IMPROVED SECURE CLOUD TRANSMISSION PROTOCOL

Dinesha H A[1] and D.H. Rao[2]

[1]Assistant Professor, Department of CSE,
S.G. Balekundri Institute of Technology, Belagavi, India
[2] Professor, Department of CSE,
S.G. Balekundri Institute of Technology, Belagavi, India

ABSTRACT

Secure cloud transmission protocol (SCTP) was proposed to achieve strong authentication and secure channel in cloud computing paradigm at preceding work. SCTP proposed with its own techniques to attain a cloud security. SCTP was proposed to design multilevel authentication technique with multidimensional password generations System to achieve strong authentication. SCTP was projected to develop multilevel cryptography technique to attain secure channel. SCTP was proposed to blueprint usage profile based intruder detection and prevention system to resist against intruder attacks. SCTP designed, developed and analyzed using protocol engineering phases. Proposed SCTP and its techniques complete design has presented using Petrinet production model. We present the designed SCTP petrinet models and its analysis. We discussed the SCTP design and its performance to achieve strong authentication, secure channel and intruder prevention. SCTP designed to use in any cloud applications. It can authorize, authenticates, secure channel and prevent intruder during the cloud transaction. SCTP designed to protect against different attack mentioned in literature. This paper depicts the SCTP performance analysis report which compares with existing techniques that are proposed to achieve authentication, authorization, security and intruder prevention.

KEYWORDS

Authentication, Cryptography, Intruder, Multidimensional, Multilevel;

1. INTRODUCTION

Cloud computing offers many cloud services in internet world. Cloud computing can be accessed through its own way. In literature many cloud protocol has been proposed to address many issues in cloud computing. It could be auditing, accounting, authentication, security and etc. However we surveyed many protocols proposed for cloud computing. Firstly, Cloud Gossip Protocol for Dynamic Resource Management [1] 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 [1].In IEEE Transaction on Parallel Distributed Systems[2], 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 [2]. IEEE Transaction on Parallel Distributed Systems [2] proposed an efficient and inherently secure dynamic auditing protocol. It protects the data privacy against the auditor by combining the cryptography method with the bi-linearity property of bilinear paring, rather than using the mask technique [2]. In IEEE conf Access Protocols-2013

[3], they developed nearby share retrieval protocols for single-version systems to improve the read access latency [3]. Cloud Fault Tolerance Protocol [4] proposes a collaborative fault-tolerant transfer protocol for replicated data available on the Cloud and the Grid during exceptional faults [4]. Agent-Based User Authentication and Access Control-2013 [5] 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 [5].In IEEE Nifco [6][7], 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 [6][7]. IaaS Authentication [8] 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 [8]. Graphic Password Authentication [9] depicts as 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 [9]. It is breakable by shoulder surfing attack. Secured Biometric Authentication [10], in 2012, An analyzed the authentication introduced by Das and claimed that the scheme of Das was under various attacks and proposed an improvement [10]. Biometric Authentication [11] Propose an improvement to overcome DOS and Server Spoofing security problems. The security analyses and performance evaluations show that our scheme is more secure and efficient [11]. Complexities are separate device and infrastructure to be placed. RFID based authentication [12], proposed cloud-based RFID authentication scheme enables readers anonymously access the cloud through wired or wireless VPN connections [12]. An encrypted hash table is utilized to prevent clients' (readers and tags) secrets from revealing to the cloud. The first RFID authentication protocol preserving readers and tags privacy against an un trusted database keeper is proposed.[12]. Eid Authentication [13] proposed to close this gap for such cloud applications by applying the STORK framework for secure cloud authentication using eIDs. The STORK framework supports various national eID solutions and will be the relevant eID framework across Europe in future. We demonstrated our approach by enabling eID authentication at two selected public cloud service providers. Finally, we also moved the STORK framework to the cloud to apply the full cloud computing paradigm [13]. Authentication Protocol [14] 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[14] . These protocols and its limitation motivates us to think for new protocol which can take care of authentication, authorization, access control, security, confidentiality and intruder detection/prevention system in a single protocol execution. Hence we proposed secure cloud transmission protocol which can deal with all these issue.

