The Thumb Authentication on Cloud Computing

Samadhan Pagar,
Vaibhav Gore,
Darshan Sant,
Pooja Satpute
AISSMS IOIT- Department of Information Technology,
University of Pune

***Abstract*—— One of the major challenges that face by cloud computing concept in its global acceptance is how to secure and protect the data and processes by user. So, The security of the cloud computing environment is a new research area requiring further development.**

The proposed system improve security enhancement in cloud computing that is based on biometric security. The term biometric security implies the parameters of security enhancement methods are Face Recognition, Finger Print, Iris Scan etc. In this proposed system, thumb authentication input comprises the adaptive security enhancement on cloud computing where existing cloud is updated with thumb authentication security. Hence, the proposed system is novel. In this system, we are implementing thumb registration, thumb authentication, cloud uploads, cloud downloads by using minutiae algorithm. The performance of the updated processing blocks is presented in the evaluation part of this paper. Minutiae-based matching algorithm in fingerprint recognition systems is the approach to fingerprint identification and verification. The performance mostly depends on the accuracy of the minutiae extraction procedure. Minutiae matching designate the time complexity of applied solution. The algorithm is evaluated towards thumb scanning, matching processing for fingerprint recognition and authentication on MySql databases. This system is useful in various banking sectors, business organizations and for individual purpose also.

***Index Terms*—**
Minutiae matching ,cloud computing, Authentication, minutiae extraction.

1. INTRODUCTION

The biggest impact the cloud has had on the way we live is unquestionably how were now living in a world where we can access anything we want from almost anywhere we want. So as long as we have a device in hand, whether were at home or on a long journey, the information we need, both personal and professional, is never any further than a few clicks away. Cloud computing refers to the use of computing resources, those being hardware and/or software) that reside on a remote machine and are delivered to the end user as a service over a network, with the most prevalent example being the internet. By definition, a user entrusts his data to a remote service, on which has limited to no influence.

When it first appeared as a term and a concept, a lot of critics dismissed it as being the latest tech fad. However, cloud computing managed to cut through the hype and truly shift the paradigm of how IT is done nowadays. The Cloud has achieved cutting costs for enterprises and helping users focus on their core business instead of being obstructed by IT issues. For this reason, it seems that it is here to stay for the immediate future. Lately cloud computing has been garnering notoriety as more and more businesses take advantage of its various benefits. According to Webopedia, cloud computing is a type of computing that relies on sharing computing resources rather than using local servers or personal devices to handle applications. Cloud computing allows a business to outsource many applications historically maintained on the company's own hardware.

There are three cloud computing models: public, hybrid and private. A public cloud is made available to the general public or a large industry group and is owned by an organization selling cloud services. A private cloud operates solely for an organization, managed by the organization or a third party and may exist on premises or off premises. A hybrid cloud is made up of two or more clouds (at least one public and one private) that remain unique entities but are bound together by technology that enables data and application portability (adapted from National Institute of Standards). Within the past year DBL has moved arguably its most important software application our time keeping system to the cloud. This serves as a perfect case study on some of the benefits, and drawbacks, of cloud computing.

2. RELATED WORK

[1] Mutual Protection in a Cloud Computing Environment, by Aiiad Albeshri and William Caelli, at-Info. Security Inst Queensland University of Technology Brisbane, Australia. Cloud computing is essentially composed of a large-scale distributed and virtual machine computing infrastructure. This new paradigm delivers a large pool of virtual and dynamically scalable resources including computational power, storage, hardware platforms and applications to users via Internet technologies. Private and public organizations alike can make use of such cloud systems and services while many advantages may be derived when migrating all or some information services to the cloud computing environment. Examples of these benefits include

increases in exibility and budgetary savings through minimization of hardware and software investments.

[2] How to Manage Information Security in Cloud Computing, by Che Hung Liu Department of Business Management, National University of Tainan at-Tainan, Taiwan Many previous studies have recognized that information security is critical issue in the age of Internet, not only because information is valuable and important, but also because information sustains an enterprises competitive advantage,

However, with Internet entering the Cloud Computing generation, the role of information security becomes extreme important. Since cloud computing technology delivers applications and hardware in the form of services over the Internet, the risk is self-evidently higher than before. In past three decades, the world of computation has changed from centralized (client-server not web-based) to distributed systems
and now, we are returning to the virtual centralization - Cloud Computing Organizations use cloud computing as a service infrastructure, critically examining the security and condentiality issues for their business critical insensitive applications.

