www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 3 March 2017, Page No. 20410-20413
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i3.01

Biometric Authentication using Software as a Service in Cloud Computing

Shreya Gawade[1], Anand Bharti[2], Ashish Raj[3],Shweta Madane[4]
[1]Dr.D.Y Patil Institute of Technology, Pimpri, Pune University, India
gawadeshreya10@gmail.com
[2]Dr.D.Y Patil Institute of Technology, Pimpri, Pune University, India
anand.bharti980@gmail.com
[3] Dr.D.Y Patil Institute of Technology, Pimpri, Pune University, India
ashishraj6124@gmail.com
[4] Dr.D.Y Patil Institute of Technology, Pimpri, Pune University, India
shwetamadane432@gmail.com

Abstract: Today many cloud users are facing the major problem of fake logging in and data theft. So it is required to authenticate the cloud user that requests access to an account for providing privacy and security. However, the techniques used for authentication so far were not capable to guarantee the same and thereby kept the data at high risk. So, we are using the concept of Biometric Authentication along with Data compression and Data Encryption. Most of the techniques of Biometric Authentication in Cloud face performance issues like time and space complexities. So it is a need to measure these flaws. This paper eventually studies all the possible techniques relevant to Biometric Authentication and upgrade the system to a new level.

Keywords: Biometric Authentication, Finger Recognition, Finger Extraction, Encryption

1. Introduction

Today Cloud Computing is becoming a hot trend in IT industries. Most of the enterprises are using cloud for storing and maintaining their huge data on cloud servers. But security of critical data over the cloud has become a concern for both cloud service users and providers. Traditional authentication mechanism like password, key generation, encryption mechanism has failed. Hackers are able to crack these passwords. So, the data is not secure until we have a secure mechanism to protect the data from intruders and hackers.

In this paper, we are presenting a secure authentication mechanism unlike password or key which can't be hacked easily. Biometrics is an automatic identification of a person by using certain physiological features associated with the person. Biometrics data is unique for every individual. So our project aims at using Biometric data of user for the authentication process. Biometric System is a combination of sensors, feature extractor and matching modules which implements biometric recognition algorithms. The sensors scan the biometric trait of the user and produce its digital representation. A quality check is generally performed to ensure that the acquired biometric sample is reliable and can be processed by the subsequent feature extraction and matching modules. The feature extraction module will discard the useless and extraneous data present in the taken sample and extracts useful information called features that can be used for matching. During matching, the query biometric sample is matched with the reference information which is stored in the database to establish the identity associated with the query. This operation is done in two stages, first is the Enrolment and second is the recognition. In Enrolment stage the biometric information of the person is stored in the database. We are implementing our project to match fingerprint data of user for authentication in cloud. We will store the users fingerprint data in compressed form on a cloud database for the time and use that for matching whenever a user tries to login the next time.

We are using Biometric scanner to extract fingerprint of user. Fingerprint data will be transmitted in the compressed from for security of users Biometric data. There is a matching module to match the fingerprints against the one stored on the database. If the fingerprint matches, it will allow the registered user to login.

Since it will be an overhead for the cloud service providers, our project aims at creating a separate web client between user and cloud service provider to provide a secure service of Biometric Authentication.

This paper is being classified as Section II dedicates for related work, Section III describes the proposed system and its architecture and Section IV concludes the effort of this paper.

2. Literature Survey

This section of Literature Survey eventually reveals some facts of Biometric Authentication based on the analysis of many authors work as follows :

Chandra ShekharVorugunti [1] has introduced a new concept of BioAaaS to maintain secure authentication. Based on SAAS model of Cloud it provides a light weight and secure authentication mechanism. It contains two steps for authentication. First is Enrolment and next is Verification. In Enrolment process the biometric data is converted into a binary form. The feature extractor then converts the binary string into a set of features. In verification process same process will be processed when the user logins to the cloud. The matching module matches the features of the stored data and login data. Thus they have provided a service to do heavy weight cryptographic encryption and decryption operation on user's biometric data.

