Biometric Approach for Confidentiality in Cloud Computing

Pankaj Mishra[*1] and Dev Ratna Singh[2]

1*. Assistant Professor, Deptt. of Computer Science and Engg., School of Management Sciences Lucknow, (U.P.) India. e-mail : pankaj.mishra.250@gmail.com
2. Wipro Technologies, Pune, India; e-mail : devratna20@gmail.com

Publication Info

Article history :
Received : 10th May, 2018
Accepted : 23rd May, 2018
DOI : 10.18090/samriddhi.v.10i01.8

Keywords :
Biometric, biometric safety system, biometrics concerns, fingerprint reader.

***Corresponding author :**
Pankaj Mishra
e-mail : pankaj.mishra.250@gmail.com

Abstract

Nowadays, progress in technology have made life simple by giving us higher levels of knowledge through the innovation of various devices. However, all technical invention harbours the potential of invisible threats to its users. One leading danger is theft of private information and data. As digital database get more prevailing, user's attempt to prevent their data with extremely encrypted Identity cards and passwords. However, the abuse and theft of these security measures are on the rise. Taking benefit of security fault in Identity cards result in the cards gets duplicated and get misused. This increasing conflict of the cyber safety has lead to the start of biometric security method. Defining the main variation between the methods of biometric system used to verify user identity will focus on the benefits and limitations of personal data security systems.

1. INTRODUCTION

A brief aspect of biometric safety and biometrics method will give a higher understanding of the idea of network security. Biometrics is nothing but the specific (private) logical/physical characteristics of the human body. [8] These characteristics are used to identify every human. Some information of human body which varies from one individual to other will be utilised as unique biometric information to provide person"s unique identification (ID), likewise:, fingerprint, Deoxyribo Nucleic Acid (DNA), palm print and, retinal, iris. Biometric security systems will combine and save this database in sequence to use, it for authenticating individuals identity. Biometric safety system is combination of biometric database systems and biometric identification technologies. The biometric safety system is nothing but the capturing and locking of mechanism to limit access to particular data.

To enter the biometric safety system, a person need to provide a specific characteristics which will be well-matched to a database in the system. If this information matches, the locking scheme will provide access to the database for the user. The capture and lock system will start and record information of persons who accessed the data. The relation between the biometric and biometric safety system is also called as the key and lock scheme. So, in this scheme lock is biometrics security system and key is biometrics to open that lock. [5]

In the biometric security system there are seven different criteria : permanence, uniqueness collect-ability, performance, circumvention universality and acceptability. [9] As given above, uniqueness is nothing but the priority and one necessity of biometric data. It will show that how uniquely and differently the biometric system will be capable of recognizing each person in between the groups of persons. For example, The Deoxyribo Nucleic

Acid (DNA) of every person is unique and it is not possible to duplicate. Universality is another important criteria for biometric security. This indicates necessary requirements for unique characteristics of all people in the world that cannot be duplicated. For example, The iris and retinal are the characteristics that will satisfy universality requirement. The next factor is permanence which is needed for every individual characteristic that is saved in the database of the system and must be consistent for a specific period of time. The collect-ability parameter follows the permanence. The collect-ability requires the combination of each characteristic by the system in the pattern to verify persons identification. The next factor is performance for system which shows how well the biometric security system works. For the biometric security system the robustness and accuracy are chief factors and these two factors will determine the performance of biometric safety system. The next parameter acceptability will going to select fields in which biometric application are acceptable. The circumvention parameter will conclude how simply every characteristic provided by the individual person can lead towards the failure at the time of the verification process. The Deoxyribo Nucleic Acid (DNA) is considered to be the most hard characteristic that leads to the failure at the time of verification process. [3]

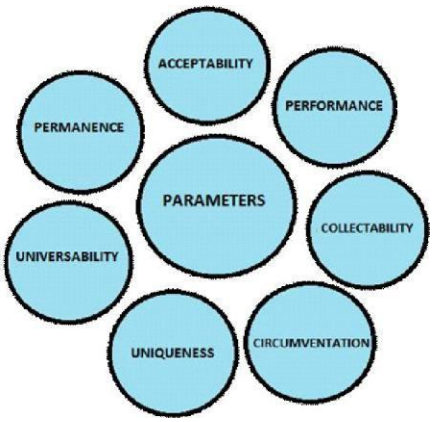

Fig.1: Basic Norm for the Biometrics Security System

2. RELATED WORK

Following part of paper represents detailed representation of the earliest work in this system.

2.1 Applications for Biometrics Technology

Physical resources contain its physical feature. Logical tool is a technique used in system. Physical Access Control is controlled by logical tool. Physical resources provide authentication which need persons to supply physical feature. It is for security purpose in various sectors such as: Hospitals, Police station, and the Forces. The most ordinary use for the physical resources is to access devices which are used in computers. This relevance is secrete and important and is responsible for high level of security. The physical resources cut down the risk of human problems. It recovers the data loss in the system. [1] The system helps to get rid of the process of identify long and difficult password with different processes. Physicalresources not only produce desired results but are also safe, secure and profitable in the organisation. Logical tools contain a process to control information. These consist of secrete information of different users. Logical tools are used by military and government organisations to protect their vital data with high security systems using biometric encryption technology. The logical tools are used for accessing the control of system and computer networks. It reduces the burden of long and complicated password requirements for users. It is more protected and produce the result for private information in the system. It also saves money and time. [1]

2.2 Biometrics Solution

2.2.1. Facial Psychological Feature Device

The human face is one of the simplest ways which is utilised in biometric system to recognise a user. Face detection technique is well known and is used more widely because it doesn‟t require physical relation between the users and device.

