International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 7 Issue 7 July 2020

Robust and Amalgam Portrayal Authentication Mechanism

Krati Sharma[1], Rakesh Shivhare[2]
Research Scholar, Department of CSE, REC, Bhopal[1]
Assistant Professor, Department of CSE, REC, Bhopal[2]
skrati06@yahoo.com[1]

Abstract: *Cloud computing is the concept of using the large amount of remote services through a network using various least amount of resources, it provides these resources to users via internet. These storage systems provide a large virtual storage. When people relocate from web applications to cloud computing platform. There are many critical problems appeared with cloud computing such as security, privacy and reliability etc. But we find that security is the most important between these problems. The traditional form of accessing cloud services is to use a username and password as a security token. During login time, new security theft may arise like account/password sniffing, virtualization attack, or phishing attack. Even though existing authentication methods have addressed different security properties, there is still need of a secure authentication mechanism. So we provide a novel approach for authentication by using Portrayal Authentication Mechanism. This technique is more efficient which provide security to the cloud data storage.*

Keywords: *Cloud Computing, Authentication, Privacy, Security.*

1. INTRODUCTION

Cloud computing has become in the last years a paradigm that attracts more and more researchers. One of the main research areas in this field is the way in which common data and processing power can be shared and distributed across single or multiple datacenters that are spread across a specific geographical area or even the entire globe. In this context a new need for IT experts is increasing: the need to know exactly how, where and in what condition is the data from the cloud stored, processed and delivered to the clients.

Historically, the main drawback of Cloud technology adoption was given by the lack of confidence it gained from potential beneficiaries, especially casual Internet users. The main questions that still arise, concerning Cloud, are not about the technology, neither the costs involved, but about the ways of preserving information confidentiality and secure authentication methods. Moreover, considering the exponential growth of modern security threats, and their level of sophistication, the traditional authentication mechanisms are far from secure, nowadays. Password based authentication, which is still used in over 75% of web applications, has a major drawback, as passwords can be easily lost, stolen or guessed, through brute force attacks, social engineering, or even accidentally. As passwords are used, in most cases, to control access to cryptographic keys, too, even modern cryptosystems are vulnerable to many attacks.

Over the years, the trend of "Big Data" has prompted many organizations to acquire in-house cluster and storage infrastructures to support computing. Because these local resources are typically shared, the desired amount of computation may not always be available, which frustrates users with application deadlines. In these situations, the emergence of cloud computing has been timely. Its ability for users to immediately demand and obtain remote resources to help with computing and storage draws much interest from the computing community.

The cloud's key features include the pay-as-you-go model and elasticity. Users can instantly scale resources up or down according to the demand or the desired response time. This ability to increase resource consumption comes without the cost of over-provisioning, i.e., having to purchase and maintain a larger set of resources than what is needed most of the time, which is often the case for traditional in-house clusters. Some recent efforts have specifically focused on exploiting the elasticity of clouds for different services,

including a transactional data store, data-intensive web services, a cache that accelerates data-intensive applications and for execution of a bag of tasks.

Figure 1: A cloud is used in network diagrams

Figure 1 show the cloud used in network and over all structure of the cloud.

2. LITERATURE REVIEW

In this paper [2] authors focused on cost and time sensitive data processing in hybrid cloud settings, where both computational resources and data might be distributed across remote clusters. Authors developed a model for the class of Map-Reducible applications which captures the performance efficiencies and the projected costs for the allocated cloud resources. There model is based on a feedback mechanism in which the compute nodes regularly report their performance to a centralized resource allocation subsystem. The resources are then dynamically provisioned according to the user constraints.

Authors have extensively evaluated there system and model with two data-intensive applications with varying cost constraints and deadlines. There experimental results show that the system effectively adapts and balances the performance changes during the execution through accurate cloud resource allocation. They show that there system is effective even when one of the involved clusters drastically and instantly reduces its compute nodes. The error margins of our system's ability to meet different cost and time constraints are below 1.2% and 3.6% respectively.

