A Study of User Authentication Techniques in Cloud Computing

[1]G. Kumaresan, [2]N. Veeraragavan, [3]Dr. L. Arockiam
[1,2]Research Scholar, [3]Associate Professor

Department of Computer Science,
St. Joseph's College (Autonomous), Tiruchirappalli, TamilNadu, India

***Abstract*—Major challenges in cloud computing are security and privacy because of its multi-tenancy nature and the subcontracting of infrastructures. Enterprises, government organizations and educational institutions are quickly accepting cloud services for their businesses. Cloud events need to be developed so that these organizations can be assured of security in their businesses and can choose an appropriate vendor for their computing needs. Various malicious activities from illegal users such as data misuse, strict access control and limited checking may result into harmful or illegal access of critical and private data of these cloud users. In this work, the researchers present a brief view of user authentication techniques in cloud computing environment.**

***Index Terms*— Multifactor Authentication System; Cloud Service Providers; Shared authority based privacy preserving protocols; HMAC**

I. INTRODUCTION

Cloud computing is a distribution of standard computing services where dynamically accessible and virtualized resources are delivered as a service across the internet. The Cloud services deliver lot of advantages especially in ubiquitous services, in which everybody can access computing services provided over Internet. Besides many assistances that the cloud computing has presented, the information security is the major barrier which makes the user worried of. According to the NIST definition, [1] cloud computing is a delivery model that enables convenient instant network access to a pool of shared configurable computing resources that can be quickly provisioned and released. Cloud model supports availability of resources and has many characteristics such as on-demand self-service distributed network access, resource pooling measured service and rapid elasticity.

II. CLOUD COMPUTING

Cloud computing comprises of three typical service standards that include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). It instances can be operated and exploited according to four different deployment models such as private cloud, public cloud, hybrid cloud and community cloud [2][3]. Cloud computing delivers various services over web such as information storage and infrastructure. Cloud service providers provide applications and computing resources through internet, in which they can be accessed anywhere using web browsers, desktops and mobile applications. Cloud computing delivers software as a service through Internet. Cloud computing is a web based model in which more than one system is connected in the distributed environment for enabling suitable, instant network access to a shared computing resources [1]. Cloud reduces the requirement of installing and executing the application on the user personnel computers. Platform as a Service is an instant platform service to deploy consumer applications [2][4] and [5]. Cloud Service Provider must ensure the security of their consumer's information and must be responsible for any security threat that would affect their customer's service infrastructure. Cloud service provider deals with many services that can help its consumers such as fast access to their data from anywhere, scalability, pay-per-use, data storage, data recovery, prevent against intruders, instant safety controls and the use of internet and infrastructure services [6].

III. CLOUD COMPUTING ISSUES

Cloud Service Providers offer aids to users but security threats post an important role in the cloud environment [7]. Basically users who use online information sharing or network services are aware of the potential loss of confidentiality [8]. In latest IDCI analysis [9][36] 74% of IT executives and CIOs specified that security is the major issue of extreme concern in any cloud computing infrastructure. User data moving to clouds large data centers may involve many security risks and challenges [10] such as virtualization accessibility, confidentiality and issues related to information retrieved from a third party, truth of data, reliability, and data loss or data theft. In Early research, few authors discuss [11][12] the security issues as information storage safety, application safety, information sharing safety and network security related to third-party resources. Different kinds of cloud service models have different security concerns between consumers and service providers in distributed environment.

Amazon [13][14] provides their elastic computing cloud address physical environmental and virtualization security whereas the users might be aware of the security of the IT systems, including the operating systems, applications and data security. Cloud computing services have been constructed through the web, any issue that is related to web security will also affect cloud

services. Moreover, the cloud resources are accessed over the internet subsequently even if the cloud providers concentrate on security in the cloud environment. So the user data is still transferred through network which leads to unreliability.

So, the purpose of this work is to analyze and learn the existing authentication techniques in the cloud environment. It analyzed the recent existing papers for user authentication and control to access cloud services from cloud server.

