JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Authentication Approch using Manual Cryptography

[1]Chandan Kumar, [2]Author Name: - Dr. Manoj Lipton, [3]Chetan Agrawal
[1]Designation of 1st Author: - Research Schooler, [2]Designation of 2nd Author: - Associate Professor, [3]Designation of 3rd Author: - Asst. Professor.
[1]Name of Department of 1st Author: - Department of CSE,
[1]Name of organization of 1st Author: - Radharaman Institute of Technology & Science
Bhopal, India

Abstract- Authentication is one of the major security parameters while providing access of the registered services to the intended users. The attractive features of cloud computing many organizations are using cloud storage for storing their critical information. The user stored information remotely in the cloud by the users and can be accessed using clients as and when required. Securing these essential data from the unauthorized access of the users is one of the major issues which lead to reduce the growth of this technology in the industries. To enhance security in authentication we provide a novel method in this paper. In this method we use manual cryptographic calculation for securing authentication.

Keywords— Authenticaion Mechanism, Manual Cipher, Cryptography, Cloud, Attacks.

I. INTRODUCTION

Cloud computing is a novel technology that provides on-demand, network access to a common pool of configurable resources on a pay per use basis [1]. This new computing prototype differs from different analogous computing technologies in this; the cloud computing services follow a self-service model. Cloud computing offers software package, platform and infrastructure over the web and this constitutes in the 3 types of cloud viz., SaaS (Software-as-a-Service), IaaS (Infrastructure-as-a-Service) and PaaS (Platform-as-a-Service) [2]. This computing form allows the cloud users to enhance their capacity and capability animatedly while not investing in new resources [1].

Cloud computing technology allows users to remotely access shared resources keep in cloud servers using web services via the internet. Therefore the cloud resident resources are viable to the safety threats applicable to web and internet services. The actual fact that the resources ought to be accessible only to legitimate use's points out to the need of deriving a secure, user authentication mechanism for the cloud atmosphere. Authentication involves the method of making certain that an individual who presents a collection of credentials is whom he or she claims to be. The cloud service providers need to tackle the problems faced by user authentication mechanisms carried out before providing access to the shared resources.

When anyone needs to access the network, for security purposes each web application provides user authentication. From ancient day's secret information or code is used for concealment and giving security to data. In user authentication the method that we've to go through is username and password. Authentication method divided into Biometric based authentication, Token based authentication and knowledge based authentication. Most of the online application provides knowledge based authentication that embrace alphanumeric password further as graphical password. In today's dynamic world once we are having variety of networks and private account some sort of simple authentication [3] schema need to be provided.

II. LITERATURE REVIEW

In this paper [4] authors acquainted a handwriting authentication system. The procedure allows secure access to confined data in the cloud exploiting a mobile phone. It's prepared of pre-processing, feature genealogy, division and authentication procedure. The division process is grounded on three different division systems ANN, KNN, and Euclidean Distance classifier. The classifier algorithm employs resemblant compound of classifiers in ordering to attain satisfactory delicacy on both recognition and error rate.

In those papers [5],[6], litterateurs have concentrated on applying graphical representation for enhancing authentication. Litterateurs present the visual password authentication scheme in this paper [5]; it can be given by taking cloud as a platform while in paper [6], litterateurs propose a undecorated and effectual online signature verification system that's competent for user authentication on a portable device. The benefits of the proposed algorithm are as follows. First, a histogram grounded point set for representing an online signature can be deduced in direct time and the system requires a slight and immutable- size space to keep the signature template. In addition, since the point set represents purely statistics about division of original online hand attributes, the metamorphosis isnon-invertible. As a result, the sequestration of the original biometric data is well- defended. Second, a stoner-specific classifier comprising of a stoner-specific quantization step size vector and its associated quantized point vector can be trained using only registration samples from that stoner without taking a training set from a large number of druggies. Several trials performed on MCYT and SUSIG datasets demonstrate effectiveness of the proposed system in terms of verification performance as compared to being algorithms.
Security analysis of online hand verification system as compared to that of 4- integers Leg, and two usability criteria is also presented. Farther disquisition includes the use of distinctive biometric key binding passages, like fuzzy commitment, in order to strengthen security of the system, indeed when stored templates, coadjutor detect., are endangered, while conserving verification performance. Incipiently, it's possible to decide a emulsion approach by combining the proposed system with other being ways, e.g., DTW, HMM-grounded, etc., in order to ameliorate verification interpretation, specifically for operations where sequestration of the hand traits is less critical.