Courtney In this paper [3], authors propose a simple and effective online signature verification system that is suitable for user authentication on a mobile device. The benefits of the proposed algorithm are as follows. First, a histogram based feature set for representing an online signature can be derived in linear time and the system requires a small and fixed-size space to store the signature template. In addition, since the feature set represents only statistics about distribution of original online signature attributes, the transformation is non-invertible. As a result, the privacy of the original biometric data is well-protected. Second, a user-specific classifier comprising of a user-specific quantization step size vector and its associated quantized feature vector can be trained using only enrollment samples from that user without requiring a training set from a large number of users. Several experiments performed on MCYT and SUSIG datasets demonstrate effectiveness of the proposed method in terms of verification performance as compared to existing algorithms.

Security analysis of online signature verification system as compared to that of 4-digits PIN, and two usability metrics is also presented. Further investigation includes the use of other biometric key binding approaches, like fuzzy commitment, in order to strengthen security of the system, even when stored templates, helper data etc., are compromised, while preserving verification performance. Lastly, it is possible to derive a fusion approach by combining the proposed method with other existing approaches, e.g., DTW, HMM-based, etc., in order to improve verification performance, especially for applications where privacy of the signature traits is less critical.

In this paper [4], 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 study also aims to contribute evidence of a bias in the user choice of images and considers the impact this could have on guessability. 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.

The combination of the cloud computing and mobile computing creates mobile cloud computing and also introduce security threats such as unauthorized users access. The authors focus in this research [5] is on the mobile cloud and protecting mobile cloud resources from illegitimate access. Biometric recognition will be used in the near future in mobile devices. The proposed solution by authors for authenticating mobile cloud users using the existing mobile

device camera as a fingerprint sensor to obtain a fingerprint image, and then process it and recognize it. Results show that the proposed solution has added value to keep performance at an accepted level.

In this paper [6], authors used principal curves approach for fingerprint minutiae extraction then these stored them in a DB on a cloud, then authors used the Bio-Hash function to secure the biometrics templates. Also they compared there approach with the approach presented in previous researches, and calculated the error rates for their approach and proved that these increase the system performance by 25%.

In this paper [7], authors present some advances on offline signature identification. Form the analysis of the recent literature in the field some of the most valuable approaches are presented and the most interesting directions for further research are highlighted.

In this paper [8], authors demonstrated how Cloud-Trust can be used to assess the security status of IaaS CCSs and IaaS CSP service offerings, and how it is used to compute probabilities of APT infiltration (high value data access) and probabilities of APT detection. These quantify two key security metrics: IaaS CCS confidentiality and integrity. Cloud-Trust also produces quantitative assessments of the value and contribution of specific CCS security controls (including several optional security controls now offered by leading commercial CSPs), and can be used to conduct sensitivity analyses of the incremental value of adding specific security controls to an IaaS CCS, when there is uncertainty regarding the value of a specific security control (which may be optional and increase the cost of CSP services).

In this paper [9], authors propose the implementation of a voice-based Fuzzy Vault authentication mechanism, for secure access and encryption support within Cloud platforms and Cloud shared storage. The experimental results, focused on evaluating the performances of the biometric matcher, have shown FRR rates varying from 0% to 32% and FAR rates varying from 2.5% and 11.3%.

In this paper [10], authors propose a new image integrity authentication scheme based on fixed point theory. In the proposed scheme, the following three criterions are considered for selecting an appropriate transform $fk(\cdot)$ whose fixed points are used for image integrity authentication. 1) Fragility: the fixed points of $fk(\cdot)$ must be sparse; 2) easy calculation: a fixed point can be easily found by few iterations; 3) transparence: a fixed point can be found in a very small neighborhood of a given image function. They construct an appropriate transform $fk(\cdot)$ satisfying these criterions, based on the Gaussian Convolution and Deconvolution, called GCD transform. After establishing a theorem for the existence of fixed points of the GCD transform $fk(\cdot)$, these give algorithms for a quick calculation of a fixed point image which is very close to the given image, and for the whole image integrity authentication scheme using the obtained fixed point image. The semi-fragility problem is also mathematically considered via the commutativity of transforms. Experimental results show that the proposed scheme has very good performance.

