ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Novel Mechanism for Authentication by using User Generated Cryptograph

Akanksha Pal[1], Mayank Bhatt[2]

P.G. Student, Dept. of CSE, LNCTS (RIT), Indore, MP, India[1]

HOD, Dept. of CSE, LNCTS (RIT), Indore, MP, India[2]

ABSTRACT: Cloud computing is that the envisioned as the next generation design of information Technology (IT) endeavor. It moves the application and databases to the central large data centers, wherever the management of the information and services might not be absolutely trustworthy. This distinctive paradigm brings concerning several new security challenges, that haven't been well understood. Securing these essential cloud resources from the unauthorized access of the users is one amongst the most important problems that cause reduces the growth of this technology within the IT Industries. Authentication is one of the most important security parameters whereas providing access of the registered services to the intended users. in this paper we provide a security mechanism for authentication in clouds by using user generated cryptograph. The idea is to develop an enhanced authentication method on hybrid cloud.

KEYWORDS: Cloud computing, cryptography, Security, Authentication, hybrid cloud.

I. INTRODUCTION

Cloud computing is basically composed of a large-scale distributed and virtual machine computing infrastructure. This new paradigm delivers an outsized pool of virtual and dynamically ascendible resources as well as process power, storage, hardware platforms and applications to users via web technologies. Private and public organizations alike will build use of such cloud systems and services and many benefits could also be derived when migrating all or some information services to the cloud computing atmosphere. Examples of these advantages include increases in flexibility and fund savings through reduction of hardware and software system investments.

However, ensuring the security and privacy in cloud computing environments is one among the foremost difficult problems that decrease the rate of dependability in cloud-based merchandise. This security has been divided to many parts and one in every of the foremost important elements is ensuring about the user authentication processes [1] and managing accesses once users outsource sensitive knowledge share on public or personal cloud servers [2]. User authentication in cloud computing environments has been divided to two main processes: investigating unique identifiers of users throughout the initial registration part and user authentication and validating user legal identities and getting their access management privileges for the cloud-based resources and services throughout the service operation part.

Today, user authentication in web plays a additional important role than ever before. For sensitive systems like on-line retail and e-banking, it's crucial to endlessly protect users' accounts and assets from malicious third parties. Even in comparatively less critical systems like desktop machines in an exceedingly corporate computer network and social networks, a fallacious login will still be abused to access confidential information, spread viruses, and spam or to conduct a social-engineering attack, presumably harming a legitimate users reputation and different users interest. The foremost common authentication issue may be a password that suffers from several weaknesses, like password cracking, condition to phishing and cross-site password applies. Once a password is compromised, an opponent will simply misuse a victim's account. Thus, there's great demand to determine a authentication system that give additional security from other system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

II. RELATED WORK

Authors introduced a handwriting authentication system [3]. This process allows users to access restricted data in the cloud using a mobile phone with security. It is composed of pre-processing, feature extraction, classification and authentication process. The classification method is predicated on three completely different classification techniques: ANN, KNN, and euclidean Distance classifier. The classifier algorithmic program employs parallel combination of classifiers so as to attain satisfactory accuracy on each recognition and error rate.

The combination of the cloud computing and mobile computing creates mobile cloud computing and additionally introduce security threats appreciate unauthorized users access. The authors focus during this analysis [4] is on the mobile cloud and protective mobile cloud resources from illegitimate access. Biometric recognition are going to be employed in the close to future in mobile devices. The projected solution by authors for authenticating mobile cloud users exploitation the present mobile device camera as a fingerprint sensing element to get a fingerprint image, then process it and recognize it. Results show that the proposed solution has supplementary value to stay performance at an accepted level.

In this paper [5], authors propose an easy and effective on-line signature verification system that's appropriate for user authentication on a mobile device. The advantages of the proposed algorithm are as follows. First, a histogram based mostly feature set for representing an online signature are often derived in linear time and also the system needs a little and fixed-size area to store the signature model. Additionally, since the feature set represents solely statistics concerning distribution of original on-line signature attributes, the transformation is non-invertible. As a result, the privacy of the first biometric information is well-protected. Second, a user-specific classifier comprising of a user-specific quantization step size vector and its associated measure feature vector are often trained victimization only enrollment samples from that user while not requiring a training set from an outsized variety of users. Many experiments performed on MCYT and SUSIG datasets express effectiveness of the proposed technique in terms of verification performance as compared to existing algorithms.