In the papers [7] [8], authors had used images as a parameter for authentication. In the paper [7] authors examine whether or not people could guess the hand-drawn images which were used as the graphical password of others, if they know some cultural information about the users, such as where they came from or their religion or even their hopes. The cram also aims to put in evidence of a bias in the user choice of images and considers the impact this could have on guess ability. However, the results show that there is no difference between males and females and between members of different cultures in their ability to guess images. One clear result of this work is that it is apparently highly possible to guess other people's pass images if they contain cultural characteristics, especially religious marks, otherwise it is much more difficult to guess them. Also the authors provide Guidelines of drawing a secret password. While in the paper [8] authors had proposed an authentication mechanism using Images. As per authors key should be shared between user and cloud service provider (CSP) to access data in secure way. To accessing data from cloud, user will only be authenticated by CSP but they are not exchanging key among each other. According to the mechanism proposed by authors to access data from cloud. Firstly user is authenticated by cloud service provider using Image based authentication scheme after that key has been exchanged between user and cloud service provider (CSP), with the help of that key CSP will send the encrypted data to user. Proposed secure mechanism to access data from cloud work in three phase- Registration phase, Image based Authentication and Key Exchange phase.

Authors presented [9] a survey of recent trends to automatic recognition of human facial behavior using soft computing. Soft computing is the mainly striking field nowadays. Soft computing proves useful technique to the difficulty of classification, prediction, pattern recognition, optimization, image processing, etc. The facial behavior recognition processes in three steps in general. Face detection is the procedure of identifying face from images. Feature pulling out is a process of accent the facial part that takes part in identification of expression and last a classifier is design that identifies the expression. There are a lot of valuable methods are there to distinguish face expression, but no method performs best in all types of situation. Each and avery method has their own limitations. The future of human facial behavior recognition system is to make a robust system that will perform efficiently in any circumstances.

Application makers may facade with a adverse set of scenarios, each with its own identity solution without claim-based identity. Claim-based identity helps in providing a consistent answer across a wide range of scenario of cloud services. By building and deploying claim-based applications besides existing application result in simpler migration. Claim-based identity is not for only Microsoft vendors-many vendors are involved. In this paper [10], authors show why claim-based identity solutions are required and how to use by the cloud service provider in cloud applications.

In this paper [11], authors identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Frontward security is realized by the session identifiers to avert the session correlation. It indicates that the proposed scheme is possibly applied for privacy preservation in cloud applications.

In this paper [12] authors states that Modern cryptosystem uses authentication mechanisms for secure communication and authentication mechanism is essential even at cryptosystems based on QKD (Quantum Key Distribution). As per Authors no practical

authentication mechanisms dedicated to quantum cryptosystem is available. Authors have proposed an authentication scheme for cryptosystem based on QKD.

This research paper [13], propose a framework with a base of Elliptical Curve Cryptography (ECC) to perform secure financial transactions through Virtual Private Network (VPN) by implementing strong Multi-Factor Authentication (MFA) using authentication credentials and biometric identity. The research results prove that the proposed model is to be an ideal scheme for real-time implementation. The security analysis reports that the proposed model exhibits high level of security with a minimal response time of 12 s on an average of 1000 users.

