IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 05, pp. 2431-2437, May, 2016

Research Article

SSQS AND OTP BASED USER AUTHENTICATION MECHANISM IN CLOUD COMPUTING

***Ankit Dhamija and Deepika Dhamija**

Assistant Professor, Amity Business School, Amity University Gurgaon

ARTICLE INFO

Article History:

Received 21st February 2016
Received in revised form
19th March 2016
Accepted 22nd April 2016
Published online 30th May 2016

Keywords:

Authentication,
Cloud, Security,
OTP, Password.

ABSTRACT

Dietary Cloud computing provides a plethora of services and applications and platforms to users and organizations to carry out their tasks without having to worry about the scarcity of computing resources. With the advantages such as cost efficiency, unlimited storage, backup and recovery, automatic software integration, easy access to information etc, also come the concerns or disadvantages like security and privacy issues, data access or authorization, data residency, industry and regulation compliances. Out of the above mentioned security areas, *authenticating users and data privacy/confidentiality* are the major concerning issue that is making users and organizations to think twice before going to the cloud platform because they have a genuine concern: the protection and privacy of their most important data. The task of establishing the user identity is of the utmost importance and is the most vulnerable point of attack as the intruders know this fact that if they are able to gain access to a particular user account, then they can access and do any sort of harm to that user account. The most common authentication methods are based on a combination of usernames and passwords for different services offered by Cloud Service Providers (CSP's). However the brute force attacks makes this username-password scheme weak. Multi-factor mechanisms like use of Biometrics like fingerprinting, iris scanning, face recognition methods, hardware based approaches like One-time-passwords (OTP), hardware tokens and bypass methods are being proposed and are under continuous developments and improvements. This paper proposes a secure two-fold user authentication mechanism which includes a normal username-password combination as the initial stage to login and a strong security question series (SSQS) method to generate a secret code using an encryption algorithm that the user is supposed to provide on the Cloud Service Provider's website to access their account.

INTRODUCTION

Cloud Computing (CC) is an emerging computing paradigm that provides large amount of computing and storage to the Clients as a service over the internet on a pay-as you- go pricing model, where the Clients are supposed to pay only according to the usage of their services. "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"- U.S. National Institute of Standards and Technology (NIST)[17]. "A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers" [18].

Some of the important features that cloud computing offers are:

On-demand self-service: Cloud computing resources (such as CPU time, network storage, software use, and so forth) can be used and disposed of by the client without human interaction with the cloud service provider. This automated (i.e. convenient, self-serve) use of the computing resources reduces the personnel overhead of the cloud provider, cutting costs and lowering the price at which the services can be offered.

Resource pooling: With the help of a technique called —virtualization, the cloud provider pools his computing resources. This resource pool enables the sharing of virtual and physical resources by multiple consumers, —dynamically assigning and releasing resources according to consumer demand. The consumer has no explicit knowledge of the physical location of the resources (e.g. database, CPU, etc.) being used, except when the consumer requests to limit the physical location of his data to meet legal requirements. For example, consumers are not able to know where their data is going to be stored in the Cloud.

****Corresponding author: Ankit Dhamija,***
Assistant Professor, Amity Business School, Amity University Gurgaon

Broad service accessing mediums: Services from the cloud servers are accessible over the network (e.g. Internet) via standardized interfaces, enabling customers to have access to the service not only by complex devices such as personal computers, but also by light weight devices such as smart phones, mobile phones, laptops, and PDAs situated at a consumer's site.

Elasticity: Elasticity is the property of increasing or decreasing the services. The available cloud computing resources are rapidly matched to the actual demand, quickly increasing the cloud capabilities for a service if the demand rises, and quickly releasing the capabilities when the need is less. This automated process decreases the procurement time for new computing capabilities when the need is there, while preventing an abundance of unused computing power when the need has subsided.

Service usage calculation: Cloud computing enables the measuring of used resources, as is the case in utility computing. The measurements can be used to provide resource efficiency information to the cloud provider, and can be used to provide the consumer a payment model based on ―pay-per-use. For example, the consumer may be billed for the data transfer volumes, the number of hours a service is running, or the volume of the data stored per month. The unlimited storage space that the clients get is one of the important services of cloud computing which is a major reason the clients are inclined towards it. And in recent years, it has become a trend and more practical to storing the data remotely cloud storage and that too at a relatively lower cost.