D J Craft [2] reports on fast hardware implementation of lossless data compression algorithms. It proposed Adaptive Lempel-Ziv Algorithm (LZ1 & LZ2). LZ algorithm are symbol based that is they operate one data one character at a time. They achieve compression by locating frequency occurring sequences of such symbol in input data stream. ALDC have two extensions as BLDC & CLDC. BLDC pre-processing works well on only bitmapped image data. CLDC is combination of ALDC & BLDC. The main difference between LZ1 & LZ2 is in the data structure employed & the way reference to sequence are coded.

Cong Li et al. [3] proposed Burrow Wheeler Transformation based DNA sequence data multi-compression using OpenMP & MPI. They proposed data compression (DNA sequence) using fewer bits rather than encoded data to represent information. BWT based DNA compression includes few steps. First DNA sequence data is encoded with 0/1 which has 4 characters. Then BWT transformation is performed over it. Again MTF transformation is performed. Then we compress data with classical algorithm.

Kiran Kumar K et al. [4] have described that there are two properties of fingerprint namely uniqueness and permanence that are used for identification and verification. These properties are judged by minutae and ridges. The method used in this paper has 8 stages. They are gray-level fingerprint image, binarization, thinning, minutae extraction, false minutae, matching scores, ridges extraction, minutae and ridge score fused using strength factor. The block filters preserve the outermost pixels along each ridge.

Jeff Collier [5] proposed a system for developing a software that would address the challenges such as in-memory map/reduce. It also deals with the node that has ability to leave and re-join the cloud by applying compression and image processing algorithms.

Hu Chun et al. [6] have proposed a situation where biometric data is kept encrypted in whole process of transmission and matching. It uses two approaches homomorphic encryption and garbled circuit. It provides highly computing capability.

Surender Sharma et al. [7] have introduced health care monitoring system application that provides the patients with necessary healthcare information yet it also gives a chance to threats of intervention that would make the critical data insecure. They have used Body Area wireless sensor network as monitoring component. The cloud based HMA was therefore developed using master slave like pattern, where the master could have generic functions while slave would have functionalities specific to the medical condition. Thus they have utilized biometric encryption for providing protection to the data. Here the user's biometric characteristics work as decryption key here fuzzy extractor scheme has been used to convert the scanned fingerprint data to some random string and an helper string to apply cryptographic techniques. This framework accomplishes both the goals, secure access and data protection.

Krishnaraj Madhavji Sunjiv Soyjaudah [8] discussed about eight points of vulnerabilities that can be hacked. In cloud data is moved dynamically so security is a major concern and there are the problems which arise in the management of biometric data. So a cancellable biometric authentication system is proposed by him.

Cancellable Biometric Authentication is a concept in which the original image is first distorted then shared on cloud. This distorted biometric image is used for authentication. This provides security and privacy as the original biometric are never revealed to authentication server. Data Hiding is also done using this technique to overcome the replay attack. This is done by secretly embedding the private information in biometric image.

Dr. Anandhakumar P et al. [9] has addressed the issues that arouse during storing different documents and files and photo contents on Cloud. Huge amount of photos are maintained by cloud providers. Huffman coding cannot achieve high levels of compression also all the binary strings or codes in the encoded data are of different lengths. So it is difficult to decode. The representative signal(RS) based approach is suitable only when images are highly correlated to each other so it fails badly in case of illumination changes. To overcome these drawbacks LZ-77 algorithm is proposed in this paper. Lz-77 replaces the repeatedly occurring data with reference to single copy which is already existing in an uncompressed data stream. It uses length-distance pair to encode the match. As compression is in cloud environment, k-means algorithm is used to transfer up by using Map-Reduce concept.They also proposed an idea for effective compression of photo albums which also reduces the time complexity.