IV. REVIEW OF LITERATURE

Authentication is a simple task where one party offers a set of permissions to a system. If the user name and password matches on the system, it returns a value which indicates that the permission has been granted.

Wenyi Liu et al. proposed a Multi Factor Authentication system via more than one factor [15]. Multi Factor Authentication has become an increasingly essential component for cloud systems. It ensures the legitimate users' access to their own protective information. In this paper the authors introduce a design of MACA. The system collects the user behavior as a second authentication factor along with the user password (First authentication factor). However unlike traditional user behavior profiling, the information gaining, spread and storage all occur in a privacy preserving system. This system can successfully validate legitimate users while identifying pretender in author's data sets.

Rohitash Kumar Banyal et al. proposed a new multifactor authentication system framework [16] for cloud computing environment. The proposed system framework has been verified by developing Cloud Access Management (CAM) pattern which authenticates the user based on multiple factors. User's secret dreadful data and encrypted value of arithmetic captcha is innovation factor for user authentication for cloud computing infrastructure. Protocol model for personnel cloud server is implemented using open source technology. So, the proposed work shows the closest contract with the standard conditions for cloud security.

Daniel Mouly et al. proposed [17] one of the most popular and mature remote user authentication schemes in which, the server sliced the value of a user passwords. In Lamport framework, it defines that the password table was used to verify the truth of authenticated user but if this password table is stolen or modified by an opponent then the system could be entirely compromised. In latest smartcard based password authentication works are based on three key sharing protocol. Smartcard is used to keep in reserve the everlasting secret key and is assumed that the smartcard is never accepted by the unwanted users. When compared to the lamport work, this smartcard authentication seems to be better.

Tapalina Bhattasali et al. proposed a two factor remote authentication in healthcare system [18]. In factor one authentication, keystroke analysis is proposed where raw data are collected first, then processed data are stored and trust scores are created. End user gets trust score at each factor of authentication and decision is taken based on final faith score of end user. Performance analysis of the proposed appliances shows its efficiency to authenticate end users.

Liliana F.B. Soares et al. proposed [19] a model that aims at decreasing the impact of the aforesaid threats by engineering a cloud infrastructure for carrying out authentication on cloud management interfaces. The infrastructure is stimulated on whonix architecture, and controls are placing in a Virtual Machine, a proxy gateway between the connection to the outside and the management interface on another Virtual Machine. The proxy gateway arbitrates access to and conceals the inner Virtual Machine transparently advancing traffic. This approach is useful for attaching capricious security controls to the proxy gateway as desired, so as to scrutinize the traffic to inhabitant attacks. A first factor of authentication can be setup on the proxy gateway, and only then access to the management boundary would be provided, on which more factors could be assessed. Both Virtual Machines are protected by an isolated private virtual network in the proposed system.

Maslin Masrom et al. proposed a model for graphical password authentication [20] that provides a different kind of solution to text based authentication, appreciated by the truth that humans can recall photos better than text information. In recent years many network systems and web based infrastructures try to use graphical authentication techniques. All the graphical passwords have two different characteristics, flexibility and security. None of the algorithms were able to cover these characteristics at a time. But this paper describes the recall based algorithms in graphical password authentication in which each of the threats and attacks are identified. The most common shortages for remember based algorithms are then identified and described.

Maslin Masrom et al. proposed a model for graphical password authentication [20] that provides a different kind of solution to text based authentication, appreciated by the truth that humans can recall photos better than text information. In recent years many network systems and web based infrastructures try to use graphical authentication techniques. All the graphical passwords have two different characteristics, flexibility and security. None of the algorithms were able to cover these characteristics at a time. But this paper describes the recall based algorithms in graphical password authentication in which each of the threats and attacks are identified. The most common shortages for remember based algorithms are then identified and described.