This paper has organized in the following manner: Chapter 2 presents the proposed SCTP and its techniques, Chapter 3, presents the SCTP Petrinet models and its mathematical analysis. Chapter 4 concludes the paper with its limitation.

2. SECURE CLOUD TRANSMISSION PROTOCOL

Proposed secure cloud transmission protocol (SCTP) has its own communication techniques algorithms to achieve strong authentication, security, confidentiality and Intruder detection. SCTP may be a solution to the many issues reported in literature. SCTP has two phases

initialization phase and execution phase as shown in figure 1. As shown in table 1, In initialization phase, SCTP initializes the cloud application with SCTP multi-levels, inputs to generate passwords, questionnaires for intruder detections and etc. In execution phase, it executes all its proposed techniques [15][16][17]. SCTP performs strong authentications, secure channel and intruder detection through its designed techniques which are described in table 2. SCTP techniques research work summary and its significance have been presented in table 3.

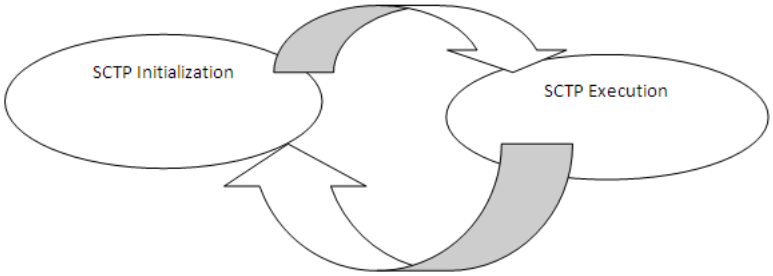

Figure 1. SCTP Phases: Initialization & Execution

Table 1. SCTP Phases and Its Action

Sl no	SCTP Phases	Action
1	SCTP Initialization	It initializes the number of levels, each levels inputs and its types. Number of levels for cryptography, Metadata structure, and key for lock/unlock. Usage profile of genuine users, questionnaires, Risk meter values
2	SCTP Execution	While accessing cloud service it executes 1st technique i.e. Multilevel authentication technique with multidimensional password generation system. Based on cloud service, SCTP switch to 2nd technique i.e. Multilevel cryptography with Metadata and Lock Approach for Storing Data in Cloud or its 3nd Technique i.e. Cloud Services Usage Profile Based Intruder Detection and Prevention System: Intrusion Meter.

Table 2. SCTP Major Three Techniques

Sl No	Techniques	Description
1.	Multilevel authentication technique (MLA) with multidimensional password (MDP) generation system [18][19].	Authentication & Authorization done in multiple levels. Each authentication level uses confidential images and text information to generate multidimensional password.
2.	Multilevel cryptography (MLC) with Metadata and Lock Approach for Storing Data in Cloud[20].	Customer performs data cryptography in multiple levels and in multiple ways. The levels and ways are decided by customer based on their data confidentiality and organizational structure.
3.	Cloud Services Usage Profile Based Intruder Detection and Prevention System: Intrusion Meter (IM) [21].	Cloud usage profile based intruder detection and prevention system is a technique where in which it detects and prevents intruders based on the customer cloud usage profiles. Customer usage profiles prepared based on their regular usage parameters.

