rnd(I1(Fe1, Fe2..Fen)*I2(Fe1, Fe2..Fen) *In(Fe1,Fe2..Fen))||Rnd(T1*T2*..Tn)).

Let us look into Complexities analysis to break SecCTP authentication i.e. MLA-MDP.

C1: Number of Levels unknown

C2: Number of images and text for generating M unknown.

C3: Confidential images are unknown and they are unique in their features.

C4: Text password unknown

C5: Order and technique for generating M Unknown

To break MLA-MDP Hk must known C1, C2, C3, C4 and C5 must be known.

SecCTP resists shoulder surfing attack: One of the potential drawbacks of graphic password authentication is Shoulder surfing attack. It happens through direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it is easy to stand next to someone and watch as they fill out. Using shoulder surfing hacker Hk may succeed to break C1, C2 and C4 but not C3 and through any intelligent observation due to order and generating techniques which are kept internal. Hence, shoulder surfing attack cannot break it.

SecCTP resists dictionary attack: One of the potential draw backs of textual password authentication. Typically, a guessing attack which uses precompiled list of options. Rather than trying infinite option, Hacker Hk creates a file with all possible dictionaries of words and tries to login using dictionary words with different combinations to break authentication. Assuming C1and C2 derives the probability of breaking the SecCTP authentication system. Dictionary of images is presented in dictionary of group 1, group 2 and text password in group 3.

Assuming C5 i.e. ordered combination of group1, group2 and group 3 values, deriving the Probability of getting actual MDP M?

Dictionary of group1 Images I1 with its features variations are: I1*Fe1, I1*Fe2.. I1*Fen. Dictionary of group 2 images I2 with its features variations are:I2*Fe1, I2*Fe2..I2*Fen and finally Group 3 contains possible password text dictionary of words. Now applying permutation by assuming C5, in G1*G2|| G3, deriving the probability of breaking CA as below:

$$CA<= \prod_{i=1}^{N1} Gi \prod_{j}^{N} \tag{6}$$

Successful break of CA has to face Ca for operations. Assuming 2 images and 1 text group again, deriving Ca as below:

$$Ca<= CA || \prod_{i=1}^{N1} Gi \prod_{j=1}^{N2} \tag{7}$$

Hence, to succeed in SecCTP authentication trough dictionary attack, assuming C1, C2 and C5 the complexities are derived as below:

$$\sum_{i=1}^{N1} Li \;||\; \prod_{i=1}^{N1} Gi \prod_{j=1}^{N2} Gj \;||\; \prod_{k=1}^{N3} Tk \tag{8}$$

SecCTP resists brute force attack: One of the potential drawbacks of textual password authentication. It attempts to determine a password by trying every possible combination. Assuming C1 and C2 , Hk tries with all possible images and texts not restricted to any set /lists/group. Automatic tools/pgms keep generating the possible inputs and combination to break the system. Considering brute force generation B1 and B2 for images and B3 for text, and assuming C4 as B1, B2 and B,. The derived complexities to break system are:

$$CA<= \prod_{i=1}^{N1} Bi \prod_{j=1}^{N2} B \tag{9}$$

Hence

$$\sum_{i=1}^{N1} Li \;||\; \prod_{i=1}^{N1} Bi \prod_{j=1}^{N2} Bj \;||\; \prod_{k=1}^{N3} Bk \tag{10}$$

SecCTP resists insider attack: One of the potential drawbacks of authentication and authorization. An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access. Personnel inside the company/system try to access the resource and perform operations to which they are not authorized to do. SecCTP resists it through strong binding and checking privilege to its level L and MDP M. Inside attacker Hk to break the system hacker has to succeed in multiple-levels with MDP M. Since Privileges Set S binds with M and L, Hk has to know the M and L. Let us analyze the complexities to break the proposed system by inside attacker Hk:

Multiple Levels L1, L2.. Ln
Multidimensional Password M1, M2, M3...Mn
Possible Privileges/operations P1, P2, P3... Pn
Set of privileges/Operation S1, S2,.... Sn

Figure 2 shows SecCTP MLA-MDP user privilege trees, representing the USER-LEVEL-PASSWORD-PRIVILIGED SET record.

L1, U1, M1, S1} ------------> {CS1}

The user U1in Level L1 holds an M1 password which binds for S1 operations on Cloud service1.

Hence CS1 authentication and authorization file contains privileged user entry with MDP and S can be derived as

$$\sum_{i=1}^{N1} Li \sum_{i=1}^{N2} UM \tag{11}$$

Strong binding of privilege with M, U and L restricts unauthorized users.

