Authenticating Cloud & Data Center with Iris

Nikhil Kumar, Dr.Yogesh Awasthi, Prof (Dr.)R.P. Agarwal

Abstract— **Cloud computing service providers provide a vast range of IT services to their clients from last few years but till now most of the IT companies have their own Data Centers/Servers due to drawback of user authentication problem in Cloud Computing Account. There is no doubt that Cloud Data Server provides fast and reliable software services to its clients. Authentication for identifying authorized user is a major issue. The user use to store and retrieve their confidential data over cloud to make it available worldwide. To resolve this issue of authentication of client of cloud service provider uses secured biometric authentication technique which bridges the gap between inadequacy of existing authentication solution. Based on authentication such as Fingerprint and Iris. In this paper author explores the techniques/methods how the user can authenticate a document using a combination of unique keys which will be user's Iris and fingerprint. The Iris code and fingerprint code both will always be matched with the owner of the cloud account.**

Index Terms— **Biometric Authentication, Cloud Security, Fingerprint, Iris.**

I. INTRODUCTION

Cloud computing is a technology that outsources the resources for the organizations from Third party companies. In this computing users access virtual severs and on payment as per usage. Nowadays organizations don't purchase hardware, software or storage they just adopt cloud services that provide great benefits. Cloud computing is using resources worldwide in any geographical location virtually by using internet. Cloud computing is used to build a security between cloud service provider and its client. Cloud computing needs security algorithms as all the data and resource utilization is over the internet.

Cloud helps in developing web applications which could be made to run on any device. It helps in standardizing applications and other business requirements. Because of Cloud Computing the user can use the services virtually. Cloud computing technology is used to build a security between Cloud Service Provider and the end-user.

Authentication means comparing credentials available on the file in the database of authorized users on a local machine or server or online database if credentials got matched then the access to the data is allowed.

II. EXISTING SYSTEM

In today's computer-driven era, data theft, identity theft and hacker's successful login are rapidly increasing problems. Everyone internet users have multiple accounts and multiple passwords on an ever-increasing number of computers and Web sites. Now a day's users are fed up with remembering password for various applications, software's, websites, desktop password, banking transactions password. User need to create very complex password to make it unique. The highly confidential department need a better authentication method in which user need not to remember complex password and is difficult to crack the password. Currently most of the industries are not migrated to the cloud computing due to security issues.

III. PROPOSED WORK

This paper deals with the new technique based on a new Authentication model which will use biometric scanning to provide a unique combination key which is very difficult to crack. This model scans all the user's fingerprints and scan iris with and with their combination a new and better idea to provide more secure mobile cloud computing. In this model the user will place the figure on the scanner and look into the eye scanner and the cloud computing account will get login without remembering any password. Login process and account security both will get unlocked by the authorized user with the same proposed model.

This model will have some priority bases login process in which iris will have always high priority and fingerprint will have low priority. This model is suitable for highly secured information's like Defense, Banking, and Govt. offices.

IV. BIOMETRIC SECURITY

Biometric security involves the identification of user by their unique characteristics. In computer field it is used for access control based on the the physical characteristics of the person. The biometric data is used for security access of the system since it does not get change during lifetime and is unique Biometric security consists of fingerprint, eyes, hands, DNA, speech, facial characteristics, etc. This systems works on the basis of pattern recognition system. In this system every time the user's fingerprint and iris got scanned using scanners and both were matched with the cloud service provider database to check the identity of authorized user.

The cloud service provider at the time of Account opening scan user's fingerprint and Iris and store them in their database for verification at the time of login.

Nikhil kumar, **Dr Yogesh Awasthi, Prof.(Dr.) R.P.Agarwal** Computer Science Department , Shobhit University, India.