Table3. SCTP Technique Research Summary

Sl.#	Significance/ Uniqueness	Literature gap /Benefits
1.	SCTP phases, design, implementation, analysis has described in details [15] [16]. Protocol Engg. Steps from requirements to testing, validation described in details [16]. It analysis SCTP MLA & SCTP MDP for strong authentication. SCTP MLC for secure channel and customer trust [15][16].	Discusses the different attacks resist by proposed techniques of SCTP. Along with strong authentication and secure channel it also resists many attacks discussed in publications. SCTP resist passive attack, man in the middle attack, replay/play back attack and impersonation attack[15]-[16].
2.	Proposed SCTP framework for Cloud specific protocol to achieve Strong Authentication, Secure Channel & Intruder Detection Proposed techniques are mentioned in [17]	SCTP proposed to overcome limitation of existing http protocols & cloud services issues mentioned below. Authentication & Man in the middle attack. No privilege checking while accessing cloud services [17].
3.	MLA technique to authenticate the cloud access in multiple levels. First level for authentication. Second level for particular cloud service authentication. Third level is for privileged access and etc depends on customer requirements, levels could be defined as per security requirements. MLA Applied on wireless sensor cloud. Cloud authentication can be made stronger by keeping multiple levels with corresponding privileges/operations to it. It protects against many active/passive attacks [18][19][20].	It overcome a drawbacks of Single level authentication which grants the full access to customer without checking detailed privileges and etc. If hacker breaks One level it grants the complete system to hacker. It defends against inside attacker by means of multiple level scrutinizes for privileges. It Improves integrity by means of multilevel authentication and authorizations. It prevents the stolen verifier attack and Phishing attack/Masquerade Attack [18]-[20].
4.	According to MDP technique, access to the cloud is authenticated using a multidimensional password. It generates the multidimensional password by considering the many parameter of cloud paradigm such as: vendor details, consumer details, services, privileges and etc. These parameters considered as input dimension. These many dimensions (input) combined together and produces multidimensional password. Here inputs to MDP are confidential images and texts [21].	It overcomes the drawback of textual password issue which is more prone dictionary and brute force attack. It overcomes the drawback of graphical password which is more prone to shoulder attack. It overcomes the drawback of 3D password and biometric password authentication which is more complex and separate device and software required [21].
5.	MLC algorithm applied in customer side against their sensitive data. Before migrating to cloud vendor storage infrastructure customer performs data cryptography in multiple levels and in multiple ways. The levels and ways are decided by customer based on their data confidentiality and organizational structure [22].	It improves the customer trust which is main drawback in cloud computing security. Improves the channel security by means of improved steps on existing cryptography algorithms. It resists impersonation attack, active & passive internet channel attacks, dos attacks and etc [22].
6.	Another features of SCTP i.e intruder detection to detect and prevent intruders in cloud service intrusion based on the cloud service usage profile. In turn, this usage profile helps to detect unusual usage and prevent intrusion [23].	It works better than current signature based detection. It uses detection meter with threshold to detect the intruders. However it is separate problem statements to work on. Hence not considering to current research [23].
7.	SCTP can be applied to e-learning applications which we presented towards improving e-learning and rural education by use of cloud services, virtualization and other latest tools in [25][26][27].	E-learning system have multilevel hierarchy like in college system, principal, subject head and teachers which can adopt by SCTP MLA & MLC[18][21][22].

3. SCTP PETRINET MODEL

Petrinet theory is used in modeling network and protocol [28]. Hence we selected petrinet model in SCTP modeling, later this model helps to derive mathematical expression and easy analysis. This section presents petrinet models for SCTP. Figure 2, presents overview of SCTP which depicts the SCTP techniques and production flow based on different places and transitions. SCTP Starts with its initialization phase then SCTP execution proceed. SCTP MLA derived in places {P0, P1, P2, P9} and Transition {T0, T1, T2, T8, T11}. SCTP MLA Levels P0, P1 and P2 receive MDP from T5, T6 and T7 respectively. States P6, P7 and P8 Generates the MDP passwords. After successful reaching P3 states with 3 token (MDP passwords), based on cloud service types MLC and IM gets executes. SCTP ends at P5 state. Figure 3 presents, detailed Petrinet Model for SCTP which describes detailed techniques of SCTP such as MLA [18], MDP [21] , MLC[22] and IM[23]. Figure 4, presents the petrinet Model of SCTP without notation which helps to derive mathematical expression of SCTP techniques.