Scenario 1: Hkis authenticated but not authorized to CS1.Then the complexity is MDP, if Hk tries with random MDP M , SecCTP tree checks for L,M and S, if permutation does not match, then, report to Level Admin with the attack details.

Lr,Hkr, Mr,-, => CS1 <>SecCTP Tree ({L1, U1, M1, S1} ... {Ln,U,Mn,Sn} Then, alert error message 'e' to Admin A.

Scenario 2: Hk is authenticated and authorised to CS1 but not having privilege Pr in Set S .Then, the complexity is is MDP if Hk tried with random MDP M , SecCTP tree checks for L,M and S, if permutation does not match, then, it reports to Level Admin with the attack details.

Lr,Hkr, Mr,Pr, => CS1 <>SecCTP Tree ({L1, U1, M1, S1} ... {Ln U, Mn, Sn} Then, alert error message 'e' to corresponding level admin A.

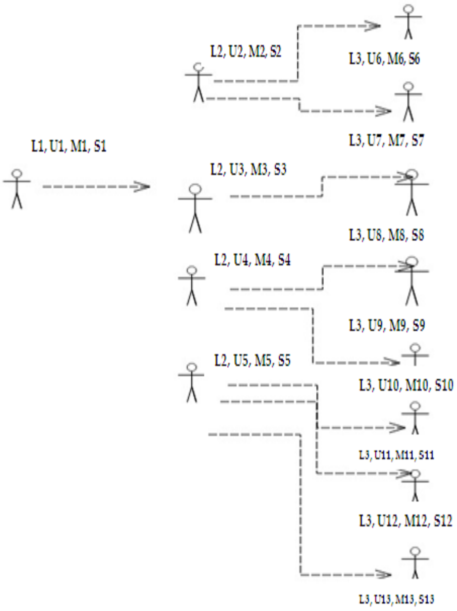


Fig.2. SecCTP MLA-MDP user Privileged Trees

SecCTP resist Phishing attack/Masquarade Attack: One of the potential drawbacks of internet authentication. It happens by masquerading as a trustworthy entity in an electronic communication and collects the confidential inputs. Assuming Hk success in this technique, Hk can collect confidential inputs like images, I1, I2.. In and texts T1, T2..Tn, hence Hk can break C1, C2, C3 and C4. Let us analyze the strength of MLA-MDP after breaking C1, C2, C3 and C4.

C5 and Level wise MDP M concatenation is again challenging, i.e. L1, L2.. Ln, passwords M concatenation. Again, each access checks against privileges set S, notes any misbehavior and wrong operation and reports to A with error 'e'. Complexity is CA and Ca matching in multiple levels and privilege Tree

That is, Lr, Hkr, Mr, Pr, => CS1 <>SecCTP Tree ({L1, U1, M1, S1} ... {Ln,U,Mn,Sn}.

SecCTP resists an integrity attack: One of the potential threats for important data where many users depend upon. A data integrity threat is when an attacker attempts to corrupt data without the permission of the owner. SecCTP MLA-MDP checks CA and Ca across Levels and MDP, unauthorized user and unprivileged operations cannot be done. If,Hk tries to change the data 'D' at DSaaS storage. L1||L2||Ln checks authentication, authorization and operation privileges. Hence, no data are modified with matching LUMS SecCTP privileged tree.

SecCTP resists a stolen verifier attack: One of the potential server data base attacks. It checks the possible verifier at server checking during CA and Ca The possible and stolen that verifies information to pass it on to Hk. MLD _MDP have multi-levels and MDP attached to previous levels. verifier to be stolen are L1,L2..Ln and M1, M2..Mn with Level dependencies. Privilege set S to be known for successful hack. Minimum verifier to be stolen for Ca -CA is Ln(Mn,Sn)||L2(M2,S2)||... L1(M1, S1)

Table 3 compares the proposed multi-level authentication with existing single level and 2- factor authentication. It differentiates the privileges with different levels. Table 4 lists the comparison of MDP with existing textual, graphical, 3D, 2 factors, Biometric and RFID.

Table 3. Multi-level vs. Single level authentication

Multi-level Authentication	Single Level Authentication
Multi-level authentication checks authentication and authorization in multiple levels with multi-dimensional password.	Authentication and Authorization binds in single level with single password. In 2 factors, it depends on secret code which sends to mobile.
Depending on level, suitable privileges will be assigned. Levels and password bind with privileges	Single level authentication grants complete access/full privileges on single successful login.
Ex: Cloud IaaS: MDP-MLA checks customer authentication and authorization in multiple sign in first level, it checks for authentication, in second level, for instance, creation, third level for only for operation with instances.	Ex : Existing Cloud IaaS uses single sign in to access the cloud IaaS instance creations, deletion, operations and software installations
Can customize the levels based on the security requirements of the customer.	Fixed sign on
Though it is multi-level, every individual has to enter one password. But below each level, individual has to wait for higher level clearance.	Customer has to remember only one password. In 2-factor authentication, customer must use mobile/email and then has to enter secret password.