GOALS:

- Our main aim towards cloud computing is that to make cloud computing more secure.
- To removes security related issues.
- Also Adaptive Fingerprint Image Enhancement with Emphasis on Pre-processing of data in cloud computing.
- Implementing cloud computing on any portable devices like mobile, PC, laptop, notebook PC etc.
  To make cloud computing user friendly and with unique security is provided to it.

OBJECTIVES:

- To make cloud computing more secure
- Improve cloud efficiency
- To provide biometric security for cloud computing
- To make cloud computing location independent

3. IMPLEMENTATION

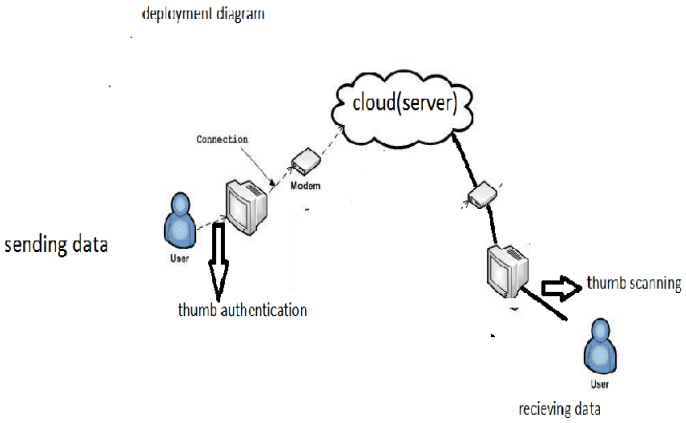


Fig. Proposed system architecture

This architecture proposes a cloud (server) in which whole data is uploaded by the user along with the image of the thumb as a security and the same user can download the data with the same thumb image to any other pc or notebook.

In the proposed system first user makes thumb registration facilitated under admin of system. Once the user has registered thumb on system it will get thumb log in id successfully. Then he can use its thumb scan and get id for getting login on the system.

Now at the client side user can make thumb scan at that time if user is valid user it will generate the particular user's registered id automatically and then user will be login. But user is not valid it will generate 0 id for unregistered user and it will not further proceed. When thumb Authentication is done successfully then user has to make registration on cloud server, user will enter details for getting register on cloud and get user id and password. Also facilitate to have unique id which will be useful foe next download from cloud. After successful registration on cloud now user can do log in for cloud.

Now user has two choices for uploading and downloading data on cloud. Using upload option user can upload any type of data on cloud server. Also for download user has to enter unique key generated at registration time, by entering proper key user can download data from the cloud server.

Fig. multiple access to cloud

4. ALGORITHM STRATEGY

➢ MINUTIAE ALGORITHM:

- The minutiae algorithm is an important algorithm in finger print recognition systems.
- Minutia matching includes fingerprint identification and verification.
- Fingerprint matching consist of two procedures: minutia extraction and minutia matching.
- The performance mostly depends on the accuracy of the minutia extraction procedure. The two most prominent used features are ridge ending and ridge bifurcation.
- Minutiae matching consist of finding the best alignment between the template (set of minutiae in the database) and a subset of minutiae in the input fingerprint, through a geometric transformation

- MINUTIAE EXTRACTION Typically each detected minutiae mi is described by four parameters: mi = (xi , yi ,q i , ti) where: xi , yi { are coordinates of the minutiae point, qi{ is minutiae direction typically obtained from local ridge orientation, ti { is type of the minutiae point (ridge ending or ridge bifurcation), The position of the minutiae point is at the tip of the ridge or the valley and the direction is computed to the X axis.
- RIDGE THINNING METHOD The most commonly used method of minutiae extraction is the Crossing Number (CN) concept [2, 3, 4].
- The binary ridge image needs further processing, before the minutiae features can be extracted. The _rst step is to binaries and further to thin the ridges, so that they are single pixel wide

- A large number of skeletonization methods are available in the literature, due to important role in many recognition systems.