Security analysis of on-line signature verification system as compared to it of 4-digits PIN and two usability metrics is additionally given. additional investigation includes the utilization of alternative biometric key binding approaches, like fuzzy commitment, so as to strengthen security of the system, even once stored templates, helper information etc., are compromised, whereas protective verification performance. Lastly, it's possible to derive a fusion approach by combining the proposed technique with alternative existing approaches, e.g., DTW, HMM-based, etc., in order to enhance verification performance, particularly for applications wherever privacy of the signature traits is a smaller amount crucial.

In this paper [6], 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 their religion or even their hopes or where they came from. The analysis also aims to contribute evidence of a bias in the user choice of images and considers the impact this could have on guess ability. However, the results analysis shows that there is no dissimilarity 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 extremely potential to guess other people's selected images if they contain cultural characteristics, especially religious marks, otherwise it is much more difficult to presume them. Also the authors provide Guidelines in this paper for drawing a secret password.

Authors proposed a completely unique mutual authentication protocol for cloud computing victimization secret sharing and steganography during this paper [7]. The protocol is intended in such some way that it uses steganography as an extra encryption theme. The theme achieves authentication victimization secret sharing. Secret sharing permits a region of the secret to be unbroken in either side that once combined becomes the entire secret. The secret contains data concerning each parties concerned. Further, out of band authentication has been used that provides extra security.

According to the difficult problems throughout the user authentication and access management method in cloud-based environments, an efficient and scalable user authentication theme was proposed during this paper [8]. It the advised model, numerous tools and techniques were introduced and employed by victimization the conception of agent. Therefore, a client-based user authentication agent was introduced to verify identity of the user in client-side.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Moreover, a cloud-based software-as-a service application was wont to make sure the method of authentication for un-registered devices.

Moreover, there are two different servers for squiring authentication and cryptography resources from main servers to decrease the colony of user authentication and encryption processes from main server. Cryptography agent was additionally introduced to encrypt resources on before send on cloud servers. In overall, the theoretical analysis of the advised theme shows that, coming up with this user authentication and access management model can enhance the reliableness and rate of trust in cloud computing environments as a rising and powerful technology in numerous industries.

In this paper [9], authors known a brand new privacy challenge during information accessing within the cloud computing to realize privacy-preserving entry level authority sharing. Authentication is confirmed to ensure information confidentiality and information integrity. Data obscurity is achieved since the wrapped data are changed throughout transmission. User privacy is increased by unknown access requests to sepratly inform the cloud server concerning the users' access needs. Forward security is complete by the session identifiers to stop the session correlation. It indicates that the proposed theme is probably applied for privacy preservation in cloud applications.

In this paper [10], authors present a survey of recent trends to automatic recognition of human facial behavior using soft computing. Soft computing is the most attractive field nowadays. Soft computing proves effective techniques to the problem of classification, prediction, optimization, pattern recognition, image processing, etc. The facial behaviour recognition processes in three steps in general. Face detection is the process of identifying face from images. Feature extraction is a process of highlighting 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 effective methods are there to detect face expression, but no method performs best in all types of situation. Each method has their limitations. The future of human facial behaviour recognition system is to make a robust system that will perform efficiently in any circumstances.

Application developers may face 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 [11], authors show why claim-based identity solutions are required and how to use by the cloud service provider in cloud applications.

III. PROPOSED TECHNIQUE

In this proposed technique we use cryptography for authentication. In registration phase firstly user enters basic details and user id & Password. After submission of basic details our system ask user to choose four alphabets and its numerical value one by one. Every time previous chooses alphabet remove from list. So we have 8 ciphers for authentication. On authentication phase firstly user enter user id and password if its match then user go to next phase of authentication otherwise authentication field. In second phase a alphabet or number prompted randomly for asking user to enter its cipher value if enter value is valid then authentication is completed otherwise authentication is failed and user back to first step.

IV. PROPOSED ARCHITECTURE

The figure 1 shows architectural diagram of proposed technique. In this diagram, we provide full process of our work from registration phase to authentication phase.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