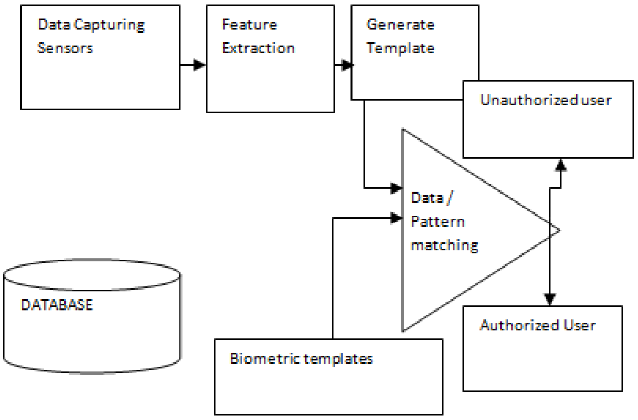


Fig.1: Basic block schematic of a typical biometric security system

V. FINGERPRINT

Fingerprint is the unique for every human being all over the world. As finger generates a unique code. Fingerprint scanning provides an identification of a person based on the acquisition and recognition of unique patterns of ridges in a fingerprint. A fingerprint is made up of ridges and furrows as well as characteristics that occur at minutiae points (i.e. ridge bifurcation or a ridge ending).

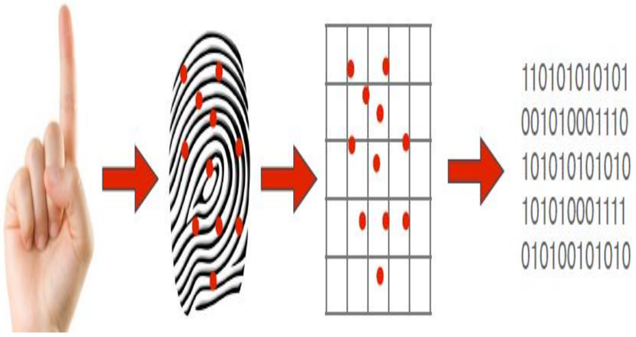


Fig.2: Every finger will generate a unique binary code

The binary code generated is stored in databases of service provider and every time user login similarly the code generated by the user hand which will be matched with this binary code. On matching user will get successful login

VI. IRIS

Iris is a complex pattern which contains many features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette. Each iris is unique and extremely difficult to surgically tamper iris texture information and it is possible to detect artificial irises. Although the early iris based identification systems need user participation and were expensive. Efforts are underway to develop more user-friendly and cost-effective versions. Both accuracy and speed of iris-based identification are highly encouraging and point to the feasibility of large-scale recognition using iris information. Due to this and to the above described characteristics, iris is considered one of the best biometric traits, although this evaluation depends on the application.

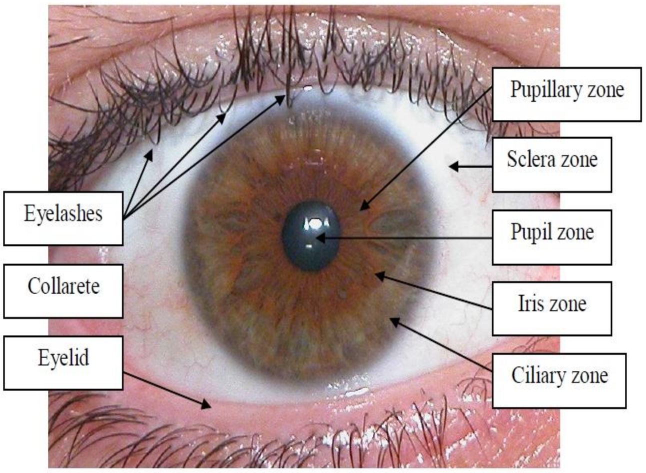


Fig.3:Typical human eye

VII. WORKING OF IRIS RECOGNITION

On considering image an iris as a system and making a 2D Gabor wavelet filters and then mapping the segments of the iris into phasors (vectors). These phasors include information on the orientation and spatial frequency ("what" of the image) and the position of these areas ("where" of the image).This information is used to genrate the IrisCodes

Iris patterns are described by an Iris Code using phase information collected in the phasors. The phase is not affected by contrast, camera gain, or illumination levels. The phase characteristic of an iris can be described using 256 bytes of data using a polar coordinate system. Also included in the description of the iris are control bytes that are used to exclude eyelashes, reflection(s), and other unwanted data. To perform the recognition, two IrisCodes are compared mathematically by the amount of difference between two Iris Codes using Hamming Distance (HD) as a test of statistical independence between the two Iris Codes. If the Hamming Distance results less than one-third of the bytes in the IrisCodes are different, the Iris Code fails the test of statistical significance, indicating that the IrisCodes are from the same iris. Therefore, the key concept to iris recognition is failure of the test of statistical