Arcangelo Castiglione et al. proposed [22] a highly secure one time authentication protocol depending on two cryptographically robust building blocks, namely the authenticated key interchange and Hash Message Authentication Code (HMAC). They provides several benefits with respect to an attribute. It enables obvious mutual authentication between two endpoints. In addition, key setup, key scheduling and key update operations are performed by both endpoints without message among them thus ensuring the full freedom by any Trusted Third Party. The proposed protocol is cryptographically safe against most of the one-time password attacks.

Viktor Taneski et al. proposed a systematic literature analysis of readings in the area of password usage and safe [23]. The analysis is classified in the articles of the reputed journals and conference papers written in English and published between 1979 and 2014. The search is lead through IEEE explore, Science Direct, Springer Link and ACM Digital Library.

FarazFatemi Moghaddam et al. discussed an agent based user authentication model to increase the reliability and security of user identity management in cloud computing environments [24]. The suggested model uses a unique installed extension in the web browser of user's registered devices. The individuality of the extension enhances the security of user authentication process by avoiding starting authentication in cloud before receiving suitable verification. Furthermore, a method for provisional accessing from unregistered devices was suggested regarding the combination of two strings in second verification code. In addition, the

proposed model was estimated on three main parameters- performance, security and scalability. The theoretical analysis shows that this model enhances the rate of security and reliability in cloud computing environments without affecting the rate of energy and time investing and scalability.

Chao Shen et al. proposed [25] a mouse dynamics, a method of finding individual user depends on their mouse functioning features. Even though earlier work has reported some encouraging results, mouse dynamics is still a newly developing technique and has not touched the acceptable level of performance. The main reason for this essential behavioral inconsistency. This review delivers a novel approach by using pattern growth based mining method to extract frequent behavior sectors in reaching firm mouse features, the classification algorithms to implement the task of continuous user authentication. This paper displays the mouse characteristics extracted from frequent behavior partitions that are much more steady than those from complete activities. These results suggest that mouse dynamics suit t for a traditional authentication scheme.

Joseph Bonneau et al. suggested a framework for assessing two periods of schemes to exchange text passwords for common purpose user authentication on the internet using a wide-range set of twenty five usability and security advantages that a perfect scheme might deliver [26]. The author's survey is also broad including password controlling software combined login protocols, graphical password systems, perceptive authentication patterns, one time passwords, hardware tokens phone assisted patterns and biometrics schemes. Author's broad approach leads to crucial ideas about the difficulty of switching passwords. No known pattern come close to providing all desired aids none even recalls the full set of advantages that truthful passwords already deliver. There is an extensive range from system involvement slight security advantages beyond truthful passwords, to those present main security benefits in return for being more expensive to deploy or more hard to use. Authors described that many academic schemes have failed to gain power because researchers rarely consider an enough broad real world limitations. Outside our analysis of present systems, this work presents the evaluation approach and regular for future internet authentication proposals.

Celeste Lyn Paul et al. discussed a field study of 24 contributors above 10 weeks travelled user behavior and sensitivities in a smartcard authentication scheme [27]. Ethnographic systems used to collect data including journals, reviews, meetings and field explanations. We perceived a number of issues like users practically knowledgeable while they combined smartcards into their task procedures. Readers who dis-remember to use smartcards to authenticate adopt digital signatures and encrypted. The extreme observed advantage was the use of an easy recollect Personnel Identification Number in replacement of difficult passwords. The highest observed disadvantage was the lack of smartcard sustained applications. In general, most members had an assured knowledge using smartcards for user authentication.

Zach Jorgensen et al. discuss [28] the idea of using one user behavior with an indicating device, such as a touchpad or a mouse, as a behavioral biometric for authentication purposes. It has intelligently increased attention to the past period. A number of interesting tactics based on the idea have developed in the literature review and encouraging experimental results have been reported. However, the authors argue that boundaries in the past experimental assessments of these tactics increase questions about their true efficiency in a theoretical setting. So, this paper reviews existing authentication tactics based on mouse dynamics and shed light on some important boundaries regarding the effectiveness of these tactics that has been evaluated in the past. The authors show the results of several trials that they conducted to determine our observations and recommend guidelines for estimating future authentication tactics based on mouse dynamics.