In this paper [11], 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 behavior 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 behavior 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 [12], authors show why claim-based identity solutions are required and how to use by the cloud service provider in cloud applications.

In this paper [13], 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. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for privacy preservation in cloud applications.

In this paper [14], authors developed an iris recognition algorithm supported Fisher algorithm which may be run in a very lighter computing platform. Experiments conducted

with CASIA information shows exciting results wherever the system achieves a awfully high accuracy. Iris recognition may be a biometrics authentication system mistreatment iris image. it's one in all the foremost reliable biometrics systems. The systems but need substantial computing power. therefore it's not been able to penetrate the market however.

This paper [15] discusses the various ICA based mostly techniques that are utilized in last decade. This paper reviews the comparative study of various face recognition techniques that is predicated on ICA. The vital a part of this survey is that the discussion of previous work of face recognition associated with ICA. There are totally different strategies obtainable associated with ICA. Also, compare the various strategies in tabular kind. During this survey paper offer the transient summary of "How to recognition face using image processing".

In this paper [16] the human behavior is recognized from a collection of video samples and therefore the features are extracted victimisation HOG transform. KNN classifiers are accustomed classify the features extracted from the videos. The HOG feature primarily based analysis has achieved higher recognition and accuracy of 93%compared to the prevailing ways. There are many factors affects this Gait Authentication which may be classified into 2 classes. they're (i) External factors: angles, lighting atmosphere, garments that have same color as background and alternative external objects. (ii) Internal factors: changes in gait because of natural effects like illness, ageing, pregnancy, gaining or losing weight.

In this paper [17] authors projected a sturdy face recognition technique by victimisation native binary pattern and bar graph of adjusted gradient feature extractor and descriptors. during this study author have found that LBP feature extractors have virtually simple fraction higher accuracy result than the HOG feature extractors that doesn't have that a lot of distinction. they need tested it for authentication purpose to register to their device by taking one label as an administrator and it gave important results.

In this paper [18], authors present a completely unique security framework for NFC Secure Element-based Mutual Authentication and Attestation for IoT access with a user device like a mobile device using NFC based mostly.

Host Card Emulation (HCE) mode for the primary time. The recently framework for NFC Secure Element-based Mutual Authentication and Attestation for IoT access provides a completely unique on-demand communication and management of IoT devices with security, privacy, trust and proof-of-locality using the NFC-based HCE mode and secure tamper-resistant SE and TPM modules. this method cannot verify the dynamic device state like Control-Flow Integrity.

Author proposes a noisy vibration method for cloaking vibration sounds throughout pairing against such attacks. The method only needs a speaker for emitting the masking sound throughout key transmission [19]. They conjointly study motion sensor exploits against this scheme and compliment it with extra measures to mask vibration effects on motion sensors. There analysis shows that whereas vibration pairing could seem to be a beautiful mechanism for guaranteeing the protection and trust in an IoT network, it must be protected against acoustic aspect channel attacks by defensive measures like masking signals that are low price and straightforward to implement.

In this paper [20], author studied the ensemble performance of biometric authentication system that is supported secret key generation. Bearing on an ensemble of codes supported Slepian–Wolf binning, we've provided elaborate, sharp analyses of the false–reject and false–accept chances, in terms of error exponents, for a large category of stochastic decoders that covers the optimum MAP decoder, in addition as many extra decoders, as special cases. Converse bounds are derived in addition.

Author propose a physical-layer challenge-response authentication approach during this paper [21] supported combined shared secret key and channel state information (CSI) between 2 legitimate nodes in an orthogonal frequency division multiplexing (OFDM) system. The projected approach used although the correlation of channel coefficients exists, which might be exploited to extract the shared secret key in standard approaches. Moreover, channel coding is utilized to mitigate the distinction between the 2 calculable channels in addition as channel fading and background noise. Thus, they ascertained that within the projected approach as a physical-layer authentication approach, the decoder's output are often used for authentication and provided a reliable decision below active attack.