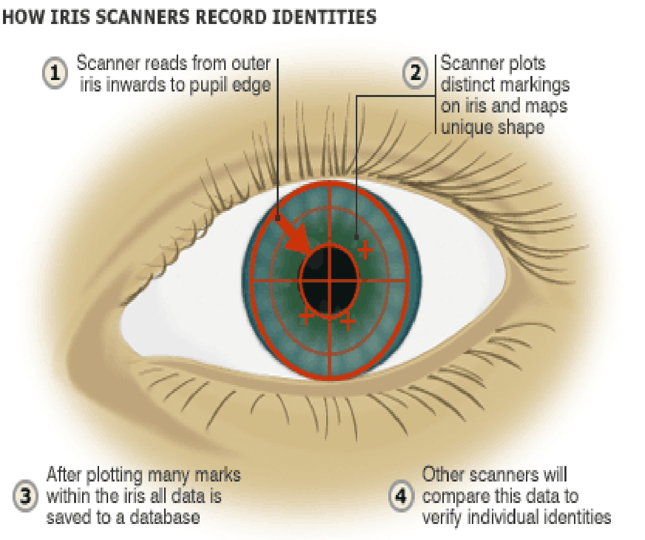

HOW IRIS SCANNERS RECORD IDENTITIES
1 Scanner reads from outer iris inwards to pupil edge
2 Scanner plots distinct markings on iris and maps unique shape
3 After plotting many marks within the iris all data is saved to a database
4 Other scanners will compare this data to verify individual identities

Fig.3: Working of Iris scanners

Iris at the time of account opening in cloud will firstly go through enrollment process in which scanned iris and its generated Iriscode will be stored in the database for matching at the login verification time.

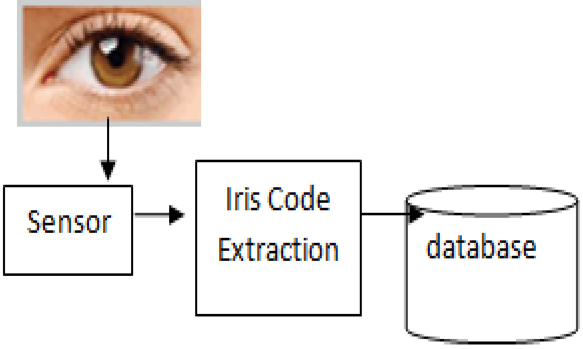


Fig.4: Enrollment process

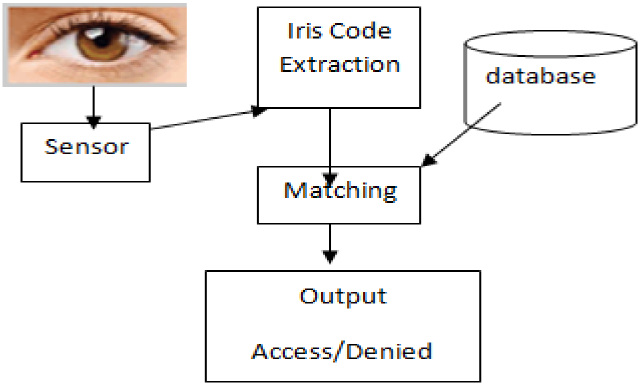
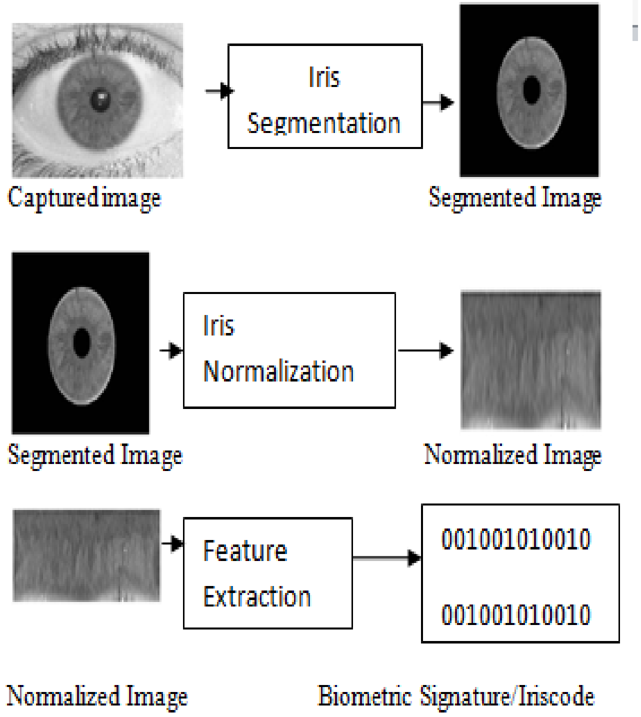


