ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

Advanced Authentication Method using Virtual Keyboard for Cloud Computing

Indra Kumar Aadiwasi[1], Prof. Vimal Shukla [2],

M.Tech. Scholar, Kailash Narayan Patidar College Science & Technology, M.P, India[1]

Asst. Professor, Kailash Narayan Patidar College Science & Technology, M.P, India[2]

ABSTRACT Cloud Computing is a transpire technology which attempts to combine the storage and processing resources of cloud environment with the dynamicity and accessibility of cloud resources. Despite it has a huge contribution to the development of the technology and society, the cloud still exists some security deficiencies to block its development such as data leakage, illegal access and privacy risks. Hence, access control and user authentication is very important in cloud environment. Authentication is a vital and indispensable technology for data and information security. It is a mechanism to find proof of identities to get entry and access to the data and information in the system. Conventional password authentication mechanisms do not provide sufficient security measures for data and information in the cloud computing environment to the most modern ways of phishing and attacks.
Therefore, we suggest a new authentication and integration framework for cloud computing to secure data and information hacks. User authentication in proposed work is performed on the basis of secure OTP & user name and email password. It is verified on the basis of several security aspects and is verified to be available, accessible, feasible, secure, and user-friendly and provides strong authentication system. The proposed framework shows the close agreement with the standard criteria for security.
In this paper we propose a novel lightweight identity authentication based access control scheme for cloud. We propose offbeat classification system for existing authentication methods in cloud computing. We present an analogously analysis and recommends future research in improving the surveyed implicit authentication in Cloud Computing.

KEYWORDS: Cloud computing, Security, user authentication, OTP, Virtual Keyboard.

I. INTRODUCTION

In the last few years, many organization have adopted cloud computing technology, as cloud computing is a considerable acceptance as a model in every case like business, academic communities. These systems are very scalable, provide virtual on demand service with a huge amount of shared resources such as network, server, storage etc. Day by day, this computing technology has been changing rapidly. Advancement of computing technology also requires the system to upgrade for achieving large virtual capacity and high computing power [1]. People do their work through online including chatting, information collection, game, financial transaction etc. All this online activity require some type of authentication to identify whether the person is same which he owned to be or not. In the financial transactions, it requires some more security information including personal information and other account related information. Cloud data is accessed by common Internet protocols and networking standards. It is distinguished by the notion that resources are virtual and limitless and that details of the physical systems on which software runs are abstracted from the user [2]. With cloud computing, you can start very small and become big very fast. That's why cloud computing is revolutionary, even if the technology it is built on is evolutionary [2].The cloud reference model is shown below with its entire component required.
Cloud computing takes the technology, services, and applications that are similar to those on the Internet and turns them into a self-service utility. The use of the word “cloud” makes reference to the two essential concepts:
i) Abstraction
ii) Virtualization.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

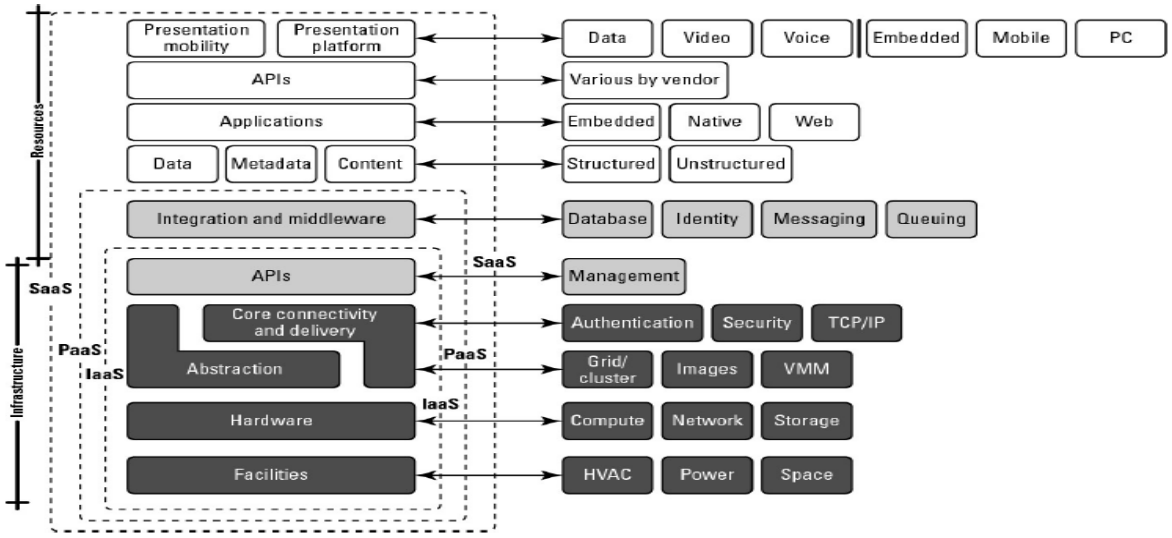

Fig. 1. Cloud Reference Model.