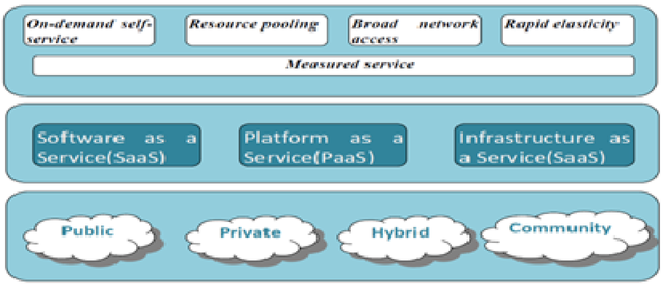


Figure 1. Cloud Computing Services, Characteristics and Models

The organizations those cannot invest heavily in buying their own infrastructure, software, etc opt for data storage on the Cloud platforms and thereby avoid the investments of initial setup and cost of maintaining data.

Cloud Service Models

Services provided by the cloud can be categorized into three:
a.Software as a Service(SaaS)
b.Platform as a Service (PaaS)
c.Infrastructure as a Service (IaaS)

Software as a Service (SaaS)

The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer. The cloud provider is responsible for the management of the application, operating systems and underlying infrastructure. The consumer can only control some of the user-specific application configuration settings. An example of this type of solutions is the e-mail service offered by Google, i.e., GMail, through its Google App Engine. In these situations, the Cloud user is only interested in getting the most out of the application provided by the Cloud. At this level the Cloud user is not seen as a developer anymore, he is a simple user of solutions offered by Cloud developers.

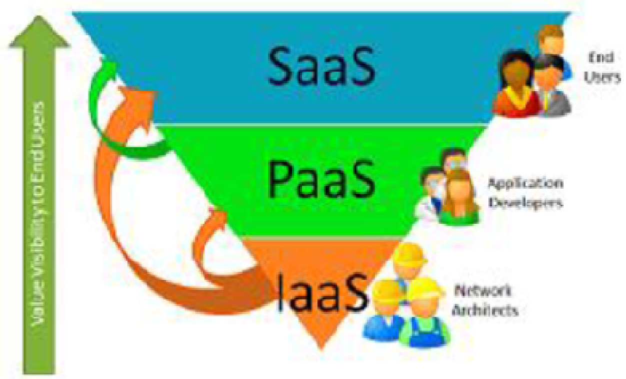


Figure 2. Cloud Service Models

Platform as a Service (PaaS)

The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a cloud-based infrastructure. ―The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Examples of PaaS can be a Linux distribution, a Web server, and a programming environment such as (PHP) in order to offer a web development environment for the Cloud developer, Windows Azure Platform, Google App Engine

Infrastructure as a Service (IaaS)

The IaaS service model offers computer Infrastructure as a service, such as raw data storage, processing power and network capacity. The consumer can use IaaS based service offerings to deploy his own operating systems and applications, offering a wider variety of deployment possibilities for a consumer than the PaaS and SaaS models. Amazon Elastic Compute Cloud or Amazon EC2 is the well-known commercial product that offers solutions at this level. This solution provides the customer with full access and control over the computing resources he paid for. This can be seen as the layer where the level of freedom of the user is the highest. At this layer the Cloud user still has to be concerned about maintaining the software he chooses to install in the resources rented to the Cloud provider.

Cloud Deployment Models

Clouds can also be classified based upon the underlying infrastructure deployment model as Public, Private, Community, or Hybrid clouds [19,20,21,22]. The different infrastructure deployment models are distinguishable with their own characteristics. The characteristics to describe the deployment models are: (i) who owns the infrastructure; (ii) who manages the infrastructure; (iii) where is the infrastructure located; (iv) who has access to the cloud services.

Private Cloud: This type of cloud is created and operated within a single organization. These are set up to maximize and optimize the utilization of existing in-house resources, make sure that the privacy and security concerns are kept at bay, to keep the data transfer cost low and to have a full control on the cloud.