Strong user authentication procedure impedes illegal access to the Service Provider which is the principal requirement for securing cloud computing ecosystem. In this regard, authors attempt to propose possible counter measures for the cloud ecosystem. Hence, this paper [14] presented a novel one way hash and nonce-based two-factor secure authentication scheme with traditional user IDs, password, and OTP verification procedure that resist brute force attack, session and account hijacking attack, MITM attacks and replay attacks.

III. Proposed Architecture

As shown in figure 1 the proposed architecture first registration is done by the user. Based on this registration details the random pattern for login phase is generated which is offered to the user when he login in the future. These patterns are so random that they are not repeated for three times & when a user enters wrong patterns up to three times then the login is blocked. This authentication approach is completely secure as compared to the previous approaches of authentication.

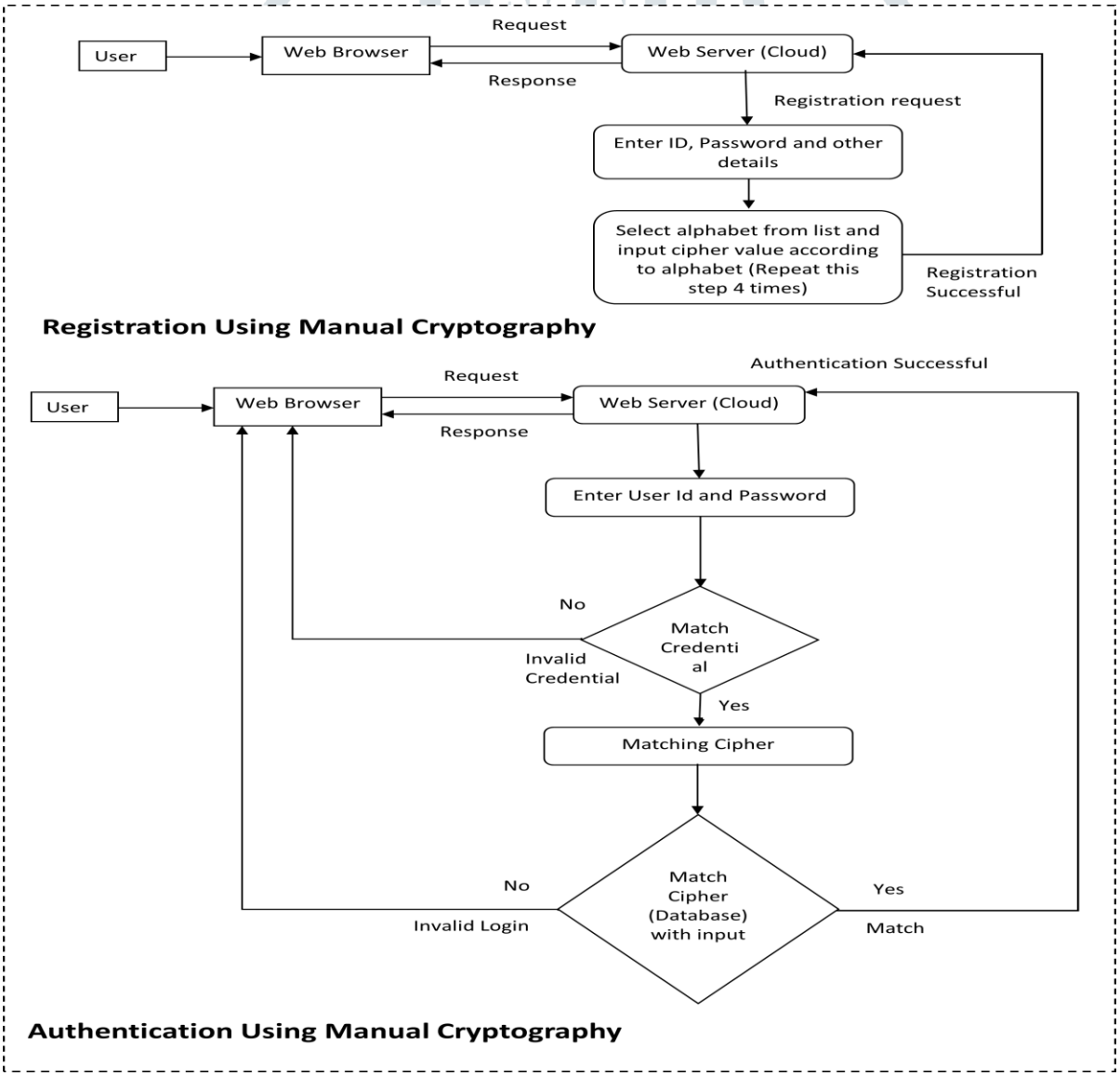

Figure 1: Architecture of proposed algorithm

Algorithm:

The algorithm can be divided in two sub parts Registration & Login.

1. Registration:-

- User fills required details for registration like User Name, Password and stores it in database.
- After that user chooses one alphabet from list of A to Z alphabet and inserts numeric value of its choice with respect to the alphabet.
- To complete the registration step II is repeated four times, every time alphabets chosen in previous steps are removed from list.

2. Login:-

- User fills user name and Password.
- Systems checks user name and password in database if match is found then step III is followed otherwise Step I is followed.
- Getting the List of stored manual cipher from the database (8 values as per registration i.e. 4 alphabets & their four numeric values) then a random number is generated and divided by 8. Then a pattern is chosen from list based on the reminder that we got after dividing the random number by 8 i.e. if reminder is 4 then choose fourth element of list.
- Check the cipher pattern that are not used in last three times, if the current pattern matched any one of last three times then repeat step III, if no then go to step V.
- User inserts numeric value or alphabet as prompted by system with respect to step III.
- If match is found then authentication is successful otherwise user is send back to step I to try again.

IV. Result Analysis

For the results we had implemented the proposed approach using .NET & SQL server. Refer table 1 & figure 2 for result analysis.

Table 1: Prevention from various attacks

Attacks	Status
Identity disclosure attack	YES
Replay attack	YES
Password based attack	YES
Identity Spoofing	YES
Outsider attack	YES
Man-in the middle attack	YES
Eavesdropping	YES
Insider attack	YES

As shown in the table 1 is the prevention of our proposed work from various attacks in the attack.