B. MLA-MDP in Cloud computing Environment

MLA -MDP can be used in cloud computing environment. This section discusses the usefulness of MLA-MDP in public cloud IaaS, PaaS, and SaaS. Public IaaS instances and PaaS platforms access are made available in single authentication. Existing IaaS, PaaS and SaaS authentication and authorization are compared with MLA_MDP in table4.

Table 4. MDP vs Existing Textual, Graphical, 3D, 2 factor, Biometric and RFID

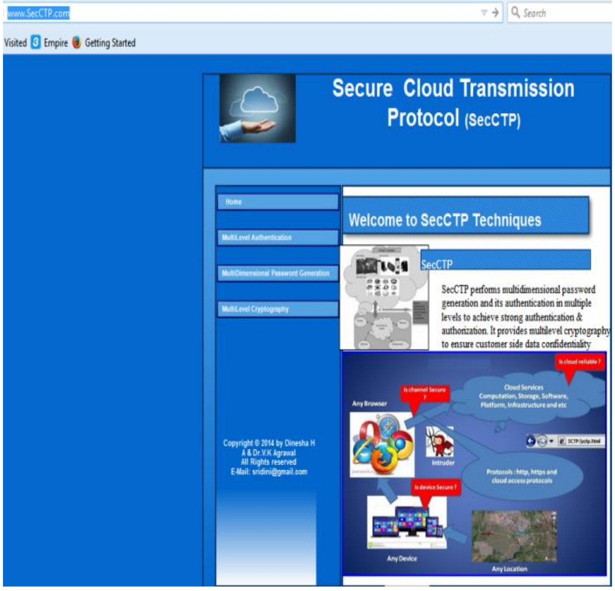
Sl No	Multi-dimensional Password	Existing Password
1	It uses confidential images features with secret text password to generate MDP.	Textual password uses only Alphabets, Numbers and special characters. Strength depends on numbers and types of characters.
2	It is difficult to break the confidential images which are unique in their pixel, RGB, brightness and other features with combination of texts.	Textual Passwords are easy to break and are highly vulnerable to dictionary or brute force attacks.
3	In MDP confidential images, it is difficult to recall the image features such as size, pixel, brightness, intensity, colors hence it is not vulnerable to shoulder surfing.	Graphical passwords uses drawing pattern, inputs from images/GUI. It requires much memory space and with time complexity. Graphical Passwords are vulnerable to shoulder surfing.
4	MDP does not require any 3D technology and latest computer. It can be implemented with existing technology and computers.	3D Password is multi-factor authentication system where it combines recognition, recalls, biometrics and token. It is a combination and sequence of user interaction done in the 3D environment. 3D password requires lots of coding and latest computer 3d technology is required to implement it.
5	It is required to have confidential folder storage at local hard disk/secret space than keeping extra devices and extra typing.	2 Factor authentication uses login password first then secret code confirmation which is sent to registered number/Email for successful authentication It is required to keep phone/token for 2FA at all times. People often get tired of having that extra bit of typing to do, and eventually disable 2FA.
6	No need to install any device and facility. No biological traits change affects here unless they change image features.	Biometric authentication depends on biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures. It depends on biological traits, ageing, timely biological changes are weaknesses. Extra device/facility is to be installed.
7	RFID fields to cloud user may not appropriate and it is additional implementation to be done.	RFID is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. Each unit has to be identified and may not be best suited to cloud.