A) User Authentication in the Cloud:

Based on Cloud Service Model, security issues can be categorized [3]. It can be categorized into network level, user authentication level, data level, and generic issues. Each cloud service model comprises its own inherent security flaws; however they also share some challenges that affect all of them. Before analyzing security challenges in Cloud Computing, we need to understand the relationships and dependencies between these cloud service models [4]. PaaS as well as SaaS are hosted on top of IaaS thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around.

To identify the top concerns, CSA conducted a survey of industry experts to compile professional opinions on the greatest security issues within cloud computing [5]. The Top Threats working group used these survey results alongside their expertise to craft the final 2016 report. In this most recent edition of the report, experts identified the following 12 critical issues to cloud security (ranked in order of severity per survey results):

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues.

There are more security issues, but it is a good start for securing web applications. To secure the web application strong authentication mechanism is a solution.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

II. RELATED WORK

Existing techniques which are used for user authentication are shown in the Table below. These user authentication techniques take different criteria to authenticate the users in Cloud [6]. Each authentication method has some advantages and disadvantages that have been mentioned in the table below. The most common techniques are mobile trusted module, User/Id password module, Smart card module, One Time password Based module and Biometric Module [7].

		Mobile Trusted Module(MTM)	Text OTP(Without Process)	Smart Card	Biometric
SECURITY	PREVENTION OF IMPERSONATION BY AN ATTACKER [7]	DIFFICULTY TO FALSIFY CALLING NUMBER	DIFFICULT TO GUESS	DIFFICULT TO DUPLICATE	DIFFICULT TO FORGE
		GOOD	**GOOD**	**GOOD**	**EXCELLENT**
	PREVENTION OF THEFT [7].	CELL OHONE THEFT IS EASILY NOTICED	THEFT UNNOTICED	DIFFICULT TO NOTICE THEFT	NO THEFT
		GOOD	**POOR**	**POOR**	**EXCELLENT**
USABILITY	EASE OF OPERATION	EASY AUTHENTICATON BY TELEPHONE	DIFFICLTY TO USE BY ELDERLY	EASY	EASY
		EXCELLENT	**POOR**	**EXCELLENT**	**EXCELLENT**
	USE OF SPECIAL HARDWARE	A CELL PHONE IS NEEDED	REQUIRES SPECIAL TOKEN,DIFFERENT FOR EACH SERVICE	REQUIRES SMART CARD FOR EACH SERVICE	NEED FOR EXTRA HARDWARE
		GOOD	**POOR**	**FAIR**	**EXCELLENT**
ECONOMY	INITIAL COST (TO STRENGTHEN AUTHENTICATION)	REGISTRATION OF TELEPHONE NUMBER IS NEEDED	REQUIRES TOKEN	REQUIRES SMART CARD READER	REQUIRES SPECIALISED HARDWARE, DIFFICUT TO INSTALL
		EXCELLENT	**EXCELLENT**	**FAIR**	**POOR**
	RUNNINGCOST((TO STRENGTHEN AUTHENTICATION)	CHARGE FOR CALL	EXPENSE OF TOKEN MAINTENANCE ,MANAGEMENT	EXPENSE OF CARD MAINTENANCE	REQUIRES MAINTENANCE AND MANAGEMENT OF HARDWARE
		FAIR	**POOR**	**FAIR**	**POOR**

Table 1. Existing Authentication Techniques.

A) Strong Authentication Strategies: Authentication is generally referred to as a mechanism that establishes the validity of the claimed identity of the individual. There are basically four kind authentication methods:

- Something an individual KNOWS (e.g. password, Personal ID)
- Something an individual POSSESSES (e.g., a token or card)[8].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

- Something an individual IS (e.g. fingerprint or voice pattern)
- Something an individual DOES (e.g. history of Internet usage).