Fig.5: Verification Process

Iris recognition process

The step by step process of Iriscode matching shown in below figure



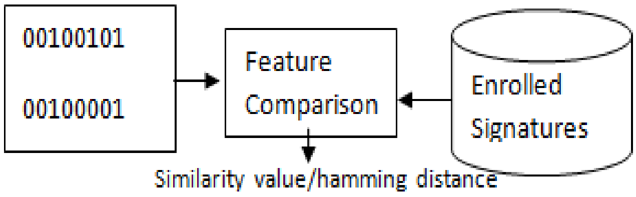


Fig. 6: Steps involved in iris recognition

In recognition process enrolled iris code and scaned iris code are compared using hamming distance and if the hamming distance is minimum i.e zero or one then this means that both the iris is of same user and this is how the user gets most secured authentication using iris and fingerprint combination as proposed model in this paper

VIII. CONCLUSION

By implementing the proposed mechanism, the online system security will be increased to a large extent and this combination of two biometric passwords, the percentage error is reduced to a minimum and the clients will get a unique and robust secure system. In this paper some directions on how to move existing biometric technology to a cloud platform were presented. In this system fingerprint service was developed and integrated with the iris recognition technology and in future a framework Module will be developed for every authentication gateways. This method in use iris feature extraction that uses cumulative sum based change analysis. In order to extract iris features, normalized iris image is divided into basic cells. And iris codes of these cells are generated by proposed code generation algorithm, which uses cumulative sums of each cell. Proposed method is relatively more secure against existing methods. A proposed mechanism is used to provide security at every authenticating gateways or cloud security. This proposed scheme provides highly reliable and secure service to its cloud clients.

REFRENCES

[1]Ari Juel and Alina Opera, "New approaches to security and availability for cloud data "Institute of Technology, RSA Laboraties Cambridge,ma, USA.

[2]E. Sasi and R. Saranyapriyadharshini "secured biometric authentication In cloud sharing system" IJCSMC, Vol. 4, Issue. 3, March 2015.

[3]Y. Shu, Y. Gu, and J. Chen, "Sensory-Data-Enhanced Authentication for RFID-Based Access Control Systems," Proc. IEEE Ninth Int'l Conf, Mobile Ad Hoc Sensor Systems (MASS), 2012.

[4]D.Kesavaraja, D.Sasireka and D.Jeyabharathi "Cloud Software as a Service with Iris Authentication"Journal of Global Research in Computer Science, 1 (2), September 2010.

About the author

Nikhil kumar did B.Tech (CS) in 2011. Thereafter he worked for 3 years as a Network Engineer in Prakash IT Consulting & Solutions Pvt. Ltd. And currently pursing M.Tech(CS) from Shobhit University, Meerut, U.P.

Dr. Yogesh Awasthi received his B.Sc. degree from Lucknow University in 1997, MCA degree in 2002 from RGTU, Bhopal and M.Tech. degree in 2009 from UPTU,Lucknow and Ph.D. from Shobhit University, Meerut in 2015. He has joined the Shobhit University in 2004 as a lecturer. Presently he is working as Asst. Professor. He has published many papers and articles in international and national journals / conferences. His research area includes Watermarking Techniques, Cloud Computing and Automata Theory.

R.P. Agarwal received B.Sc. degree from Agra University, B.E. degree in E&CE with Hons. in 1967 and M.E degree from poona university in 1970. He received his Ph.D. from University of Newcastle upon Tyne, UK, in 1977. Dr.Agarwal joined Department of E&CE, IIT, Roorkee, as a Lecturer in 1970, where he worked as Professor and Dean till 2009. Thereafter he worked as a vice-chancellor of H.S.Gour Central University, Sagar, M.P. & Bundelkhand University, Jhansi, U.P. & Shobhit University, Meerut, U.P. He is currently working as Academic Advisor at Shobhit University, Meerut, U.P. His research interests include signal processing systems and VLSI technology, Computer Engineering and systems.