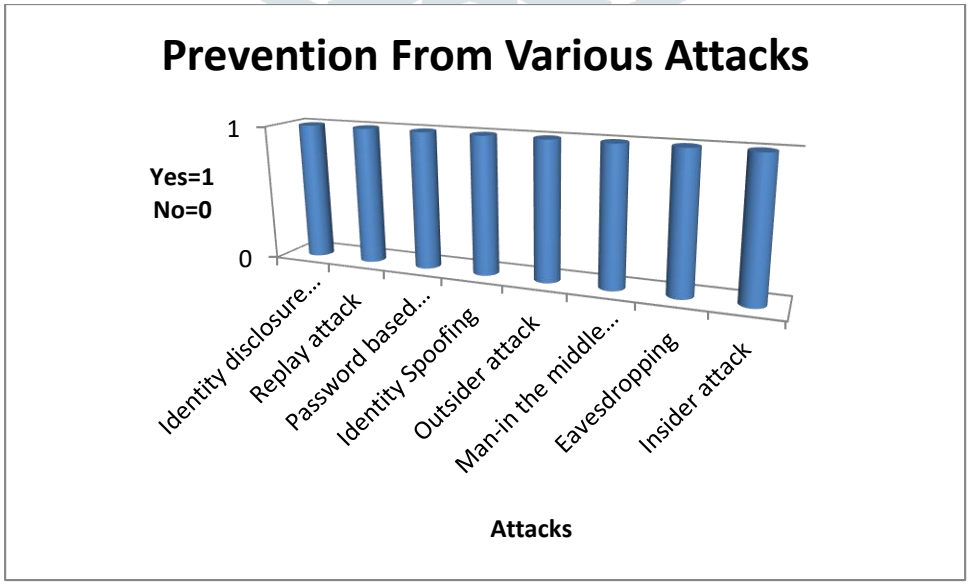

Figure 2: Prevention from various attacks

4.1 Comparison of proposed Approach with OTP, Finger Print, Face Recognition & Smart Card

The proposed approach is compared with Finger Print recognition, OTP, Smart Card systems & Face Recognition used for authentication. The comparison is based on various dependency parameters as mentioned on Table 2 & figure 3. The value 1 represents 'YES' & value 0 represents 'NO'.

As per table 2 and figure 3 it is clear that OTP system is more dependent on various dependency parameters as compared to the other mechanisms of authentication. The proposed approach has least dependency on various dependency parameters as compared to Finger Print, OTP, Smart card and Face Recognition authentication system. The failure rate of proposed approach will be less as it dependency is less as compared to other authentication mechanisms.

Table 2: Comparison of Proposed Approach

Dependency Parameter	Finger Print	OTP	Proposed Approach	Smart Card	Face Recognition
Internet	1	1	1	1	1
Extra Hardware	1	1	0	1	1
Mobile Network	0	1	0	0	0
Failure due to third party	1	1	0	1	1