3. PROPOSED ARCHITECTURE

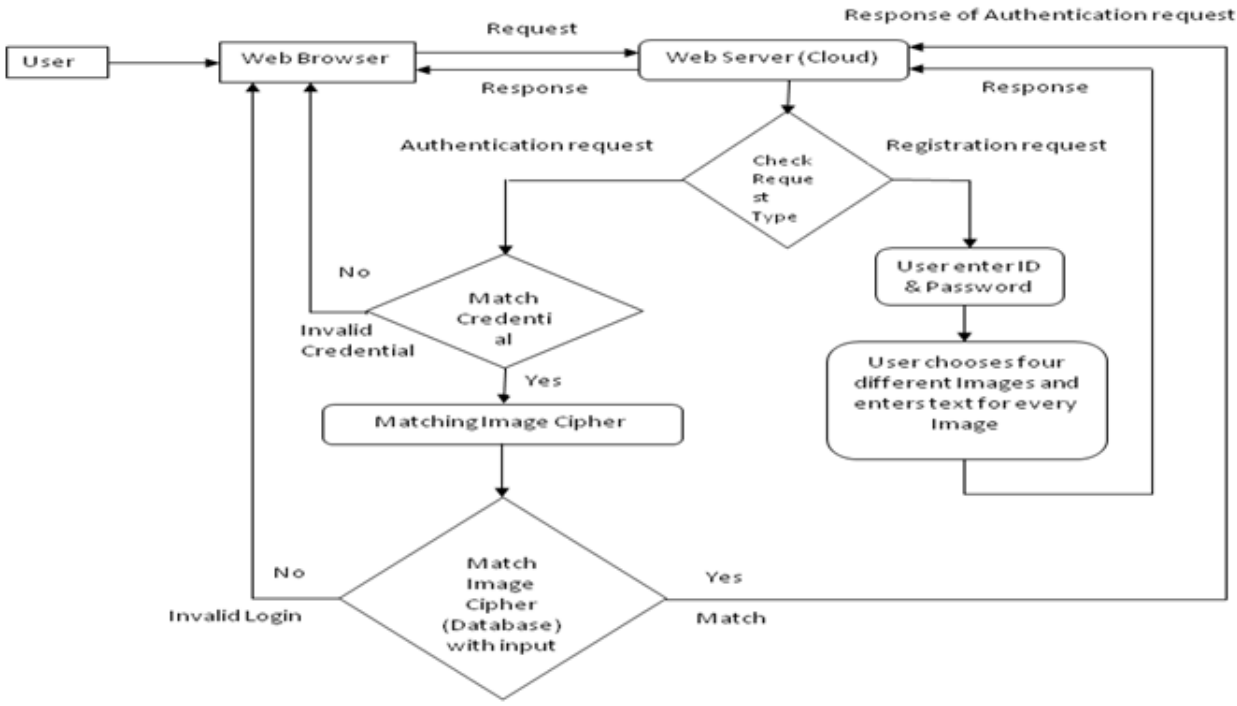

Figure 2: Proposed Architecture of Portrayal Authentication Mechanism

The functional flow of the algorithm is given in the figure 2.

3.1 Algorithm

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

1. Registration:-

I. User fills required details for registration like User Name, Password, Email, Address and stores it in database.
II. After that user chooses one Image from list of images and inserts cipher value (It should be number or text) of its choice with respect to the Image.
III. To complete the registration, step II is repeated four times, every time Image chosen in previous steps is removed from Image list.

2. Login:-

I. User fills user name and Password.
II. Systems checks user name and password in database if match is found then step III is followed otherwise Go to Step I.
III. List of stored image cipher patterns is retrieved from the database (8 elements as per registration phase i.e. 4 Images & their four text 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.

IV. Check the Image 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.
V. User inserts cipher value or chooses an image cipher as prompted by system with respect to step III.
VI. If match is found then authentication is successful otherwise user is send back to step I to try again.

4. SIMULATION AND RESULT

4.1 Comparison on various types of dependency parameters

Various types of dependency parameters which causes system to fail in certain circumstances like

- Internet
- Extra hardware required
- Mobile network
- Failure due to third party

If for the authentication purpose OTP and Finger Print recognition system is used which need a lot of dependency in terms of extra hardware, software, mobile network and failure due to third party; but proposed system need only internet connectivity. The proposed approach is also compared with the OTP (one Time Password) and finger print techniques as shown in table 1.