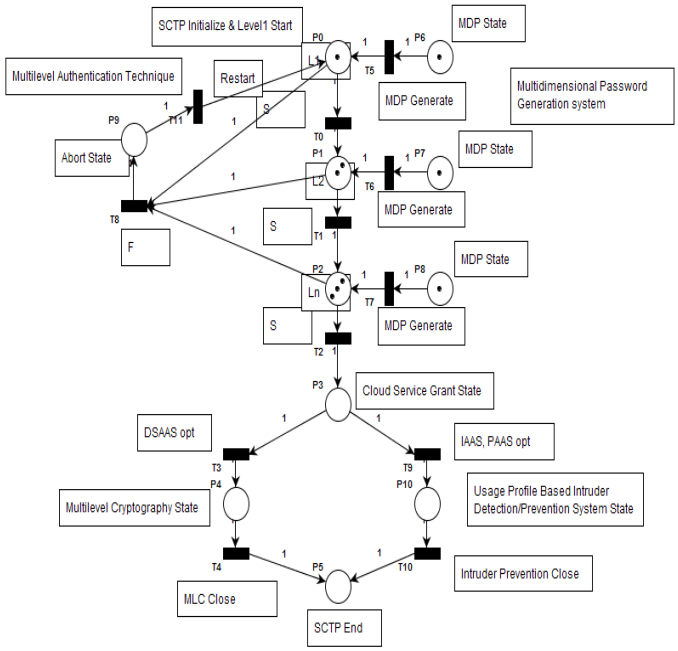

Figure 2. Overview of SCTP

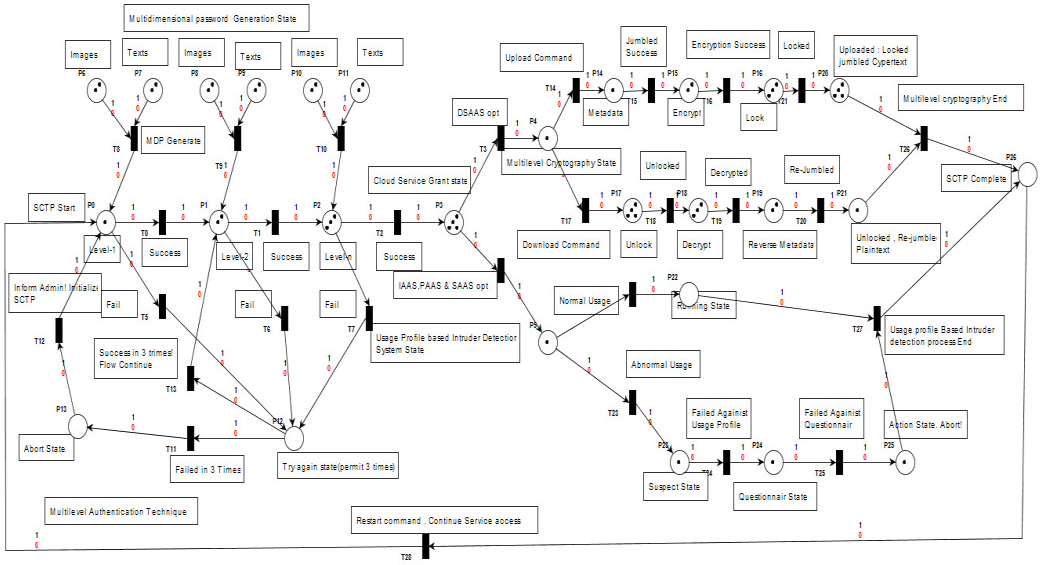

Figure 3. SCTP Detailed Petri net Model

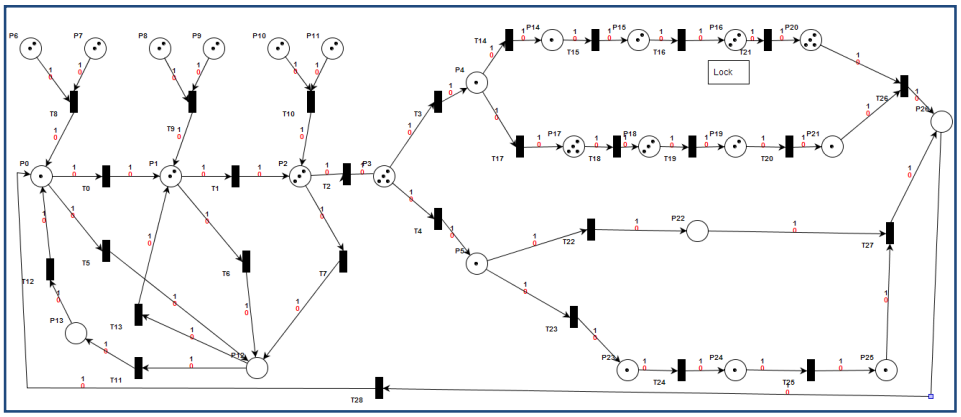

Figure 4. SCTP Detailed Petri net Model without notation

Refer to figure 4, SCTP starts by firing transition T 28 at P0 and ends after firing transition T26 & T27 at P26. Let us derive places and transition for each SCTP techniques discussed earlier, i) A = MLA = {P0,P1,P2,P13,P12} {T20,T0,T1,T2,T5,T6,T7,T11,T12,T13}, ii) P = MDP = {P6,P7,P8,P9,P10,P11} {T8,T9,T10}, iii) C = MLC = {P4,P14,P15,P16,P17,P18,P19,P20,P21} {T3,T14,T15,T16,T17,T18,T19,T20,T26} iv) I = IM = {P5,P22,P23,P24,P25} {T4,T22,T23,T24,T25,T27}. Hence SCTP= { AUPUCUI} {AUP} is to achieve Strong Authentication, C to achieve Secure Channel, I to ensure Intruder Detection and Prevention.

DETAILED ANALYSIS

A Petri net graph is a 4 tuple (S,T,W,M0) where S is a finite set of places represents states/conditions, T is a finite set of transitions represents action/execution. S &T are disjoint, that means no object can be both a place and a transition. W:(S x T) U (T X S) -> N is a multiset of arcs, i.e. it assigns to each arc a non-negative integer arc multiplicity. Refer to figure 3, N represents SCTP. No arc may connect two places or two transitions. The flow relation is the set of arcs, F={(x, y)| W(x, y) > 0}. In texts often define Petri nets using F instead of W. When using this convention, a Petri net graph is a bipartite multigraph (S U T, F) with node partitions S and T. The preset of a transition t is the set of its input places: t={s € S | W(s, t)>0}; its postset is the set of its output places: t={s € S | W(t, s)>0}. SCTP each techniques places and transition described in figure 3. M0 is the initial marking, a marking of the Petri net graph. Firing a transition t in a marking M consumes W(s,t) tokens from each of its input places s, and produces W(t,s) tokens in each of its output places s. SCTP each techniques tokens described in figure 3. We are generally interested in what may happen when transitions may continually fire in arbitrary order. A firing sequence for a Petri net with graph G and initial marking M0 is a sequence of transitions σ =<ti1...tin> such that M0--> G,ti1 M1^...^Mn-1 --> Mn.

Formulation in terms of vectors and matrices, its transition relation can be described as a pair of |S| by |T| matrices

- W^-, defined by ∀s,t:W^-[s, t] = W(s, t)
- W^+, defined by ∀s,t:W^+[s, t] = W(t, s)

The set of firing sequences is denoted as L(N). Firing sequence of SCTP techniques A, C & I are derived below.