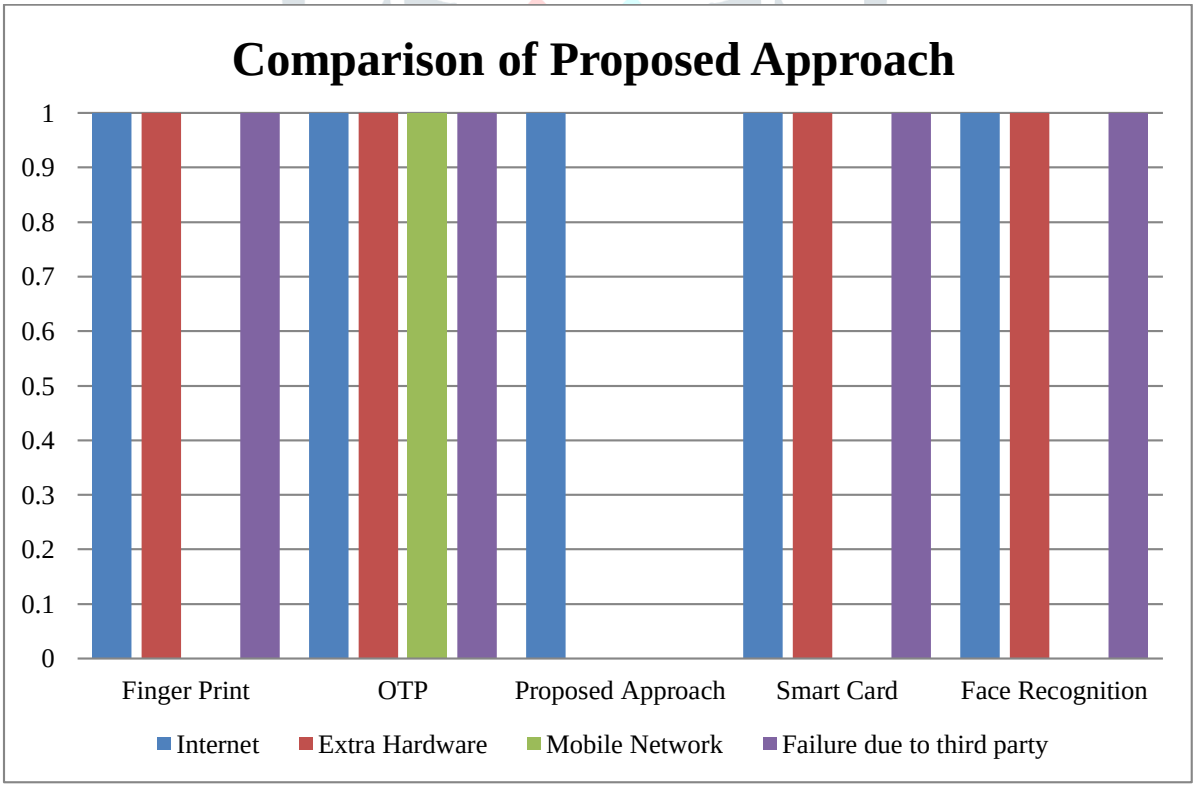

Figure 3: Comparison of Proposed Approach

V. CONCLUSION

There are extreme benefits in using a cloud-based system this system solve several practical issues. Cloud computing is a tumultuous technology with profound implications not just for web services however additionally for the IT sector as a whole. Still, many outstanding problems exist, particularly related to security and privacy. As described within the paper, presently security has lot of loose ends which scares away a lot of potential users. Still a proper security module isn't in place; potential users won't be ready to

leverage the benefits of this technology. This security module should cater to any or all the problems arising from all directions of the cloud.

The Authentication level security method described in this paper. The manual cryptography is easy to use for the users and this method used dynamic combination of cipher for enhancing security. The result analysis show that this method provides security from various threats and also it is better and simple then OTP based authentication & finger print based authentication.

REFERENCE

[1] V. Kavitha, S. Subashini, "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Journal of Network and Computer Applications, vol. 34, ,no.1, pp. 1 -11, 2011.
[2] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011.
[3] J. Birget, S. Wiedenbeck, A. Brodskiy "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice" SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security, Pittsburgh, Pennsylvania, USA-July 06 - 08, 2005.
[4] F. Omr, S. FoufoU, R. HamiIa & M. Jarraya presented paper entitled "Cloud-based Mobile System for Biometrics Authentication" at IEEE 2013 13th International Conference on ITS Telecommunications (ITST).