Amit K. Awasthi et al. discuss about in the year 2000, Hwang and Li proposed a framework for new remote user authentication pattern using smart cards [29]. Chan and Chang presented the masquerade hacker that is successful on this scheme. Shen, Lin and Hwang mention that a different type of attack on this scheme and presented an improved system to eliminate these mistakes. Leung et al. presented that this modified scheme is still in danger to the attack suggested by Chan and Cheng. Furthermore, they presented that the continued attack suggested by Chang and Hwang also works well in this method. Kumar have recommended the idea of check digits to overcome the above mentioned attacks in the pattern. This paper proposes a new pattern by using check digits which also overcomes these mentioned attacks and is more effective than kumar pattern.

Shraddha M. Gurav et al. proposed a model for graphical password authentication which is one of the further solutions to alphanumeric password [30]. It is very boring process to recall alphanumeric passwords. It is presented with user friendly authentication, easy to entrance and use that application. The main purpose behind this scheme is human mind can easily recall photos than letters or numbers. This paper represents the authentication by using graphical password. It also suggested that cloud with graphical security by worth of image password. It gave an algorithm that is usually based on user name and photos as a password. These authors try to deliver a set of pictures on the basis of letters series location of characters in user name.

Hong Liu, et al. proposed a method as a pervasive data cooperate with each other pattern to understand user's data that are remotely stored in an online cloud central data server [31]. Existing security solutions mainly pay attention on the authentication to understand a user's private data. They cannot be unrestricted call up but abandonment an indirect privacy issue for the duration of a user challenging the cloud data server to request other users for data distributing. The admission request itself may state the user's secrecy. The author presented a distributed authority based on privacy preserving authentication protocol to address privacy issue for cloud storage. The protocol is defined as 1) distributed access specialist is achieved by anonymous access request matching with security and privacy reflections (e.g., authentication, data confidentiality, user secrecy and advancing security)

2) quality based access control is recognized to understand that the user can only access its own data arenas 3) proxy encryption is applied by the cloud data server to deliver data distribution among many users. In the meantime, universal ability model is conventional to prove that the SAPA preferably has the scheme accuracy. It shows that the recommended protocol getting privacy preserving data access expert sharing is a pretty for multi-user collective cloud applications.

A. Mercy Gnana Rani et al. discuss the cloud computing in various services which include storage platform and very easy to get to maximum calculation [32]. Due to minimum cost, strong point, elasticity and multi-tenancy nature, cloud computing changes the route objects to manage their own data. In cloud computing environment, now-a-days, safe outsourcing is one of the active research areas, as the cloud environment can't be reliable. The situation becomes more complex when the ubiquitous data sources in a cloud

computing environment are assured with multiple outsourcers who are available with different access permission. Session key management is one of the important aspects for safe outsourced data in cloud computing environment. In this paper, a new encryption protocol called Key Insertion and Splay Tree encryption are proposed. This algorithm makes use of an asynchronous key series and splay tree for encryption. This encryption model provides better key management approach for validating the users in the cloud environment. The experimental result displays that it is very efficient in providing authentication and security to the distributed cloud data.

Nimmy K. et al. proposed a model for appropriate authentication that is a necessary technology for cloud computing atmospheres in which the links to outside atmospheres are same and threats are high [33]. The authors present a new model for mutual authentication where the cloud data server and users can authenticate each another. The procedure is designed and it uses steganography as a further encryption pattern. The pattern achieves authentication using secret sharing. Secret sharing permits a part of the secret to be kept back in two sides and when they joined, it becomes the complete secret. The secret holds information about two parties that are involved. Further authentication has been used which delivers further safety. The proposed procedure delivers session key setting up and mutual authentication between the cloud server and users and also the users have been given the mobility to change the password. In addition, the robust security features makes the procedure well suited for the cloud computing atmosphere.