Community Cloud: Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud community forms into a degree of economic scalability and democratic equilibrium. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community.

Public Cloud: These are the cloud service providers who offer storage services to their clients. The organizations who can't afford to build their own private cloud, opts to keep their data on public cloud service providers' servers. Public cloud users are considered to be untrusted, which means they are not tied to the organization as employees and that the user has no contractual agreements with the provider.

Hybrid Cloud: The cloud infrastructure is a combination of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology. Organizations use the hybrid cloud model in order to optimize their resources to increase their core competencies by margining out peripheral business functions onto the cloud while controlling core activities on-premise through private cloud.

However, Despite having so much of variety in different types of cloud platforms and despite the different type of services being offered by cloud service providers, Maintaining and enhancing the security and privacy in cloud environments is one of the most challenging issues that work as a hindrance element in the approach of users. This threat makes people hesitant in adopting the cloud platform.

Authenticating the users in a secure manner is the first most aspect of the security issue as it is only after a secure login, the user can access their data and the cloud service providers try to make this point the most safe.

In a traditional username-password authentication scheme, the server allows or denies any remote user based on identity and password. In general, textual password schemes are the most widely used, but they have many weaknesses. These drawbacks denotes that the user find it difficult in memorizing long or complex passwords, and the security risks can be obtained by depending short simple passwords. Hackers can use brute force attacks, dictionary attacks, on/off-line attack, replay attack, Man-in-the- Middle (MITM) attack to gain crack the passwords entered by the user as it is a common tendency to use phone number, favorite game, and name to use as a password. The previous approaches used only single tier techniques where biometric methods such as fingerprinting, iris scanning were used to authenticate a user. With the increase in the attacks mentioned above, two tier techniques came into picture which used an extra step in user authentication, thereby providing additional security for authenticating the user. Such techniques used the hardware devices such as smart phones as a means to convey to the user, a One Time Password (OTP) which the cloud service provider computes and sends it as an SMS on the registered mobile number of the user.

In this paper, the authors propose a secure twofold OTP based technique. The approach presents architecture of registering with the cloud vendor and for double authentication, This paper proposes a secure two-fold user authentication mechanism which includes a normal username-password combination as the initial stage to login and a strong security question series (SSQS) method to generate a secret code using an encryption algorithm that the user is supposed to provide on the Cloud Service Provider's website to access their account. The proposed model intends to provide an enhancement to the limitations posed by the normal hardware based OTP scheme where a user is supposed to enter a pin or password, received on their mobile handset. In the proposed solution architecture, the authors have ensured that the OTP is generated in a much secure and dynamic manner so that the whole authentication process gets more secure and less prone to attacks. The rest of this paper is organized as follows. The literature study and existing work exist in section II. The proposed scheme and its working are explained in detail in section III. The benefits of the proposed scheme are covered in Section IV. Finally, the Conclusion is presented in section V.

Literature Study & Related Work

A single technique can`t provide security in depth in Cloud, it really requires a strong authentication, confidentiality in transit and data integrity. Various blended approaches have been discussed below which provide different tier of authenticity in order to ensure security.

- Viet et al. [1] proposed the first anonymous password authentication scheme that aggregates a password scheme with the Private Information Retrieval (PIR) scheme. The limitations of this scheme are that it requires the server to be passed a whole database to detect user and it cannot resist on-line guessing attacks.
- Florencio and Herley [2] proposed a proxy web service that allows customers to arrive at web sites by employing a MITM proxy. The password customer is pre-encrypted and implemented as one-time passwords' list. Thus, the proxy cannot contain the passwords, but more correctly the keys with which the customers' passwords have been encrypted previously. This, however, is classified within a single-factor scheme. Moreover, there is a drawback to an adversary who misappropriates one-time password.
- Balfanz and Felten [3] presented a smart card task using a mobile phone. They used a sequence link to a remote computer and supported the mobile device by trusting the authentication path. There are several suggestions that denoted to use a cell phone as a second factor for authentication. However, this scheme is restricted by the cellular network coverage area.
- The smart card based authentication schemes [4-7] implement two factors of the authentication researches. In the first factor, users' investigation credentials are saved in the smart card while the password represents as a second factor, the smart card has been preserved by password. These two factors do not need the server to store a password

file. The negative side of smart card is that it is not a simple device.