[5] Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane & Nilesh R. Khochare presented paper entitled "Graphical Password Authentication" at IEEE 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.
[6] Napa Sae-Bae & Nasir Memon presented paper entitled "Online Signature Verification on Mobile Devices" at IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.
[7] Salem Jebriel & Dr. Ron Poet presented paper entitled "Exploring the Guessability of Hand Drawn Images Based on Cultural Characteristics" at IEEE 2014 6th International Conference on CSIT Published by the IEEE Computer Society.
[8] Anurag Singh Tomar, Gaurav Kumar Tak, Ruchi Chaudhary "Image based Authentication with Secure Key Exchange Mechanism in Cloud", 2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom).
[9] Khyati Kantharia & Ghanshyam I Prajapati presented paper entitled "Facial Behavior Recognition using Soft Computing Techniques: A Survey" at IEEE 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
[10] Ashish Singh & Kakali Chatterjee presented paper entitled "Identity Management in Cloud computing Through Claim-Based Solution" at IEEE 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
[11] Hong Liu, Huan sheng Ning, Qing Xu Xiong & Laurence T. Yang presented paper entitled "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing" at IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 1, JANUARY 2015.
[12] Minyoung Bae, Ju-Sung Kang, Yongjin Yeom, "A Study on the One-To-Many Authentication Scheme for Cryptosystem Based on Quantum Key Distribution" 978-1-5090-5140-3/17/$31.00 ©2017 IEEE.
[13] D. Prabakaran and Shyamala Ramachandran, "Multi-Factor Authentication for Secured Financial Transactions in Cloud Environment", Computers Materials & Continua, DOI:10.32604/cmc.2022.019591.
[14] Sandeep kaur, Gaganpreet kaur and Mohammad Shabaz, "A Secure Two-Factor Authentication Framework in Cloud Computing", Security and Communication Networks, Volume 2022, Article ID 7540891.