Table 1: Comparison based on various dependency parameters

Dependency Parameter	OTP	Biometric	Proposed Approach	Face Recognition
Internet	1	1	1	1
Extra Hardware	1	1	0	1
Mobile Network	1	0	0	0
Failure due to third party	1	1	0	1

The result shows that OTP authentication mechanism depends on internet, it needs extra hardware, mobile network and also depends on third party. If the third party fails to do the work then the OTP system also fails. In case of finger Print Technique, is also depends on all the dependency parameters except Mobile Network. But the proposed work is depends only on the Internet. So the failure rate of proposed work is decreased as compared to other techniques as shown in Figure 3.

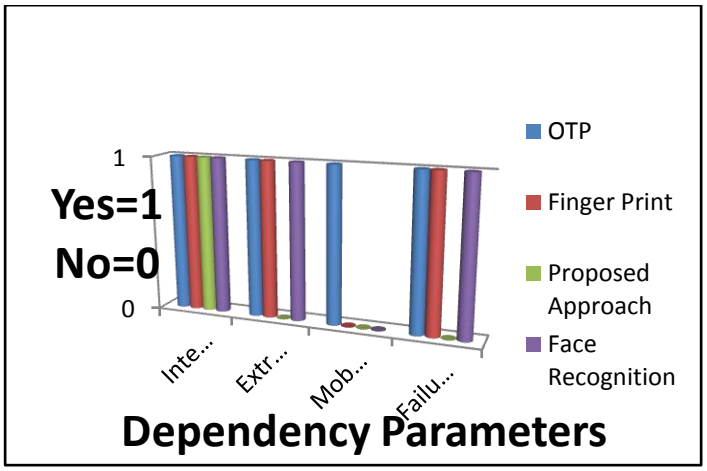

Figure 3: Comparison of Proposed Approach based on Dependency Parameters

4.2 Comparison based on various types of Attacks

The authentication security on the cloud is the very important because the various type of attacks are made by intruders for gathering important data and information of cloud users. The existing authentication systems are not much capable of preventing the cloud from the various attacks while the proposed system can prevent the cloud data from almost all the attacks.

Table 2: Prevention from various attacks

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

As shown in table 2 is the prevention of our proposed work from various attacks in the attack.

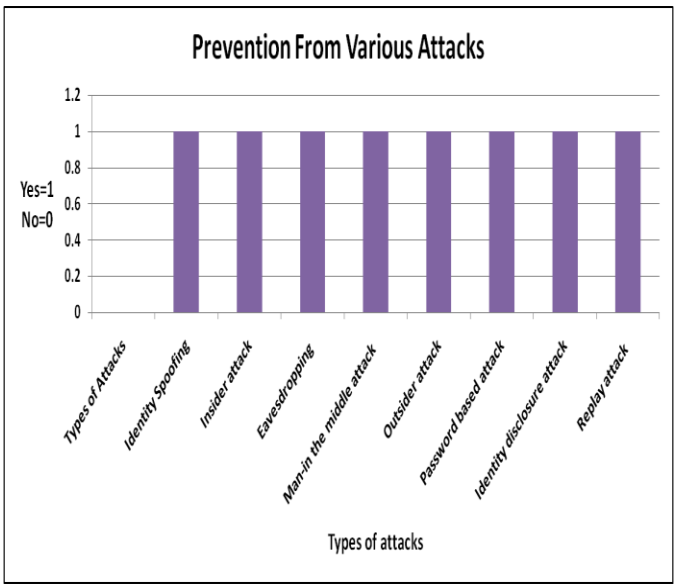

Figure 4: Prevention from various attacks.

5. CONCLUSION

In the real world, every people are work online and saved its important data in the cloud. So security is the measure concern today. Various researches are made for data and authentication security. In literature review section we study various authentication technique most of the techniques are Id & password based and extra hardware are required for authentication like Thumb expression based authentication, Retina scan based authentication, Mobile OTP-based authentication etc. But in our proposed methodology no extra hardware needed and also it provides security from various types of attacks. The result analysis section in above describes that our proposed mechanism provide prevention from various type of attacks like Password attacks, Insider attack, Outsider attacks etc. Also the proposed method is less dependent on extra hardware as compared to other authentication mechanisms.