- Sulochana and Parimelazhagan [8] have described a puzzle based authentication scheme in Cloud computing in which user first registers and solves the puzzle, puzzle solving pattern and time is stored and validated by local server and if user get authenticated, start accessing the Cloud services. Although this scheme ensures 2 tier authentications but static in nature, if attacker once identified the stored pattern, he could easily break the security.
- Yogita et al. [9] have described that not a single technique is enough to provide security in Cloud, she has used Diffie Hellman with digital signature for providing 2 tier authentication. But digital signature uses so many parameter that`s why it is heavy enough and also requires a proper key management.
- Maninder and Sarbjeet [10] have provided an advance multi tier authentication scheme for enhancing security in financial transactions, in which in first tier, user has to simply pass the traditional login authentication and in second tier a fake screen will appear before user from local server, which is filled by the user by predefined stored pattern, if it is correct then only server will allow access to the resources. Problem with this approach is that it is static in nature, once user identifies or observes the pattern of fake screen from behind, he can easily break this authentication.
- Satish and Anita [11] have proposed a method of fake screen for ensuring two tier authentication in Cloud computing. In this method of authentication, first user registered himself with Cloud server, and then registered his device. So secret code gets sent to the registered devices which ensure second level of authentication. This method involves additional hardware which is costly and must be along with you every time when you are going to login in the system.
- Parsi and Sudha [12] have proposed method that use RSA algorithm for authentication and data transfer securely. This method involves a phase of key generation, encryption and decryption.
- Priyank Rajvanshi et al [13] proposed an approach of protecting the confidentiality of users' data from service providers, and ensure that service providers cannot access or disclose users' confidential data being processed and stored in cloud computing systems. They suggested an efficient and supple spreading system with open dynamic data support to make sure the accuracy of user’s data in the cloud.
- B Wang et al [14] propose a simple, efficient, and publicly verifiable approach to ensure cloud data integrity without sacrificing the anonymity of data owners nor requiring significant overhead. Specifically, they introduce a security-mediator (SEM), which is able to generate verification metadata (i.e., signatures) on outsourced data for data owners. Their approach decouples the anonymity protection mechanism from the PDP.
- L. B. Jivanadham [15] et al proposed an integrated authentication mechanism called the Cloud Cognitive Authenticator (CCA), an API proposed for the cloud environment integrating bio-signals, one round Zero Knowledge Protocol (ZKP) for authentication and Rijndael algorithm in Advance Encryption Standard (AES). CCA is proposed to enhance the security in public cloud through four procedures providing two levels of authentication as well as encrypting/decrypting the user id.

Below is the table which summarizes the approaches proposed by the researchers above. On rigorous study of the literature, the authors tried to found the flaws and scope of improvement in the existing methods or techniques that are already proposed by other researchers.

Table 1. A comparative analysis of the existing authentication techniques

Sr No	Technique (Year)	Security Technique	Tier	Flaws Identified
1	A Puzzle Based Authentication Scheme for Cloud computing(2013)	Solve puzzle for Authentication	2	Static in nature, once stored puzzled is identified then
2	Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption algorithm to Enhance Data Security in Cloud computing(2013)	Ensure security using Diffie Hellman + Digital Signature	2	Key management is a problem
3	Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm(2013)	Ensure authentication and privacy using HMAC.	1	Weak authentication Process
4	Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography(2012)	Ensure Security using Diffie Hellman+ECC	1	One way traditional Authentication
5	Third party auditing for secure data storage in Cloud through digital signature using RSA(2012)	In this Third party is used to store the encrypted data using private and public key in RSA algorithm, Digital signature for Authentication	1	Costly because of third party involvement, one way authentication
6	Design and Implementation of Multi-tier Authentication Scheme in Cloud(2012)	Ensure authentication using traditional login and fake screen examination	2	Static in nature, once attackers detect the pattern of fake screen, security may be easily broken.
7	Multi Authentication for Cloud Security – A Framework(2014)	Ensure two tier authentication using registered devices	2	Require additional hardware
8	Data Security in Cloud computing using RSA Algorithm(2012)	Ensure one tier authentication using RSA cryptography	1	Data integrity not Assured
9	Authentication, Authorization, and Contextualization in Fermi Cloud(2010)	Authentication based on x.509 digital certificate	1	Certificate expiration problem, key management problem
10	A Physiological Authentication Scheme in Secure Healthcare Sensor Networks(2010)	A novel two-tier authentication approach based on physiology, RSA digital signature	2	Key management is a problem, costly because usage of additional hardware devices