Navneet Singh et al. discuss the cloud computing as a recent trend for its multi tenancy based gain access to software but with the transmission in development of travelling from dedicated IT infrastructure to using the services of a cloud provider makes the issue of security more scornful [34]. Most solutions are delivered for security of a code when it is accessed through a network but still the cloud provider are facing the risk of defending the application from complication, manipulation and damaging. Watermarking is a solution for defending from prohibited access that has been predictable as a solution for a network based applications. This application will only be retrieved using key delivered through encryption code. This paper provides a model that will defend a code while using it on a cloud computing environment i.e. on cloud application data servers by executing an outline for cloud security in cloud computing environment. Kerberos procedure that forms a dominion of authentication server and ticket permitting server with back end database connectivity for handling user's passwords and using the custom class loader for honest user who needs entree to the application.

V. COMPARATIVE STUDY ON EXISTING USER AUTHENTICATION TECHNIQUES IN CLOUD COMPUTING

Table 1 Existing User Authentication Techniques

S.No	Author Name	Issues	Algorithms/Tools/Methods	Results
[15]	A. Wenyi Liu et al.	Multi Factor Authentication	Fuzzy Hashing Encryption Algorithm	In this system successfully validate legitimate users while identifying pretender in our data sets.
[16]	Rohitash Kumar et al.	Secret Splitting Data	CAM Tool	Close Contract with the standard conditions for security.
[17]	Daniel Mouly et al.	Data Security	Three Part Key Distribution Protocol	Smart Card is never compromised with the previous Password table.
[18]	Tapalina Bhattasali et al.	Key stroke Analysis	K means clustering Algorithm	Performance analysis of the proposed appliances shows its efficiency to authenticate end users.
[19]	Liliana F.B. Soares et al.	Single Sign On	Whonix Tool	Virtual machines are protected by an isolated private virtual network.
[20]	Maslin Masrom et al.	Graphical Authentication	Syukri Algorithm	It is prove that, It is better than text based authentication scheme.
[21]	Jiangsham Yu et al.	Three Factor Authentication	Fuzzy Vault	The analysis of proof show that the three factor scheme is secure and privacy preserving technique.
[22]	Arcangelo Castiglione et al.	One Time Authentication	OTP Protocol	This protocol cryptographically secure, standard civilizations against most of the already known One Time Password attacks

[23]	Viktor Taneski et al.	Data Security	Analysis Tool	The search is conducted through IEEEXplore, Science Direct, Springer and ACM Digital Library.
[24]	Faraz Fatemi Moghaddam et al.	Scalability	Second Pass word Algorithm	Theoretical analysis shows that security and reliability in cloud without affecting energy and time ingesting, scalability.
[25]	Chao Shen et al.	Continuous Authentication	Mouse Behavior Pattern Mining Method	FAR-7.78%, FRR-9.45% Time-5 minutes
[26]	Joseph Bonneau et al.	Replacing the text passwords for general purpose user authentication	Visual Crypto-Pass window Graphical-Pass no	Analysis Report for Usability,Deployability and Security
[27]	Celeste Lyn Paul et al.	Perceptions in smart card authentication	Ethnographic methods	Analysis of Qualitative data
[28]	Zach Jorgensen et al.	Mouse dynamic authentication low error rates and recurring problems	Remote access scenario, detecting device type controlled environment	Better than previous mouse dynamic authentication system
[29]	Amit K. Awasthi et al.	Remote user authentication pattern using smart cards	Huwag Pattern Shen Lin Hwang	Get the Modify the HWWAG SCHEME and check digits overcome the previous attacks
[30]	Shraddha M.Gurav et al.	Graphical Password Authentication	Selection Algorithm	Easily remember password and High Protection
[31]	Hong Liu, et al.	Shared Authority based Authentication	Privacy preserving authentication protocol	Guarantee Data confidentiality and Data Integrity
[32]	A.Mercy Gnana Rani et al.	Data Outsourcing in cloud	Key Insertion Algorithm, Tree Encryption Algorithm	Better Key Management, Very efficient in providing authentication & security to the cloud data
[33]	Nimmy K et al.	Secret Sharing & Steganography	Novel Mutual Authentication Protocol	Strong security benefits makes the protocol well suited for cloud computing environment
[34]	Navneet Singh et al.	Software protection in cloud computing	Kerberos Protocol	Provide Strong Authentication