A= (P0,T0,P1,T1,P2,T2)
C =(P4,T14,P14,T15,P15,T16,P16,T20)
I = (P5,T23,P23,T14,P24,T25,P25,T27)

Then their difference $W^T = W^+ - W^-$ can be used to describe the reachable markings in terms of matrix multiplication, as follows. For any sequence of transitions w, write 0(w) for the vector that maps every transition to its number of occurrences in w. Then, we have R(N)={M | ∃w:M=M0 + WT . 0(w)^w is a firing sequence of N}.

SCTP MLA, MLC and IM reachability and technique firing sequence derivations illustrated in table 4.

Let us apply probability and analyze the failure of SCTP technique execution. Let us take SCTP as sample space S , its techniques(A,C & I) firing sequence as mutual disjoint subsets A1, A2, A3, E are events (executions) and subset of S for technique execution. S= A U A2 U A3 Then E =E ∩ S, => E ∩ (A U A2 U A3) => (E ∩ A1) (E ∩ A2) (E ∩ A3). Since E ∩ A are disjoint we obtain P(E)= P(E ∩ A1)+ P(E ∩A2)+P(E ∩ A3), using multiplication theorem we obtain, P(E ∩A3)=P(A3 ∩ E)= P(A3)P(E\A3). Thus we arrive total probability P(E)= P(A1)(P(E\A1)+ (P(E\A2)+ (P(E\A3). Let us apply bayes theorem k =1,2,3 the multiplication theorem for conditional probability tells that P(Ak ∩E)=P(Ak)P(E|Ak). Therfore P(Ak|E) = P(Ak ∩E)/P(E) => P(Ak)P(E/Ak)/P(E) use law of total probability for denominator P(E). Hence , P(Ak/E)= P(Ak)P(E/Ak)/ P(A1)(P(E\A1)+ (P(E\A2)+ (P(E\A3).

Considering MLC upload and MLC download independent events as P (A∩B) = P (A) P (B)

Table 4 . SCTP Techniques firing sequence matrix analysis

A = MLA	C = MLC (Upload)	I = IM/IDP (Abnormal usage)
W^- = T0 T1 T2 P0 1 0 0 P1 0 1 0 P2 0 0 1 W^+ = T0 T1 T2 P0 0 1 1 P1 1 0 1 P2 1 1 0 W^T = T0 T1 T2 P0 1 -1 -1 P1 -1 1 -1 P2 -1 -1 1 M_0 = {1,2,3}	W^- = T14 T15 T16 T20 P4 1 0 0 0 P14 0 1 0 0 P15 0 0 1 0 P16 0 0 0 1 W^+ = T14 T15 T16 T2 P4 0 1 1 1 P14 1 0 1 1 P15 1 1 0 1 P16 1 1 1 0 W^T = T14 T15 T16 T20 P4 1 -1 -1 -1 P14 -1 1 -1 -1 P15 -1 -1 1 -1 P16 -1 -1 -1 1 M_0 = {1,2,3,4}	W^- = T23 T14 T25 T27 P5 1 0 0 0 P23 0 1 0 0 P24 0 0 1 0 P25 0 0 0 1 W^+ = T23 T14 T25 T27 P5 0 1 1 1 P23 1 0 1 1 P24 1 1 0 1 P25 1 1 1 0 W^T = T23 T14 T25 T27 P5 1 -1 -1 -1 P23 -1 1 -1 -1 P24 -1 -1 1 -1 P25 -1 -1 -1 1 M_0 = {1,1,1,1}

4. CONCLUSION AND LIMITATION

SCTP techniques to achieve cloud specific strong authorization and authentication, secure channel and intruder has been designed. SCTP MLA & MDP to ensure strong authentication, SCTP MLC to achieve strong authentication and SCTP IM to achieve usage profile based intruder detection & prevention has been designed. SCTP techniques complete design has been presented using Petrinet production model. SCTP petrinet models and its analysis are presented. SCTP performance analysis has been made to compares with existing techniques that are proposed to achieve authentication, authorization, security and intruder prevention. SCTP designed to protect against different attack mentioned in literature. SCTP can be used in cloud application where it needs higher security such as defense, military, university marks database

and etc. Simpler application and generic application may not be required such a strong authentication, secure channel and intruder detection as it leads to unnecessary complexity.