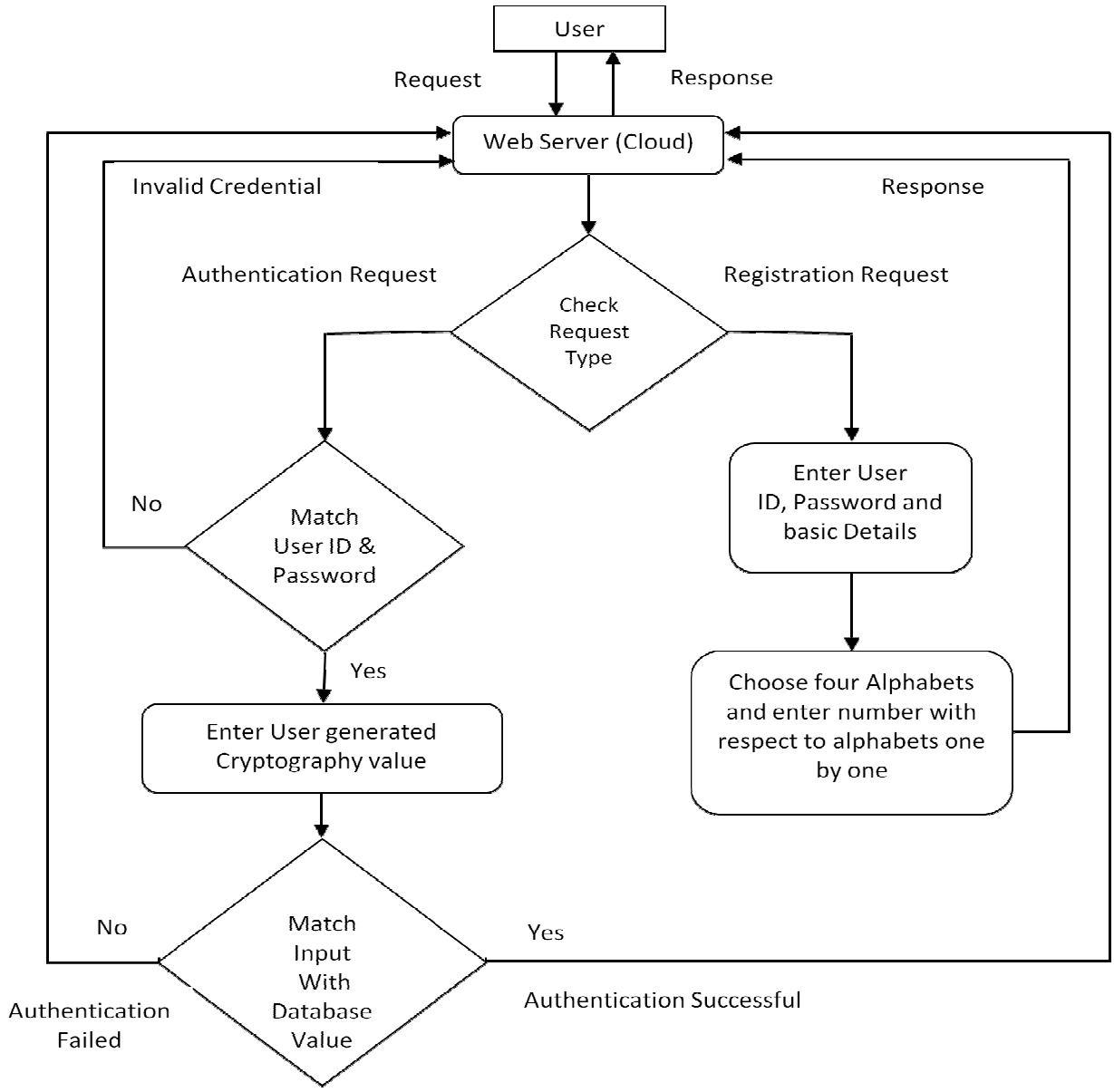


Figure 1: Architectural diagram of proposed technique

V. PROPOSED ALGORITHM

The algorithm divided in two phases Registration phase and Authentication phase. Algorithm describe below:

1. *Registration Phase*:-

Step 1:- User enters basic details like Name, contact number, address and User ID & Password.

Step 2:- After submission of basic details user choose one alphabet from list of A to Z alphabets and enter its numerical value.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Step 3:- For completing registration phase II step repeat four times for choosing four alphabets and entering four numbers.

2. *Authentication Phase*:-

Step 1:- User enter User ID (Name) and Password and submit authentication request to server.

Step 2:- On server side system match User ID and Password with saved information. If match found go to the next step otherwise server send invalid credential message to user.

Step 3:- List of stored user generated cryptography cipher patterns is retrieved from the database (8 elements as per registration phase i.e. 4 alphabets & their four number) then a random number is generated and divided by 8. Then an element is chosen from list based on the reminder that we got after dividing the random number by 8 elements i.e. if reminder is 2 then choose second element of list.

Step 4:- Check the selected element that are not used in last three times authentication, if the current element matched any one of last three times used element then repeat step III, if no then go to step V.

Step 5:- User enters numeric value or alphabet as prompted by server with respect to step III.

Step 6:- Server match entered value with saved value if match is found then send authentication is successful message to user otherwise invalid user message send to user and user is send back to step I to try again.