Table 5. IaaS, PaaS, SaaS and DSaaS Authentication and Authorization

Sl N	Existing Cloud Service Authentication	Strong authentication/privileged access using MLA_MDP
1	Data Storage as a service: DSaaS: Ex: Drop box service. Data storage folder, files are kept in cloud. Individual can edit, delete and add the data on successful login.	DSaaS authentication done at organization Level i.e. at first level. Then second level checks the DSaaS authorization to add, delete, modify etc. Third level checks the individual read, write operation. It helps to restrict modify, delete, edit, add operations if the user is restricted.
2	SaaS: Grants software service over website. ex: MS office 365, CAD software. In single sign in, customer can access the complete privileges. No organization level authentication and administration control is required. Within organization, no sub levels, no flexibility to bind with organization policy is required	Authentication of SaaS done in level1 i.e. organization level with its MDP password. Authorization of particular software service done in level2. Operation Privileges i.e. read, write, execute, update and delete etc binds with 3rd level. Authentication and authorization strictly check at different levels. Customer side MLA_MDP admin map the policies with privileges.
3	PaaS: Multi-tenancy is the major issue at this level. Request information on how multi-tenanted applications are isolated from each other. A high level description of containment and isolation measures is required. Consider a webhosting platform, how customer gets authentication and gets privileged access. Ex: Institution has N departments; each dept. updating must be done by their dept head/web admin. All faculties' needs to update only his/her faculty profile displayed at website. How to achieve this in existing sign in. Webpage role creation could be a solution. How do you grant different role access. Single sign in may not gain complete customer trust.	PaaS Authentication to update website is done in first level using MDP. In second level, it allows departments to update dept information. Head/dept web admin logins to update only his dept information. Writes /updates privileges to his dept web pages and only read privileges to other department WebPages. Similarly, in third level, faculty can update only his/her webpage not dept or institutional. At each level, MDP is required. It can be generated using their institutional/dept/individual confidential images and secrete code. Hence, it could be the best demonstration to earn customer faith on multi-tenanted application issues.
4	IaaS : VM instances, privileges for create, delete, update, vms are given on single sign in. VM access through RDP grants VM complete access for installing/un installing software and application, change OS, software, memory settings etc. Folder creation, deletion, execution of any malware program allowed.	In first level, it checks the organization authentication and allows department to continue. In second level, dept privileges checks for VM create, delete and updation. In third level i.e. RDP access, it allows customer to perform specific operation as stated at previous level. Hence, strong authentication is achieved.

III. SecCTP GUI Implementation

This section presents the SecCTP typical graphical user interfaces for representing its techniques and functionalities. It presents sequence of SecCTP major GUI which are important in commissioning of proposed protocol for cloud computing environment.

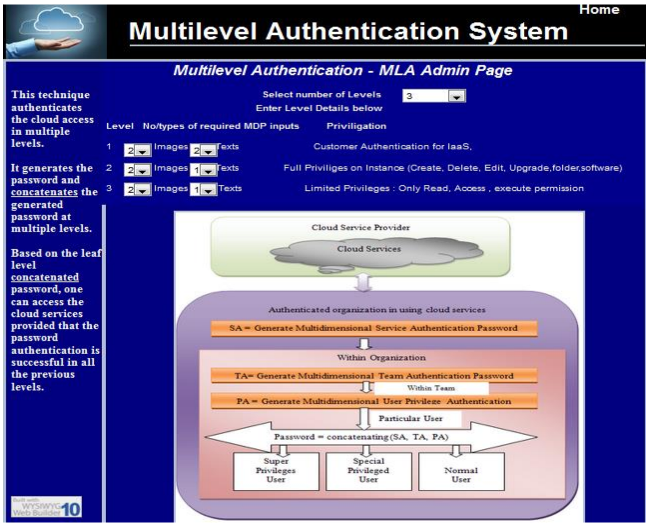

www.SecCTP.com
Search
Visited
Empire
Getting Started
Secure Cloud Transmission Protocol (SecCTP)
Home
MultiLevel Authentication
MultiDimensional Password Generation
MultiLevel Cryptography
Welcome to SecCTP Techniques
SecCTP
Is cloud reliable ?
Is channel Secure ?
Any Browser
Cloud Services Computation, Storage, Software, Platform, Infrastructure and etc
Intruder
SCTP://sctp.html
Protocols : http, https and cloud access protocols
Is device Secure ?
Any Device
Any Location

SecCTP performs multidimensional password generation and its authentication in multiple levels to achieve strong authentication & authorization. It provides multilevel cryptography to ensure customer side data confidentiality

Copyright © 2014 by Dinesha H A & Dr.V.K Agrawal All Rights reserved E-Mail: sridini@gmail.com

Fig.3. SecCTP Home Page

Figure 3 shows, SecCTP home page to access the major MLA, MDP and MLC admin pages. This particular page offers by vendor to define the customer side authentication and confidentiality. This runs with http protocols. After Service Level agreement, it has to be defined by customer. Customer security team may define internal policies of accessing the cloud IaaS instances, Platforms and storing the data on cloud DSaaS. Defined policies levels, password generation modes and confidentiality methods have to be entered in admin pages.