Abdullah A. Albahdal et al.[10] explored the mutual benefits of biometrics technology and cloud computing. Presently cloud providers mainly depend on password authentication to authenticate their clients. However, password based authentication suffers from a lot of problems. The most common criticism of password-based authentication is the lack of authenticity. The major barriers preventing individuals and organizations from taking advantage of the cloud are security and privacy challenges. Cloud storage service model provides clients with a remote storage that comes with many desirable features including on-demand model, scalability, accessibility, and cost reduction. Identity management refers to the administration of users' identities within a system. It includes establishing users' identities, managing users' authentication and authorization, and maintaining users' permissions. The promising features of the cloud are attractive to biometrics systems. These features include the unbounded storage and processing power, elasticity and flexibility, and cost reduction. Biometrics systems can migrate data to storage or processing in the cloud. Biometrics systems rely on computation-intensive processes to perform the different biometric functions such as identification (1:N), verification (1:1), and de-duplication (N:N) process. Biometrics with its strong authentication properties can be leveraged by the cloud to enhance the security of the cloud and to offer new models of service.

Dasardha Ramaiah K et al. [11] proposed a novel approach to detect most effective compression technique based on compression ratio and time complexity. They compared few popular lossy data compression technique like Discrete Wavelet Transform(DWT), K-Mean and 3d Spiral JPEG.

Ms. D. Preetha Evangelina et al. [12] proposed and efficient mechanism for storing photo albums on cloud storage. They gave the idea to reduce the time complexity of photo album compression for cloud storage. They also proposed cluster

DOI: 10.18535/ijecs/v6i3.01

formation (map reduce) ,SURF(Speed up Robust Feature) extraction and prediction using Hessian matrix

Jaime Moreno et al. [13] provided computationally simple algorithm for image compression based on Hilbert Scanning of Embeddedquad Trees(Hi-SET) .It allows to represent an image as an embedded bit stream along with a fractal function. Embedding's an important feature of modern image compression algorithms, there should be that unique feature that leads to achieving the best quality for the number of bits input by the decoder during the decoding. Hi-SET possesses also this latter feature. Furthermore, the coder is based on a quad tree partition strategy, that applied to image transformation structures such as discrete cosine or wavelet transform allows to obtain an energy clustering both in frequency and space. The coding algorithm is composed of three steps, using a list of significant pixels. The implementation of the proposed coder is developed for gray-scale and colour image compression. Hi-SET compressed images are on average, 6.20dB better than the ones obtained by other compression techniques based on the Hilbert scanning.

3. System Architecture

In general, the BioAaaS based authentication scheme consists of two stages:

1)Enrolment process.

2) Verification process.

The user provides biometric information i.e. fingerprint to the biometric sensor, which converts the biometric data into a binary string. The feature extractor converts the binary string into a reduced representation set of features (eliminates the redundancy). The feature vector of a user is stored into a data base of service provider. In verification process, when a user tries to log in into the remote cloud server, same steps will be executed. The feature vector is extracted by the feature extractor and submitted to matching module. The matching module intercepts the feature vector stored against user during enrolment process. The matching module executes an algorithm to check the matching similarity between enrolment and verification feature vectors for the user trying to log in. In our scheme we use standard correlation to measure the similarity matching, which is considered to be efficient for vector processing. The Figure 3.1 shows the architecture diagram of the system.