VI. RESULT ANALYSIS

For result analysis we implement this proposed technique in .NET and SQL server. For performance analysis proposed technique is compared with Finger Print recognition systems and OTP system used for authentication. This comparison is based on various dependency parameters as mentioned on Table 1 & figure 2.

Table 1: Comparison of Proposed Technique

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

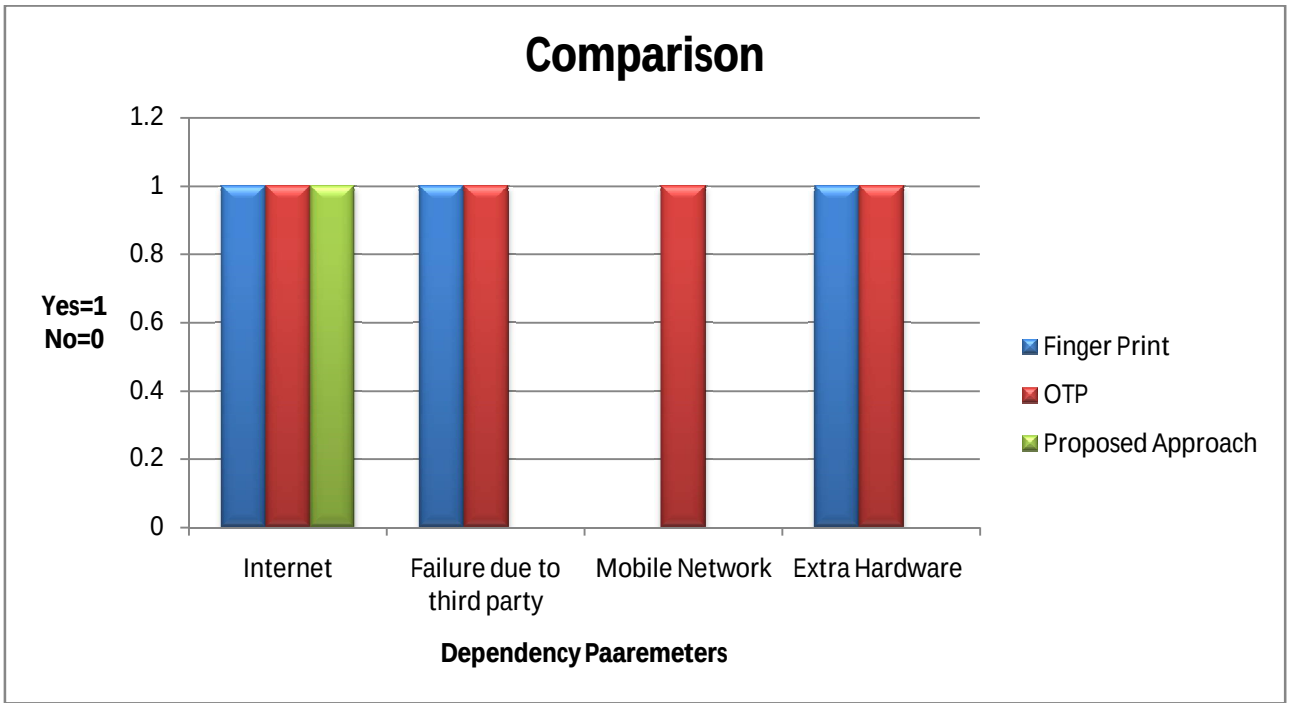


Figure 2: Comparison of proposed technique

In table 1 value 1 represent yes and value 0 represent No. For various attack we analysis our work that show in table 2 and figure 3.