Home
Multilevel Authentication System
Multilevel Authentication - MLA Admin Page
Cloud Service Provider
Cloud Services
Authenticated organization in using cloud services
SA = Generate Multidimensional Service Authentication Password
Within Organization
TA= Generate Multidimensional Team Authentication Password
Within Team
PA = Generate Multidimensional User Privilege Authentication
Particular User
Password = concatenating (SA, TA, PA)
Super Privileges User
Special Privileged User
Normal User
Built with WYSIWYG Web Builder 10

This technique authenticates the cloud access in multiple levels.

It generates the password and concatenates the generated password at multiple levels.

Based on the leaf level concatenated password, one can access the cloud services provided that the password authentication is successful in all the previous levels.

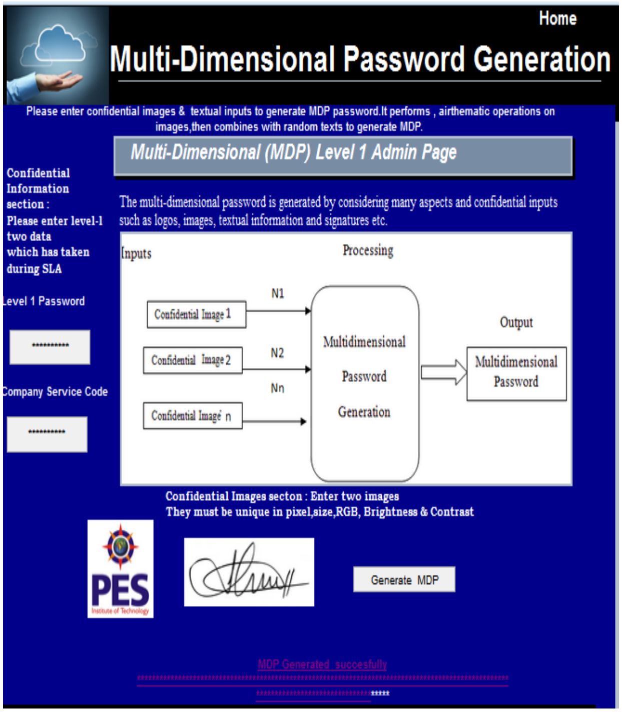
Select number of Levels 3

Enter Level Details below

Level	No/types of required MDP inputs	Priviligation
1	2 Images 2 Texts	Customer Authentication for IaaS,
2	2 Images 1 Texts	Full Priviliges on Instance (Create, Delete, Edit, Upgrade,folder,software)
3	2 Images 1 Texts	Limited Privileges : Only Read, Access , execute permission

Fig.4. MLA and MDP Admin Page

Figure 4 shows the MLA and MDP admin page. This page allows customer side admin to enter number of levels in authentication, types and number of inputs to consider in each levels to generate the MDP passwords, Privileges to be bound in each level with each MDP. Based on these inputs, multi-level authentication starts its functions, before granting cloud service, it authenticates in multi-level with MDP passwords. It uses tree structure, based on leaf level; it checks authentications and access privileges.


Home
Multi-Dimensional Password Generation
Multi-Dimensional (MDP) Level 1 Admin Page
Inputs
Processing
N1
N2
Nn
Confidential Image 1
Confidential Image 2
Confidential Image n
Multidimensional Password Generation
Output
Multidimensional Password
PES Institute of Technology
Generate MDP

Please enter confidential images & textual inputs to generate MDP password.It performs , airthematic operations on images,then combines with random texts to generate MDP.

Confidential Information section : Please enter level-1 two data which has taken during SLA

Level 1 Password **********

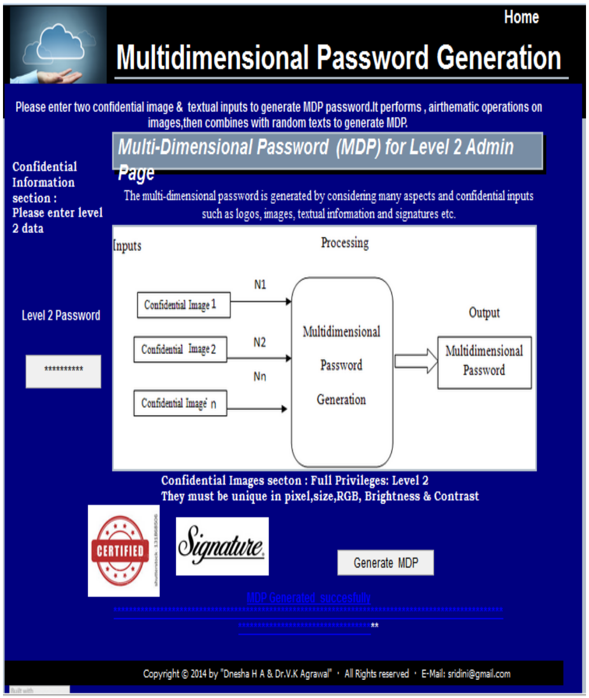
Company Service Code **********

The multi-dimensional password is generated by considering many aspects and confidential inputs such as logos, images, textual information and signatures etc.