From the above table, the authors come to a consensus that in a dynamic environment like cloud servers, a single approach or security mechanism cannot ensure the required level of security and thus, the authors are in favor of using a combined approach of security which ensures that the client or user is made to go through a series of security checks before they can access their accounts. In the above summarized table, the authors have categorized the techniques proposed as one tier and two tier. One tier techniques are those where the user has to pass through only a single security check and two tier techniques are those where the user have to cross multiple layers of security. The authors have found that multiple layers ensure stronger security methods which give the clients a surety that their data with cloud service providers is safe. Also, the cloud service provider's business is totally dependent on this safe management of data

Proposed Scheme

This section presents a secure twofold OTP based technique that uses a strong security question series (SSQS) method to generate a secret code using an encryption algorithm that the user is supposed to provide on the Cloud Service Provider's website to access their account to ensure a secure authentication over a cloud network. The proposed approach is presented in the form of a block diagram: The same block diagram will be used for depicting the client/user's account creation stage and for account accessing stage.

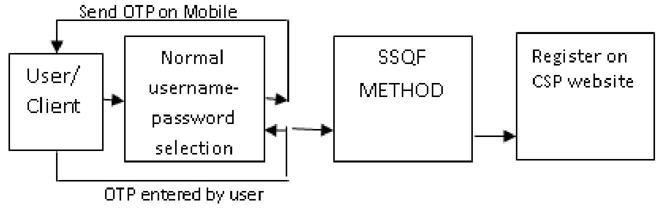


Figure 3. Block Diagram of the Proposed Approach

Account Creation Stage

STEP 1: The client/user visits the cloud service provider's website where they have to create their account.

STEP 2: The client/user is required to fill all the fields like name, company name, contact details and any other information asked by the cloud service provider and finally selects a username-password combination.

STEP 3: An OTP gets generated from the CSP website and is sent on the user's specified mobile number

STEP 4: User enters the received OTP on the website.

STEP 5: If validated, the user clears the initial stage of account creation and proceeds towards the selection of security questions. Here the user is presented a series of security questions which they have to answer. The user can also create their own security question if they are willing to.

STEP 6: The user answers all the questions, the answers are registered and saved and the user gets registered on CSP website.

Account accessing Stage

After the user is registered, they automatically logs out and are supposed to log in to their account again. Following are the steps in the account accessing stage:

STEP 1: The client/user visits the cloud service provider's website where they had created their account and here, they are supposed to enter their username-password combination on the cloud service provider's website.

STEP 2: If validated, the user clears the initial stage of Login and proceeds towards the selection of security questions. Here the user is asked to select a number of security questions. The user has to enter a numeric value such a s 2,3,4 and so on.

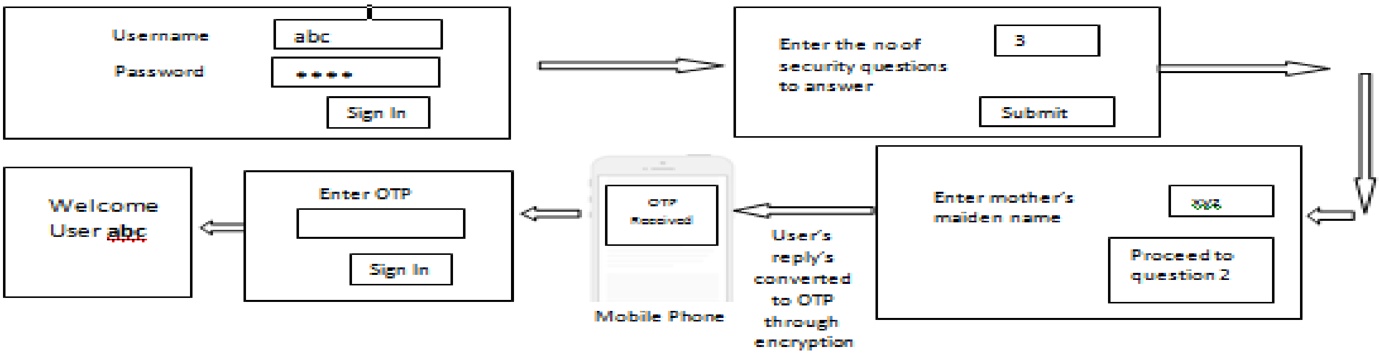
STEP 3: Based on the no of questions the user is willing to answer, the random questions from the question set that the user had answered while registering for the account come in front of the user. User has to provide the answers for each of them.