Table 2: Preventions from various attacks

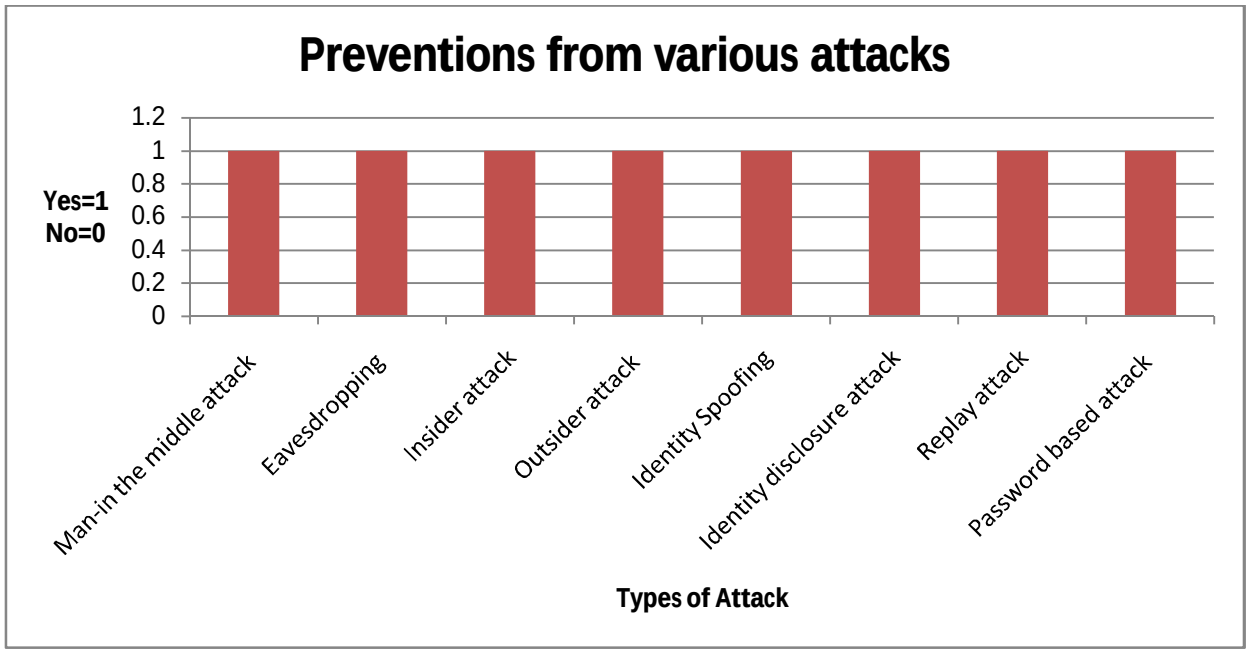
Attacks	Status
Man-in the middle attack	YES
Eavesdropping	YES
Insider attack	YES
Outsider attack	YES
Identity Spoofing	YES
Identity disclosure attack	YES
Replay attack	YES
Password based attack	YES

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016



1111

Figure 3: Preventions from various attacks

VII. CONCLUSION

In this paper we provide the new technique for authentication using user generated cryptography. Firstly we provide general introduction of cloud computing and authentication process after that we study previous implemented authentication techniques in previous work section. In proposed technique section we provide details description of our work and algorithm. In the result analysis section show that proposed authentication provide batter performance in the real world environment and it's also provide security from various attacks. On comparison of other technique it provides better security that show in result analysis.

REFERENCES

1. F. Fatemi Moghaddam, M. T. Alrashdan, and O. Karimi presented paper entitled "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments", Journal of Advances in Computer Networks, vol. 1, no. 3, pp. 238–241, 2013.
2. F. Fatemi Moghaddam, M. T. Alrashdan, and O. Karimi presented paper entitled "A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments", in Proc. IEEE 2nd International Conference on Cloud Networking (CloudNet), San Francisco, USA, November 2013.
3. F. Omr, S. Foufou, R. Hamia & M. Jarraya presented paper entitled "Cloud-based Mobile System for Biometrics Authentication", at IEEE 13th International Conference on ITS Telecommunications (ITST) in 2013.
4. Iehab AL Rassan & Hanan AlShaher presented paper entitled "Securing Mobile Cloud Computing using Biometric Authentication (SMCBA)", at IEEE International Conference on Computational Science and Computational Intelligence in 2014.
5. Napa Sae-Bae & Nasir Memon presented paper entitled "Online Signature Verification on Mobile Devices", at VOL. 9, NO. 6, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, JUNE 2014.
6. 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.
7. Nimmy K. and M. Sethumadhavan presented paper entitled "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography", 978-1-4799-2259-14/$31.00©2014 IEEE.
8. Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi, Shirin Dabbaghi Varnosfaderani presented paper entitled "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", 2014 IEEE Region 10 Symposium.
9. Hong Liu, Huansheng Ning, Qingxu Xiong & Laurence T. Yang presented paper entitled "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", at IEEE on Parallel and Distributed Systems, VOL. 26, NO. 1, JANUARY 2015.
10. Khyati Kantharia & Ghanshyam I Prajapati presented paper entitled "Facial Behavior Recognition using Soft Computing Techniques: A Survey", at IEEE Fifth International Conference on Advanced Computing & Communication Technologies in 2015.
11. Ashish Singh & Kakali Chatterjee presented paper entitled "Identity Management in Cloud computing Through Claim-Based Solution", at IEEE Fifth International Conference on Advanced Computing & Communication Technologies in 2015.