Confidential Images secton : Enter two images
They must be unique in pixel,size,RGB, Brightness & Contrast

MDP Generated succesfully

Fig.5. MDP Level 1 Admin Page


Home
Multidimensional Password Generation
Multi-Dimensional Password (MDP) for Level 2 Admin Page
Inputs
Processing
N1
N2
Nn
Confidential Image 1
Confidential Image 2
Confidential Image n
Multidimensional Password Generation
Output
Multidimensional Password
CERTIFIED
Signature.
Generate MDP
Built with

Please enter two confidential image & textual inputs to generate MDP password.It performs , airthematic operations on images,then combines with random texts to generate MDP.

Confidential Information section : Please enter level 2 data

Level 2 Password **********

The multi-dimensional password is generated by considering many aspects and confidential inputs such as logos, images, textual information and signatures etc.

Confidential Images secton : Full Privileges: Level 2
They must be unique in pixel,size,RGB, Brightness & Contrast

MDP Generated succesfully

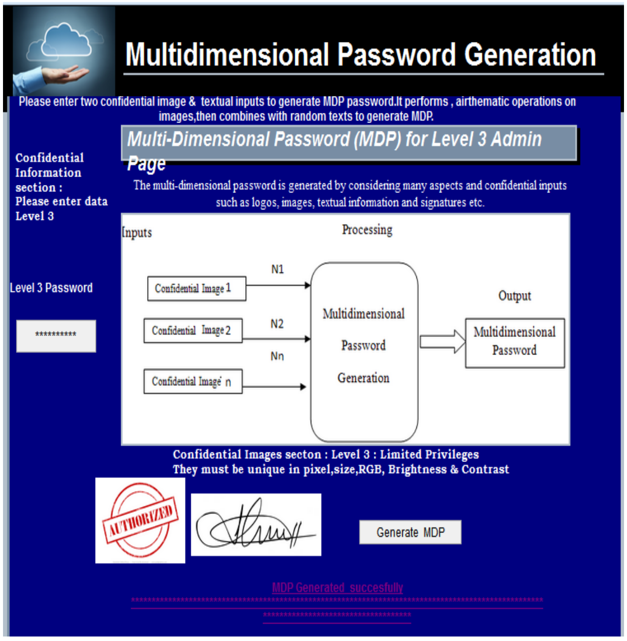
Copyright © 2014 by "Dnesha H A & Dr.V.K Agrawal" · All Rights reserved · E-Mail: sridini@gmail.com

Fig.6. MDP Level 2 Admin Page

Figure 5 shows, MDP Generation at Level 1 admin page, which accesses the confidential inputs from organization head/chief/senior related to organization which are given during SLA with Cloud service Provider CSP. After entering these confidential inputs in images and texts format, technique extracts image features combines with textual data and binds them with level and their privileges which are entered at MLA admin page. Output of this page is generated MDP level 1 for customer authentication.

Figure 6 shows the MDP Generation at Level 2 admin page, which accesses the confidential inputs from team/department/division related to department which are given at level1 authority. After entering these confidential inputs in images and text format, technique extract image features combine with text data and bind them with level and their privileges which are entered at MLA admin page. Output of this page is MDPlevel2 for cloud service authorization. Related to cloud IaaS Instances creation, deletion and updating can be assigned to this level.

Figure 7 shows MDP Generation Level 3 admin page, which accesses the confidential inputs from individuals related to their personal details which are given at level2 authority. After entering these confidential inputs in images and text format, technique extracts image features, combines with text data and binds them with level and its privileges which are entered at MLA admin page. Output of this page is MDP level3 for cloud service operation authorization. Related to Cloud IaaS, Instant operations like folder creation, software installation/un installation could be defined for level 3.



Multidimensional Password Generation

Please enter two confidential image & textual inputs to generate MDP password.It performs , airthematic operations on images,then combines with random texts to generate MDP.

Multi-Dimensional Password (MDP) for Level 3 Admin Page

Confidential Information section : Please enter data Level 3

The multi-dimensional password is generated by considering many aspects and confidential inputs such as logos, images, textual information and signatures etc.