VI. MOTIVATION

The user authentication techniques are reviewed in the cloud computing environment. In general, this paper includes some surveys conducted by International Data Corporation that shows the motivation for the adoption of cloud computing. This work identifies the user authentication issue and the solution to overcome these problems. So the main motivation for the research paper survey is to analyze a secure user authentication technique in cloud computing environment.

VII. CONCLUSION

The result of the review shows that the computer science research community has not made very good authentication techniques to be available in the cloud computing environment. This survey elaborately examines the technologies and techniques. It deals with the above direction and also need to study more on user authentication techniques and prevention methods in cloud computing environment.

REFERENCES

[1] Mell .P Grance T. The NIST definition of cloud computing versiong 15 technical report. computer and information Sciences, 53(6), 2009, pp.1-10.

[2] Vaquero. L,Rodero-Merino,L,Caceres, J,and Lindner, M, A break in the clouds toward a cloud definition. ACM sigcomm Computer communication review, 39, 2009, pp.50-55.

[3] Lee Badger,Robert Bohn,Shilong Chu, Mike Hogan, Fang Liu, Viktor Kaufmann and Jian. useful information for cloud adopters. NIST cloud computing program, 2(1), 2011, pp.1-73.

[4] Buyya. R, Yeo, C and Vengopal, S, market oriented cloud computing vision, hype, and reality for delivering IT services as computing utilities, proceedings of the 10th IEEE international conference on high performance computing and communications, 2008, pp.5-13.

[5] Buyya. R., Yeo. C, Venugopal. S, Broberg. J, and Brandic, I. cloud computing and emerging IT platforms vision hype and reality for delivering computing as the 5th utility. Further generation computer systems, 25, 2009, pp.599-616.

[6] Subashini S, Kavitha V " A survery on security issues in service delivery models of cloud computing", Journal of network and computer applications, 2011, pp.1-11.

[7] Viega J, cloud computing and common man, Computer, 42(8), 2009, pp.106-08.

[8] Cachin. C, Keidar. I and Shraer, A trusting the cloud, ACM sigact news, 40(2), 2009, pp.81-86.

[9] S. Lee, I. Ong, H.T. Lim, H.J. Lee, "Two factor authentication for cloud computing", International journal of kimics, vol 8, 2009, pp. 427-432.

[10] Wang C, et al. Ensuring data storage security in cloud computing, Proceedings of the 2009 17th International Workshop on Quality of Service (IEEE), 2009, pp.1-9.

[11] Michael E.Whitman In defense of the realm: Understanding the threats to information security International Journal of Information Management, 24, 2004, pp.43-57.

[12] Dimitrios Zissis , Dimitrios Lekkas,Addressing cloud com-putting security issues Future Generation Computer Systems, 28, 2012, pp.583-592.

[13] Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A,Licciardi A, et al. Security guidance for critical areas of focus in cloud computing, Cloud Security Alliance, 25, 2009, pp.1-177.

[14] Ristenpart T, et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, Proceedings of the 16tj ACM conference on computer and communication security (ACM), 2009, pp.199-212.

[15] A. Wenyi Liu, Selcuk Uluagac, and Raheem Beyah, "MACA: A Privacy-Preserving Multi-factor Cloud Authentication System Utilizing Big Data,"in IEEE INFOCOM Workshop on Security and Privacy in Big data 2014, pp.518-523.