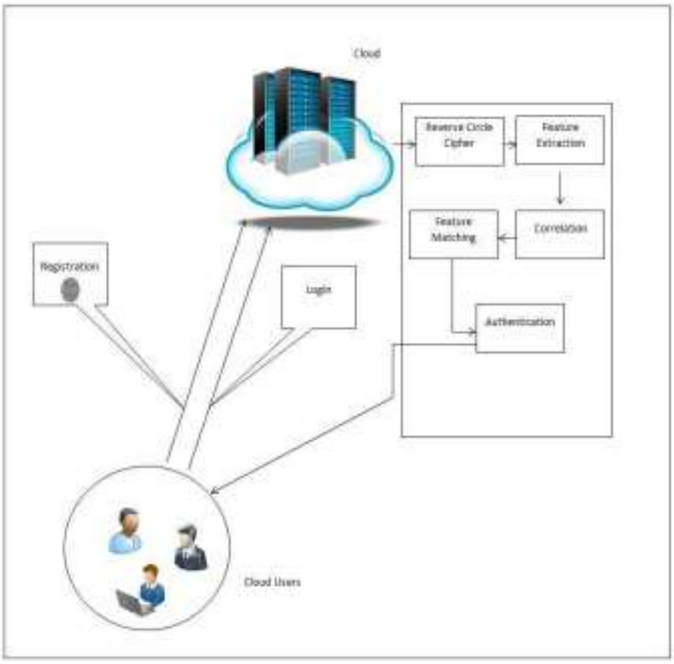

Figure 1 : System Architecture

Whenever the new user wants to access the Cloud the first thing he must do is to register by using his fingerprints. Once he is registered he becomes a valid user and can login to the cloud. The fingerprint image is then stored and encrypted using the Reverse Circle Cipher algorithm.

The feature extraction is performed on encrypted data. It takes the mean of all the blocks from Reverse Circle Cipher algorithm. This mean is compared with the mean of the data that is already stored in the database while registration. This process of matching is done using a Pearson's formula. It finds the correlation between the two images and gives the result whether he is a valid user or not. Pearson algorithm gives value ranging from -1 to 1. If the value comes closer to 1 than the two images are considered same and user is considered authenticated and allowed login to the cloud.

CONCLUSION

The existing systems have technologies that save the whole data on cloud that gives heavy load on the resources which ultimately leads to slow processing. Also the earlier techniques used for matching images fails in matching those images that have orientation change. So, we proposed a biometric authentication mechanism which allows us to provide secure login into cloud server and verifying the user even if the orientation of fingerprint is changed. All this is done by an Outsourceable two party Privacy preserving Biometric Authentication method. This reduces the threat of data theft and reduces the load on resources.

References

[1] Chandra ShekharVorugunti, "A Secure and efficient Biometric Authentication as a service for cloud computing," IEEE, October 09-11 2014.

[2] D. J. Craft "A fast hardware data compression and some algorithmic extensions," IBM J. RES. DEVELOP. VOL. 42 NO. 6 NOVEMBER 1998 .

[3] Cong Li, Zhenzhou Ji, Fei Gu "Efficient parallel Design foe BWTBased DNA Sequence Data Multi-compression Algorithm," Harbin Institute of technology,150001, Harbin, China.

[4] Kiran Kumar K, K.B Raja, "Hybrid Fingerprint Matching using Block filter and strength factor," Second International Conference on Computer Engineering and Applications,2010.

[5] Mr.Jeff Collier, "CIRRUS : Increased Image Dissemination Speed using Cloud resources," 978-1-4673-7565-8/15,2015 IEEE .

[6] Hu Chun, Feng Li "Outsourceable two party privacy preserving biometric authentication," June 4–6, 2014, Kyoto, Japan.

[7] Surender Sharma and Venki Balasubramanian"A Biometric Based Authentication and Encryption framework for sensor Health Data in Cloud ,"2014 IEEE.

[8] Krishnaraj Madhavji Sunjiv Soyjaudah, "Cloud Computing Authentication Using Cancellable Biometrics,"2013,IEEE.

[9] Dr.Anandhakumar P. and Ms. D. Preetha Evangeline, "An Effective Mechanism for Storing Photo Albums on Cloud Storage," 2015 IEEE.

[10] Abdullah A. Albahdal and Terrance E. Bould "Problems and Promises of using the Cloud and Biometrics," 11th International conference on Information Technology: New Generations,2014.

[11] Dasaradha Ramaiah K and T Venugopal "A novel approach to detect most effective compression Technique Based on Compression Ratio and time complexity with huge data Load for Cloud Migration," IEEE 2016.

[12] Ms D Preetha, Cephas Paul Edward V and Dr. Anandh Kumar P "An Efficient Mechanism for storing Photo Album on Cloud Storage," IEEE 2015.

[13] Jaime Moreno and Xavier Otazu "image Compression Algorithm Based on Hilber Scanning of Embedded Quadtrees: An Introduction of the Hi-Set Coder," IEEE 2011.