Level 3 Password: **********

Confidential Images secton : Level 3 : Limited Privileges
They must be unique in pixel,size,RGB, Brightness & Contrast

MDP Generated succesfully

Fig.7. MDP Level 3 Admin Page

IV. Conclusion and Future Enhancement

SecCTP facilitates the MLA and MDP to achieve the strong authentication and secure channel. SecCTP resist the different attacks such as brute force attack, dictionary attack, insider attack and etc. Tree- based authentication checks for strong authentication against privileges. MDP increases the strength of password by means of confidential images. MLD facilitates the secure channel with its own way of locking, metadata operation and its cryptographic algorithms. Though there are multiple levels, user has a burden to remember only one password. SecCTP GUI describes the admin inputs in MLA and MDP. SecCTP runs on http. It can be further improved by adding more features such as, Multilevel Cryptography IDS/IPS and multi-level stenography.

Acknowledgment

Our sincere thanks to Shri. S.G. Sambargimath, Chairman and Dr.S.S.Salimath, Principal SGBIT, VTU Belagavi, for their constant encouragement

References

[1] Jaydip Sen, Security and Privacy Issues in Cloud Computing, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA, 2011-13.

[2] Siani Pearson and Azzedine Benameur, Cloud and Security Research Lab HP Labs Privacy, Security and Trust Issues Arising from Cloud Computing, 2nd IEEE International Conference on Cloud Computing Technology and Science, 978-0-7695-4302-4/10,693-792.

[3] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma, Accenture Technology Labs, Accenture Bangalore, India, Cloud Computing Security - Trends and Research Directions, 2011 IEEE World Congress on Services, IEEE computer Society,978-0-7695-4461-8/11,524-531.

[4] Ponemon Institute, Security of Cloud Computing Users Study, CA Technologies Independently conducted by Ponemon Institute, LLC Publication Date: March 2013

[5] Nelson Gonzalez1*, Charles Miers1,4, Fernando Red´ıgolo1, Marcos Simpl´ıcio1, Tereza Carvalho1, Mats N¨aslund2 and Makan Pourzandi3, A quantitative analysis of current security concerns and solutions for cloud computing, springer , Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11

[6] Slawomir Grzonkowski and Peter M. Corcoran, Thomas Coughlin, Security Analysis of Authentication Protocols for Next-Generation Mobile and CE Cloud Services, 2011 IEEE International Conference on Consumer Electronics - Berlin (ICCE-Berlin), 978-1-4577-0234-1/11, 83-87.

[7] Fetahi Wuhib, Rolf Stadler, and Mike Spreitzer, A Gossip Protocol for Dynamic Resource Management in Large Cloud Environments, ieee transactions on network and service management, vol. 9, no. 2, 1932-4537, 213-225,June-2012.

[8] Kan Yang, Xiaohua Jia, An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, IEEE transactions on parallel and distributed systems, vol. 24, no. 9, September 2013, 1717-1726.

[9] Yunqi Ye, Liangliang Xiao, Yinzi Chen, I-Ling Yen, Farokh Bastani, Ing-Ray Chen, Access Protocols in Data Partitioning Based Cloud Storage, 2013 IEEE Sixth International Conference on Cloud Computing, 978-0-7695-5028-2/13, 398-397, 2013.

[10] Nader Mohamed and Jameela Al-Jaroodi, A Collaborative Fault-Tolerant Transfer Protocol for Replicated Data in the Cloud IEEE transaction, 978-1-4673-1382-7/12, 203-210, 2012.

[11] Mostafa Hajivali , Faraz Fatemi Moghaddam , Maen T. Alrashdan , Abdualeem Z. M. Alothmani , Applying an Agent-Based User Authentication and Access Control Model for Cloud Servers, ICTC 2013, 978-1-4799-0698-7/13, 807-902,2013.

[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public

Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 5,pp. 847-859, May 2011.

[13] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,", Proc. IEEE INFOCOM, pp. 525-533, 2010

[14] Laurent Hubert, Renaud Sirdey, Authentication and secured execution for the Infrastructure-as-a-Service layer of the Cloud Computing model, 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 978-0-7695-5094-7, 291-296, 2013.

[15] Ming-Huang Guo, Horng-Twu Liaw, Li-Lin Hsiao, Chih-Ta Yen, Authentication Using Graphical Password in Cloud, 177-181, 2013.

[16] H. B. Tang*, Z. J. Zhu, Z. W. Gao, Y. Li, a secure biometric-based authentication scheme using smart card,ieee, 39-43,2013.

[17] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards",. IET Information Security, 5 (3), pp. 145-151, 2011.