Recently many security researchers are focusing on various new techniques of authentication in cloud computing that include one or more of the above mentioned methods of authentication.[9]
Therefore it becomes inevitable to survey the various authentication methods recently proposed and implemented in the Cloud computing environment. The distribution of different Authentication method in Cloud computing is shown in figure 3 below:

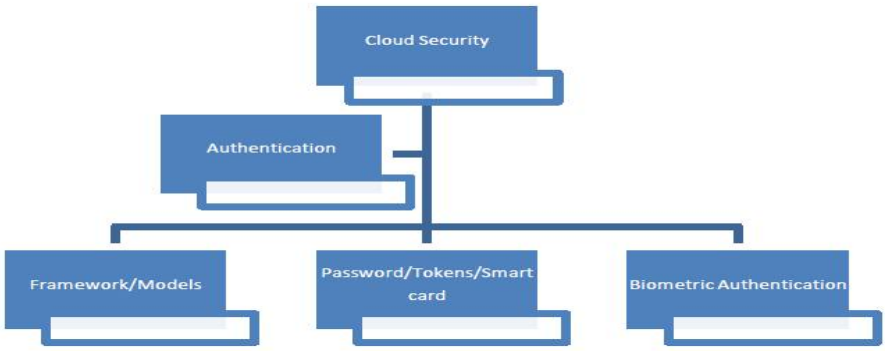

Fig. 2: Different Authentication method in Cloud computing

Next we will look on comparative study of numerous authentication factors and the implemented technologies with examples. Also, the comparison of techniques proposed by varied authors and applied algorithms.

III. PROPOSED ALGORITHM

A) Proposed key generation algorithm
System proposes a new key generation method, which generates key string for digits from 0 to 9 at the time of registration. That will be utilized by user for encoding the OTP received everytime. Generated key string will be mailed to user. User enters encoded OTP using virtual keyboard. Algorithm uses the concept of random number generation. IT will store all possible symbols used in virtual keyboard in a character array. Random numbers will be generated for digit 0 between 0 to 32, for digit 1 between 0 to 32 and so on to all digits. Corresponding symbols to random number will be stored in a array for digits of size 10. After this all symbols corresponding to digits are concatenated to make key string. Array of symbols utilized to generate key string is shown in figure below:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

a	b	c	d	e	f	g	h	i	j
0	1	2	3	4	5	6	7	8	9
k	l	m	n	o	p	q	r	s	t
10	11	12	13	14	15	16	17	18	19
u	v	w	x	y	z	.	,	;	?
20	21	22	23	24	25	26	27	28	29
!	:	&							
30	31	32							

Fig. 3 Symbols used in key string

Now system will generate random number between 0 to 32 for digits from 0 to 9. System fetch corresponding symbol from the symbol array and store it on another array sequentially to make key string. Example is shown below:
Array correspond to digit with randomly generated symbol :

&	z	t	.	w	?	e	y	m	c
0	1	2	3	4	5	6	7	8	9

So generated key string is &zt.w?eymc .

Algorithm contains following steps:

Step 1: First time user register in the system by filling form entry and submit it.

Step 2: Take an array d of 10 size for digits and declare a constatnt array c of 33 size.

Step 3: Array c has assign 33 symbols like alphabets from a to z & other symbols . , ; ? ! : &.

Step 4: For digits i=0 to 9 loop

Step 4.1: call random() method to generate random no between 0 to

32 , Suppose it is r

Step 4.2: store d[i]=c[r]

Step 5: Store key string in database.

Step 6: Send key string on user's registered email id.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