REFERENCES

[1] Abhilasha Bhargav-Spantzel and Steve W. Deutsch," Platform Capability Based Identity Management forScalable and Secure Cloud Service Access", GC'12 Workshop: First International workshop on Management and Security technologies for Cloud Computing 2012.

[2] Tekin Bicer, David Chiu & Gagan Agrawal presented paper entitled "Time and Cost Sensitive Data-Intensive Computing on Hybrid Clouds" at 2012, 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.

[3] 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.

[4] 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.

[5] Iehab AL Rassan & Hanan AlShaher presented paper entitled "Securing Mobile Cloud Computing using Biometric Authentication (SMCBA)" at IEEE 2014 International Conference on Computational Science and Computational Intelligence.

[6] Heba M. Sabri, Kareem Kamal A.Ghany, Hesham A. Hefny & Nashaat Elkhameesy presented paper entitled "Biometrics Template Security on Cloud Computing" at 978-1-4799-3080-7/14/$31.00 @ 2014 IEEE.

[7] Heba D. Impedovo, G. Pirlo & M. Russo presented paper entitled "Recent Advances in Offline Signature Identification" at IEEE 2014 14th International Conference on Frontiers in Handwriting Recognition.

[8] Dan Gonzales, Jeremy Kaplan, Evan Saltzman, Zev Winkelman & Dulani Woods presented paper entitled "Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds" at IEEE TRANSACTIONS ON JOURNAL GONZALES, TCC-2014-03-0102.

[9] Marius-Alexandru Velciu1, Alecsandru P˘atra¸scu & Victor-Valeriu Patriciu presented paper entitled "Bio-cryptographic authentication in cloud storage sharing" at 9th IEEE International Symposium on Applied Computational Intelligence and Informatics • May 15-17, 2014 • Timişoara, Romania.

[10] Xu Li, Xingming Sun & Quansheng Liu Patriciu presented paper entitled "Image Integrity Authentication Scheme Based on Fixed Point Theory" at IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 2, FEBRUARY 2015.

[11] 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.

[12] 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.

[13] Hong Liu, Huansheng Ning, Qingxu 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.

[14] Hermawan Nugroho, Hamada Rasheed Hassan Al-Absi and Lee Pei Shan, "Iris Recognition for Authentication: Development on a Lighter Computing Platform", in IEEE 978-1-5386-8369-9/18/$31.00 ©2018.

[15] Rajat Naik, Dr. Dhirendra Pratap Singh and Dr. Jaytrilok Choudhary, "A Survey on Comparative Analysis of Different ICA based Face Recognition Technologies", Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1.

[16] S. Joul Monisha and G. Merlin Sheeba, "Gait Based Authentication with Hog Feature Extraction", in IEEE 978-1-5386-1974-2/18/$31.00 ©2018.

[17] Melkye Wereta Tsigie, Rasika Thakare and Rahul Joshi, "Face Recognition Techniques Based on 2D Local Binary Pattern, Histogram of Oriented Gradient and Multiclass Support Vector Machines for Secure Document Authentication", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2.

[18] Divyashikha Sethia, Daya Gupta and Huzur Saran, "NFC Secure Element-based Mutual Authentication and Attestation for IoT access", JOURNAL OF TRANSACTIONS ON CONSUMER ELECTRONICS, VOL. 14, NO. 8, SEPTEMBER 2018, DOI 10.1109/TCE.2018.2873181, IEEE, Transactions on Consumer Electronics.

[19] S Abhishek Anand and Nitesh Saxena, "Noisy Vibrational Pairing of IoT Devices", DOI 10.1109/TDSC.2018.2873372, IEEE.

[20] Neri Merhav, "Ensemble Performance of Biometric Authentication Systems Based on Secret Key Generation", DOI 10.1109/TIT.2018.2873132, IEEE.

[21] Jinho Choi, "A Coding Approach with Key-Channel Randomization for Physical-Layer Authentication", DOI 10.1109/TIFS.2018.2847659, IEEE.