Fig. Fingerprint image 1) binarization 2) skeletonization

- The minutiae points are determined by scanning the local neighbourhood of each pixel in the ridge thinned image, using a 3*3 window

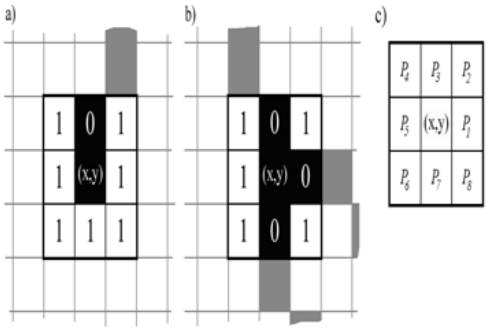
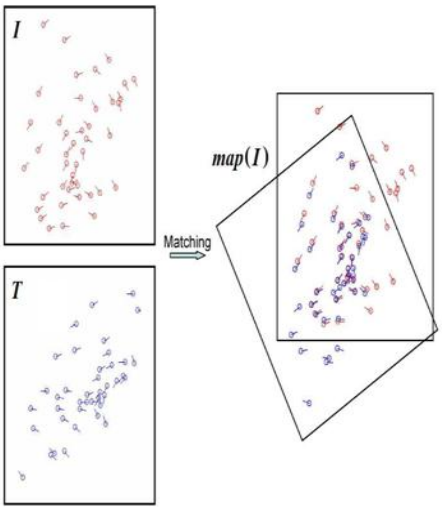


Fig. a) Ridge ending b) bifurcation c) 3*3 window.

- Matching algorithm ,it compares two minutiae sets: template T = m1,m2 ,...,mj from reference fingerprint and input 1 2 , ,..., i I = m m m from the query and returns similarity score S (T, I) .
- The minutiae pair i m and j m are considered to be match only if difference in their position and directions are lower then tolerance distances.



➢ DES ALGORITHM

- DES is a block cipher it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of the same size.
- Thus DES results in permutation among the 2 to the 64th power possible arrangements of 64 bits, each of which may be either 0 or 1.Each block of 64 bits is divided into two blocks of 32 bits each, a left half block L and right half R.
- DES operates on the 64-bit blocks using key sizes of 56- bits.
- The keys are actually stored as being 64 bits long, but every 8th bit in the key is not used. However, we will nevertheless number the bits from 1 to 64, going left to right, in the following calculations. But, as you will see, the eight bits just mentioned get eliminated when we create subkeys.

- The DES algorithm uses the following steps:
  Step 1: Create 16 subkeys, each of which is 48-bits long.
  Step 2: Encode each 64-bit block of data.

5. CONCLUSIONS

The cloud computing is today's need in this computer age. Security is an important issue in cloud computing so we are implementing cloud security using biometric security like thumb authentication. A multi-user authentication scheme based on cellular automata in cloud computing environment was proposed. In the cloud environment, an authentication scheme should be the lightweight and robust from security attacks. The proposed scheme was based on CA that is suitable for these properties. Moreover, the proposed scheme is a secure because of biometric mechanism based security. Therefore, the randomness quality of the proposed scheme is high. In other words, the proposed scheme is secure.

6. FUTURE WORK:

As we know that cloud is very useful and large amount of storage of data, now a days cloud use is increasing day by day so to make cloud more secure we can use other biometric security along with the thumb authentication to cloud. Also we can provides data backup and data recovery in cloud so that in case of data corruption that can be easily overcome.

REFERENCES

[1] OwenO Malley, Integrating Kerberos into Apache Hadoop, Kerberos Con-ference 2010, 26-27 October 2010 MIT, USA.

[2] P. P. Chaudhuri, D. R. Chowdhury, S. Nandi and S. Chattopadhyay, Additive Cellular Automata Theory and Applications Vol. 1, IEEE Computer Society Press.

[3] Yanjiang Yang, Feng Bao, Enabling Use of Single Password Over Multiple Servers in Two-Server Model 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).

[4] Adaptive Fingerprint Image Enhancement With Emphasis on Preprocessing of Data,by-Josef Strom Bartunek, Mikael Nilsson, Benny Sberg, Ingvar Claesson, year 2013

[5] Deyan Chen and Hong Zhao Data security and privacy protection issues in cloud computing. International conference on Computer Science and Electronics Engineering 2012.

[6] K. Valli Madhavi , R. Bala Dinakar and R. Tamil kodi Data storage security in cloud computing for ensuring eective and exible distributed system. National conference on research trends in Computer Science and Technology 2012.

[7] Mandeep Kaur and Manish Mahajan Using encryption algorithm to enhance data security in cloud computing International journal of Communication and Computer Technology 2013.

[8] Bhavna Makhija and Indrajeet Rajput Enhanced data security in cloud computing and TPA International journal of Advanced Research in Computer Science and Software Engineering. 2013.