STEP 4: At the backend, all the answers from the user are combined together and based on an encrypted formula, an encrypted code is generated which is sent on the registered mobile number of the user as an OTP.

STEP 5: The user is supposed to enter this encrypted code on the CSP's website in order to authenticate them.

STEP 6: If the One time password entered by the user is valid and correct, the user moves to the welcome screen on the service provider's website where they can access or store the data that they had saved or they wish to store. Else, in case of invalid login due to some reason, the user is redirected to appropriate location to verify the details they have entered.

This is a very simple and secure two fold authentication method because the user, in order to gain access to their accounts have to pass through very strict and stringent security mechanisms that ensure the safety of the cloud servers and also ensure that the hackers from different sources who are trying to gain access to the sensitive data kept on the cloud servers remain safe and the client/user also remain worriless.


Username
abc
Password
****
Sign In
Enter the no of security questions to answer
3
Submit
Enter mother's maiden name
xxx
Proceed to question 2
User's reply's converted to OTP through encryption
OTP Received
Mobile Phone
Enter OTP
Sign In
Welcome User abc

Demonstration

In the above image, the author has depicted step by step approach that the user is supposed to follow while accessing their account on the Cloud Service Provider's website.

- Assuming that the user had already registered, he will provide his valid username and password on the CSP website and click on Sign In button.
- On the click on Sign In, the user is not redirected directly to his account. Instead, the user is supposed to choose the number of security questions he wishes to answer.
- Next, assuming that the user had entered 3, the 3 random security questions from the set of questions that the user had already answered in the Account creation stage appears on screen for the user to answer.
- The user's response gets recorded with each answer and based on an encryption algorithm, these answers gets converted into an encrypted code which acts as an OTP and is sent to the user's registered Mobile Number.
- The user is required to enter the OTP received on his device in the appropriate space provided on website.
- The OTP is validated and of correct, the user finds the welcome screen and can access his account.

Benefits of the Approach

As we have seen the working of the proposed scheme, the benefits can be figured out from the working and the demonstration. First, the proposed scheme provides additional level of security for secure login of the user. Second, it uses hardware based OTP method which is the best secure way of communicating with the user. Third, the proposed scheme always generates the encrypted code from security questions dynamically in a sense that the code generated and its length will always be unique. Fourth, the scheme is much better than the costlier biometric schemes that are based on fingerprinting scan, iris scan etc. Fifth, the complexity involved is much less than the other biometric based schemes.

Conclusion

In this paper, the authors have proposed a secure two-fold user authentication mechanism based on strong security question series (SSQS) to securely authenticate a user on the Cloud Service Provider's website. As the authentication of user is very important to ensure the safety of the data kept at the Cloud Servers, This approach addresses this issue by proposing a combined approach using OTP and SSQF. The benefits of the approach can be seen from the fact that the user is able to access their account by answering a set of security questions and then entering the OTP received on mobile, which makes the approach even more secure and stronger. For future work, the authors look forward to select a suitable encryption algorithm which best suits to the approach discussed here and perform its implementation & finally comparing the benefits of this approach with other existing approaches.

REFERENCES

Balfanz, D. and Felten, E. W. 1999. "Hand-held computers can be better smart cards", *Proc. of the 8th Conference on USENIX Security Symposium*, Washington, D.C, USA, 1999, pp.3-11.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., and Brandic, I. 2009. Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Generation Computer Systems, Elsevier, 25, pp. 599–616.