ACKNOWLEDGMENT

Our sincere thanks to Dr. Karisiddappa, Vice Chancellor and Dr. H. N. Jagannatha Reddy, Registrar VTU Belagavi, for their constant encouragement & support.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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

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

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

[10] Z. J. Zhu, Z. W. Gao, Y. Li, A SECURE BIOMETRIC-BASED AUTHENTICATION SCHEME USING SMART CARD,IEEE, H. B. Tang39-43,2013.

[11] 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.

[12] 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.

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

[14] Safiriyu Eludiora1, Olatunde Abiona2, et. al, A User Identity Management Protocol for Cloud Computing Paradigm , in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163

[15] 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

[16] Dinesha H A, Dr.V.K Agrawal, "Development of Secure Cloud Transmission Protocol (SecCTP) Engineering Phases: Multilevel Security & Cryptography", International Journal on Cryptography and Information Security (IJCIS) ISSN: 1839-8626, December 2015.

[17] 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.

[18] 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.

[19] R. Monica, Dinesha H A, Dr.V.K Agrawal, "Wireless Sensor-Cloud Integration Using Ant Colony Routing Algorithm", International Conference on cloud computing and service engineering (CLUSE2012), held at Raja Rajeshwari College of Engineering & KINGSTON, UK, 11-13 April 2012, 294-298, Received Best Paper Award, Referred to ISEEC Journal.

[20] Dinesha H A, R Monica and V.K. Agrawal, "Formal Modeling for Multi-Level Authentication in Sensor-Cloud Integration System". International Journal of Applied Information Systems 2(3) (IJAIS) Published by Foundation of Computer Science, New York, USA, May 2012, 16-21.

[21] 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.

[22] Dinesha H A, Dr.V.K Agrawal, "Multilevel Cryptography with Metadata and Lock Approach for Storing Data in Cloud", Springer Journal of Cryptographic Engineering (JCEN) (submitted).

[23] Dinesha H A, Dr.V.K Agrawal, "Usage Profile Based Intruder Detection System for accessing cloud service", Transactions on Networks and Communications, Volume 2, Issue 6, 10.14738/tnc.26.590. Dec 2014.

[24] Ms. R Monica, Mr.Dinesha H.A,Prof.V.K Agrawal, "Cloud Computing – Phone Call as a Service: A Concept", to IEEE Internl.. Conference on Advances in Computing, Communications and Informatics (ICACCI-2013), 978-1-4799-2432-5, 13861185, 22-25 Aug. 2013, 236 – 242.

[25] Abhishek A, Dinesha H A, Dr. V. K Agrawal, "Cloud Computing Technologies in Indian Rural Schools and Engineering College Education " , International conference on Intelligent computational systems (ICICS's2012), Dubai, January7-8, 2012, 67-70.

[26] Dinesha H A, Dr. V. K Agrawal, "Advanced Technologies and Tools for Indian Rural School Education System", International Journal of Computer Applications (IJCA) (0975 – 8887) Volume 36– No.10, December 2011, 54-60.

[27] Dinesha H A, Dr. V. K Agrawal, "Virtualization Technologies and Techniques in Education Learning Applications ",International Conference on e-Education and e-Learning ICEEEL, held at World Academy of Science, Engineering and Technology, PARIS-FRANCE on November 14-16, 2011, 984-991.

[28] Petri, Carl Adam; Reisig, Wolfgang (2008). "Petri net". Scholarpedia 3 (4): 6477. doi:10.4249/scholarpedia.6477.

[29] 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.

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

AUTHORS

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 & CO**RI 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,

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 Professor CSE & Dean (Research and Skill), Belagavi.