[16] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain, "Multi factor authentication framework for cloud computing", in Fifth international conference on computational intelligence, modelling and simulation 2013, pp.105-110.

[17] Daniel Mouly: Strong User Authentication, Information Systems Security, 11:2, 2002, pp.47-53.

[18] Tapalina Bhattasali, Khalid Saeed, "Two Factor Remote Authentication in Healthcare", in International conference on advances in computing,communications and informatics,2014, pp.380-386.

[19] Liliana F. B. Soares, Diogo A. B. Fernandes, Mario M. Freire and Pedro R. M. Inacio, "Secure User Authentication in Cloud Computing Management Interfaces", 2013, pp.78-79.

[20] Maslin Masrom, Farnaz Towhidi and Arash Habibi Lashkari, " Pure and Cued Recall-Based Graphical User Authentication ", 2009, pp.40-45.

[21] Jiangshan Yu, Guilin Wang and Yi Mu , " An efficient generic framework for three-factor authentication with provably secure instantiation " IEEE Transactions On Transaction Forensics and Security, Vol 9, issue 12, December 2014, pp.2302-2313.

[22] Arcangelo Castiglione, Alfredo De Santis and Francesco palmieri, " An efficient and transparent one time authentication protocol with non interactive key scheduling and update ", IEEE 28th International Conference on Advanced Information Networking and Applications, 2014, pp.351-358.

[23] Viktor Taneski, Marjan Hericko and Bostjan Brumen,"Password Security-No Change In 35 Years?", in MIPRO, May 2014, pp.1360-1365.

[24] Faraz Fatemi Moghaddam, Nasrin Khanezaei and Sina Manavi,"UAA: User Authentication Agent for Managing User Identifies in Cloud Computing Environments", IEEE 5th Control and System Graduate Research Colloquium, August 2014, pp.208-212.

[25] C. Shen, Z. Cai, and X. Guan, "Continuous authentication for mouse dynamics: A pattern-growth approach," in *42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2012, pp. 1-12.

[26] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, " the quest to replace passwords : a framework for comparative evaluation of web authentication schemes ",in *proc. of the IEEE symposium on security and privacy*, 2012, pp.553–567.

[27] C. Paul, E. Morse, A. Zhang, Y.-Y. Choong, and M. Theofanos, " a field study of user behavior and perceptions in smart card authentication ", in *Human-Computer Interaction INTERACT*, ser. Lecture Notes in Computer Science Springer, vol. 6949, 2011, pp. 1–17.

[28] Z. Jorgensen and T. Yu, " on mouse dynamics as a behavioral biometric for authentication " ,in *proc. of the 6th ACM symposium on information, computer and communications security*, 2011, pp.476–482.

[29] M. Kumar, " new remote user authentication scheme using smart cards ", *consumer electronics, IEEE Transactions on*, vol. 50, 2004, pp.597–600.

[30] ShraddhaM. Gurav, et al, "Graphical Password Authentication", in International conference on Electronic Systems, Signal Processing and computing technologies, 2014, pp.479-483.

[31] Hong Liu, et al.," Shared authority based privacy-preserving authentication protocol in cloud computing " , in IEEE Transactions on Parallel and Distributed Systems, 2013, pp.1-11.

[32] A. Mercy Gnana Rani, et al, "Key insertion and splay tree encryption algorithm for secure data outsourcing in cloud", in world congress on Computing and Communication Technologies, 2014, pp.92-96.

[33] Nimmy K. et al, " Novel mutual authentication protocol for cloud computing using secret sharing and steganography", 2014, pp.101-106.

[34] Navneet Singh et al., " An efficient approach for software protection in cloud computing ", in Fourth International Conference on Communication Systems and Network Technologies, 2014, pp.550-554.

[35] B,P, Rimal, Choi Eunmi, I. Lumb, " A taxonomy and survey of cloud computing systems ", in International Joint Conference on INC, IMS and IDC, Aug 2009, pp. 44-51.