Chien, H. Y., Jan, J. K. and Tseng, Y. M. 2002. "An efficient and practical solution to remote authentication: smart card", *Journal. of Computers and Security*, Vol.21, No. 4, pp.372-375, 2002.

Das, M. L. Saxena, A. and Gulati, V. P. 2004 "A dynamic ID-based remote user authentication scheme", *IEEE Transactions on Consumer Electronics,* Vol.50, No. 2, pp.629-631, 2004.

Florencio, D. and Herley, C. 2008. "One-Time Password Access to Any Server Without Changing the Server", *Proc. of the International Supercomputing Conference(ISC"08), Taipei, Taiwan*, 2008, pp.401- 420.

Jeon, S., Kim, H. S. and Kim, M. S. 2011. "Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards", *Journal. of Security Engineering*, Vol.8, No.2, Apr. 2011, pp.237-254.

Jivanadham, L. B. et al, 2013. "Cloud Cognitive Authenticator (CCA): A public cloud computing authentication mechanism", *International Conference on Informatics, Electronics & Vision* (ICIEV), Print ISBN: 978-1-4799-0397-9 17-15 May, Page(s): 1 – 6.

Juang, W. S. 2004. "Efficient password authenticated key agreement using smart cards", *Journal. of Computers and Security*, Vol. 23, No.2, pp.167-173, 2004.

Judith, H., Robin, B., Marcia, K., and Fern, H. —Cloud Computing FOR DUMMIES‖, by WILEY INDIA EDITION.

Kalpana, P. and Singaraju, S. 2012. "Data security in cloud computing using RSA algorithm" IJRCCT, vol. 1, no. 4, pp. 143-146, Sep. 2012.

Kumar, S. and Ganpati, A. 2014. "Multi-authentication for cloud security: A framework" *International Journal Special Conference Issue: National Conference on Cloud Computing & Big Data of Computer Science & Engineering Technology*, vol. 5, no. 4, pp. 295 303, Apr. 2014.

Mather, T., Kumaraswamy, S., and Latif, S. 2009. Cloud Security and Privacy‖O'REILLY Publication, 2009.

Mell, P., and Grance, T. Draft NIST working definition of cloud computing,‖ Online at csrc.nist.gov/groups/ SNS/cloudcomputing/ cloud-def-v15.doc, 10-7-09.

Mell, P., and Grance, T. Draft NIST working definition of cloud computing,‖ Online at csrc.nist.gov/groups/ SNS/cloudcomputing/ cloud-def-v15.doc, 10-7-09.

Rajvanshi, P. et al. 2013. "Data Protection in Cloud Computing", *International Journal of Innovative Technology and Exploring Engineering* (IJITEE) ISSN: 2278-3075, Volume-3, Issue-3, August.

Rewagad, P. and Pawar, Y. 2013. "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing" *International Conference on Communication Systems and Network Technologies, CSNT,* IEEE, pp. 437-439, 2013.

Singh, M. and Singh, S. 2012. "Design and implementation of multi-tier authentication scheme in cloud" *International Journal of Computer Science Issues,* IJCSI, vol. 9, issue 5, no. 2, Sep. 2012.

Sulochana, V. and Parimelazhagan, R. 2013. “A puzzle based authentication scheme for cloud computing” *International Journal of Computer Trends and Technology*, IJCTT, vol. 6, no. 4, pp. 210-213, Dec. 2013.

Velte, T., Velte, A., and Elsenpeter, R. 2010. Cloud Computing: a Practical Approach‖, 1st edn., McGraw-Hill, New York, NY, USA ,Chap. 7.

Viet, D. Q., Yamamura, A. Hidema, and T. 2005, ”Anonymous Password-Based Authenticated Key Exchange”, *Proc. of 6th International Conference on Cryptology in India (Indocryp"05)*, Bangalore, India, Dec. 2005, pp.233- 257.

Wang, B. et al, 2013. “Storing Shared Data on the Cloud via Security-Mediator”, *IEEE 33rd International Conference on Distributed Computing Systems* ISSN 1063-6927, 8-11 July, Page(s) 124-133.

****