IV. SIMULATION RESULT

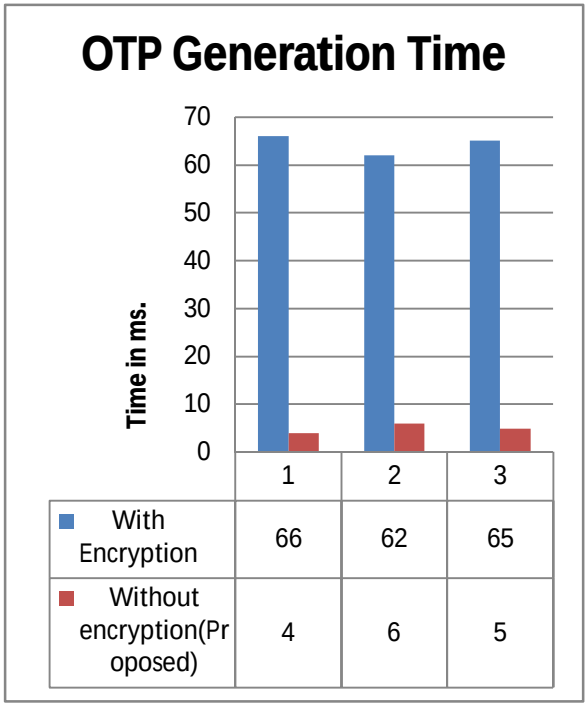

Fig. 3 OTP Generation Time

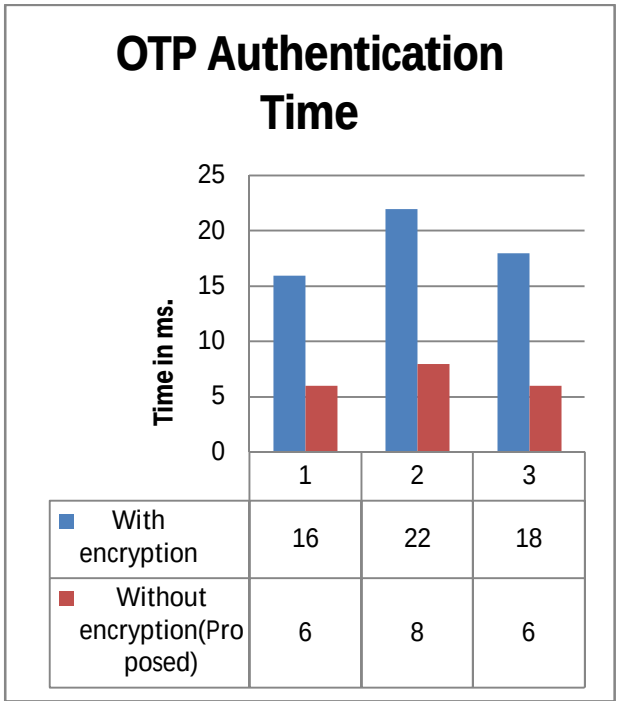

Fig. 4 OTP Authentication Time.

V. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better with the total transmission energy metric than the maximum number of hops metric. The proposed algorithm provides energy efficient path for data transmission and maximizes the lifetime of entire network. As the performance of the proposed algorithm is analyzed between two metrics in future with some modifications in design considerations the performance of the proposed algorithm can be compared with other energy efficient algorithm. We have used very small network of 5 nodes, as number of nodes increases the complexity will increase. We can increase the number of nodes and analyze the performance.

REFERENCES

[1]. W. Liu, "Research on Cloud Computing Security Problem and Strategy", International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp.1216 – 1219.
[2]. Baker, M. Mackay, and M. Randles, "Eternal Cloud Computation Application Development." *Developments in E-systems Engineering (DeSE)*, pp. 392-397, 2011.
[3]. Shyam Nandan Kumar, "DecenCrypto Cloud: Decentralized Cryptography Technique for Secure Communication over the Clouds." Journal of Computer Sciences and Applications, vol. 3, no. 3 (2015)
[4]. Cloud Security Alliance Security guidance for critical areas of focus in Cloud Computing. https://cloudsecurityalliance.org/guidance/csaguide.v3.0,2016.
[5]. CLOUD SECURITY ALLIANCE The Treacherous 12 - Cloud Computing Top Threats in 2016, © 2016, Cloud Security Alliance.
[6]. Jinsook Bong et al. "Fast User Authentication Method Considering Mobility in Multi Clouds", IEEE 2016.
[7]. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", Proceedings of Advances in Computing and Communications, Vol. 193, pp. 44-54, 2011.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

[8]. Jian Shen1,2,3, Dengzhi Liu3, Shaohua Chang3, Jun Shen3, Debiao He4," A Lightweight Mutual Authentication Scheme for User and Server in Cloud", IEEE 2015.
[9]. Jian Shen1,2,3, Dengzhi Liu3, Shaohua Chang3, Jun Shen3, Debiao He4," A Lightweight Mutual Authentication Scheme for User and Server in Cloud", IEEE 2015.
[10]. Ashish Singh, Kakali Chatterjee, "A Secure Multi-Tier Authentication Scheme in Cloud Computing Environment", IEEE 2015.