[18] Wei Xie1, Lei Xie2, Chen Zhang1, Quan Zhang1, Chaojing Tang1, Cloud-based RFID Authentication, 2013 IEEE International Conference on RFID, 978-1-4673-5750-0/13,168-175, 2013.

[19] Bernd Zwattendorfer, Arne Tauber, SECURE CLOUD AUTHENTICATION USING EIDS, Proceedings of IEEE CCIS2012, 978-1-4673-1857-0/12/, 397-401, 2012.

[20] Safiriyu Eludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehinde, A User Identity Management Protocol for Cloud Computing Paradigm, apeared in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163

[21] Hong Liu, Huansheng Ning, Qingxu Xiong, Laurence T. Yang, Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing, ieee transactions on parallel and distributed systems, vol. 26, no. 1, january 2015, 241-251.

[22] Jun Zhou, Xiaolei Dong, Zhenfu Cao, Athanasios V. Vasilakos, Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs, ieee transactions on information forensics and security, vol. 10, no. 6, june 2015, 1299-1314.

[23] Jun Zhou, Xiaodong Lin, Xiaolei Dong, and Zhenfu Cao, PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System, ieee transactions on parallel and distributed systems, vol. 26, no. 6, june 2015, 1693-1703.

[24] Zhou Quan, Tang Chunming, Zhen Xianghan and Rong Chunming, A secure user authentication protocol for sensor network in data capturing, Springer Quan et al. Journal of Cloud Computing: Advances, Systems and Applications (2015 May) 1-12.

[25] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. Parallel and Distributed Systems,vol. 24, no. 9, pp. 1717-1726, Sept. 2013.

[26] Jianbing Ni, Yong Yu, Yi Mu, Qi Xia, On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage, ieee transactions on parallel and distributed systems, vol. 25, no. 10, October 2014, 2760-2761.

[27] Dinesha H A, Dr. V. K Agrawal, "Framework Design of Secure Cloud Transmission Protocol", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013, ISSN (Print): 1694- 0784 | ISSN (Online): 1694-0814,74-81.

[28] Dinesha H.A, Dr. V. K Agrawal, "Development of Secure Cloud Transmission Protocol (SeCTP) Engineering Phases: Multilevel Security and Cryptography", International Journal on Cryptography and Information Security, Vol. 5, No. 3/4, December 2015, ISSN: 1839-8626, December 2015.

[29] Dinesha H A, Dr. V. K Agrawal, "Multi-dimensional Password Generation Technique for accessing cloud services", Special Issue on: "Cloud Computing and Web Services", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.2, No.3, June 2012, 31-39.

[30] Dinesha H A, Dr.V.K.Agrawal, "Multi-level Authentication Technique for Accessing Cloud Services", IEEE International Conference on Computing, Communication and Applications (ICCCA-2012), Dindigul, Tamilnadu, India, 22-24 February 2012, 978-1-4673-0270-8, 1 – 4.

[31] Dinesha H A, Dr.V.K Agrawal, "Multilevel Cryptography with Metadata and Lock Approach for Storing Data in Cloud", Transactions on Networks and Communications, Volume 2, Issue 6, 10.14738/tnc.26.591. Dec 2014, 48-56.

Authors' Profiles

Dinesha H. A. has completed his bachelor of engineering from Malnad College of Engineering, Hassan and Master of Technology from R.V.C.E, Bangalore. Presently, he is pursuing his PhD on cloud computing security. He was working with VMware pvt India ltd, PES Institute of Technology as Assistant Professor in ISE & CORI R & D and DIAT-DRDO as a Officer In Charge Data Center. Presently he is working in SGBIT as a Assistant Professor CSE dept. He has published cloud computing research papers in many international journals and conferences. His research interest areas are virtualization technology, cloud computing and software engineering. He is a member in ISTE, IACSIT and IAEng., received best paper award in CLUSE2012. Ph: +91-7767076988, sridini@gmail.com.

Dr.D.H. Rao completed B.E, M.E, MBA, M.S, and Ph.D. He was working with VTU, Jain College of Engineering, and GIT, Belagavi. He is a member of various reputed bodies. He has published various papers in many reputed journals and conferences. He was a chair in many international conferences. At present he is working in SGBIT as a Dean (Research and Skill), Belagavi. Contact email id: dr.raodh@gmail.com

How to cite this paper: Dinesha H.A, D.H.Rao,"Evaluation of Secure Cloud Transmission Protocol", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.3, pp. 45-53, 2017.DOI: 10.5815/ijcnis.2017.03.06