S-JPSET : Vol. 10, Issue 1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

Photographic camera scan the users face and match it to the present database for right result. It is very easy to install and doesn‟t ask for any hardware. Facial identification technology is utilised widely in a various of security systems. It is still not as specific because one person in one position and device in another. So, we use different parts as such as retina, iris or DNA. Hence, it is usually used with other features in the system. Time contain negative impact for face recognition because as the user „s age will change over time.[2]

Biometric face identification systems will assemble information from the persons face and save them in the database for future. It will measure the total structure, form of user‟s face such as: spacing between eyes, nose, mouths, ears, size of eyes, mouth and others contents. Facial looks are also measurable during a user‟s facial recognition process. Such as smiling, crying, and lines on the face.[2]

2.2.2. Fingerprint Reader

Our fingerprint is made of a number of elevation and ravine on the surface of finger that are specific to each human. Elevation are the upper skin layer portion of the finger and ravine are the lower part. The elevation form two detail points: elevation endings where the elevation end, and elevation forked where the elevation separated into two parts. The individuality of a fingerprint can be observed by the different form of elevation and lines and the details points. There are five basic form which make up the fingerprint: the curve such as tented and plain curve covers 5% of fingerprint; left and right disk covers 60% of fingerprints; whorl covers 34% of fingerprints and inadvertent scroll covers 1% of fingerprints.

To get the surface of the fingermarks for confirmation during the identification of users, new technologies are designed with tools such as: visual and ultrasound. There are chief algorithms which are used to recognise fingerprints: detailed matching and structure matching. Detailed matching will compare the details of the extract detailed to identify the difference between one users fingerprint to others. When users catalogue with the system, they will record images of finer points direction and location on the finger surface. When person‟s use fingerprint detection system to confirm their identification, a detailed location image is brought and compared with the one which provided at the time. [2]

Structure matching will analyze all the surfaces of the finger‟s rather of one particular point. It will concentrate more in broadness, curvature and compactness of finger‟s plane. The image of the fingers plane for this method will contain the area around a finer points region with low status radius or region with different combinations of elevation. [2]

2.2.3 Voice Recognition

There are mainly two component which makes a person‟s voice unique. Firstly, it is a biology component which is well known as voice tract. Secondly, it is a behavioural component which is called as the voice accent. By the combination of these factors, it is nearly impossible to re-create some other person‟s voice exactly. Taking benefit of these characteristics, biometrics technology generated voice identification systems in order to confirm each person‟s identification using only users voice. Mainly, voice recognition will concentrate on the vocal tract because it is a unique characteristic of a biology trait. Biometric technology works perfectly in the physical access power for users. [1]

Voice identification systems are effortless to set up and it requires a minimal quantity of equipment. This equipment includes microphones, telephone and PC microphones. However, there are some silent factors which can have bad impact on the quality of the system. Firstly, presentation of the users when they record their sound/voice to

database is most important. For that reason, users are asked to restate a short pass phrase or a sequence of numbers and sentences so that the system can examine the user‟s voice more accurately. On the other side, unauthorised users can record authorised user‟s voices and tally it through the verification activity in order to get user access control to system. To control the hazards of unauthorised access via recording devices, the voice identification systems will ask users to restate random state which are provided by the system during verification state. [1]

2.2.4 Iris Scanner And Recognition

The human iris is a thin rounded structure in the eyes which is answerable for controlling the diameter and size of pupils. It also controls the amount of light which is granted through the retinal in such order to protect the eye‟s tissue layer. Iris colouring is also a changeable according to different person, each iris depending upon their genes. Iris colour is decided by eye colour for each individual. There are various colours for iris like wise: brown (most popular and common colour) green, blue, grey, hazel (the unit of brown, green and gold), violet, pink (in truly rare cases). The iris also has its own patterns from person to person and eye to eye , this will make up to singularity for each single. [1]

The iris identification systems will examine the iris in various ways. It will analyse over 200 points of the iris considering: rings, furrows, freckles, the corona and the others characteristics. Later on recording the database from each individual one, it will save the information in a database for future day use, in comparing it each time the person wish to access the system. [1] Iris identification safety systems are considered as one of the most faithful safety system nowadays. The system is quit simple and unique to identify the user. Even with the system needs installation equipment and expensive charge; it is still the effortless and quickest technique to determine a user. There should be no physical relation in between user and the system whiles the verification procedure. During the verification procedure, if the users are carrying accessories likewise: contact lenses and glasses, system will work as natural because it does not change any characteristics of the person‟s iris. In theory, even if users have eye surgery, it will have no side effect on the iris characteristics of that single. [1]

2.2.5 Veins Recognition

One of the modern biometric technologies invented is the vein recognition system. Nerves are blood vessels that transfer blood to the heart. Each person‟s nerves have specific physical and behavioural traits. Taking benefit of this, biometrics uses special characteristics of the nerves as a method to identify the person‟s. Vein recognition method is mainly concentrate on the nerves in the users hands. Each finger on human hand has nerves which link directly with the heart and it has its personal physical traits. [2] Pair down to the other biometric methods, the user‟s nerves are situated inside the human body. Therefore, the identification method will acquiring images of the nerves structure at inner side of user‟s fingers by applying light transmitting to each finger. For much information, the method works by passing close to infra-red light through fingers, this way a photographic camera can record nerves patterns. [2]

Vein identification methods are acquiring more attention from experts because it has many other utilities, which other biometrics technologies don‟t have. It has a high level of safety which can secure data and accessing power is more improved. The level of accuracy utilised in nerves identification systems is very amazing and reliable by the examination of the recorded data to that of the present database. Furthermore, it too have a low prize upon instalment and equipment. Period which is taken to identify every single is smaller than other techniques (ratio is 1/2 per second).[2]

S-JPSET : Vol. 10, Issue 1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

3. METHODOLOGY

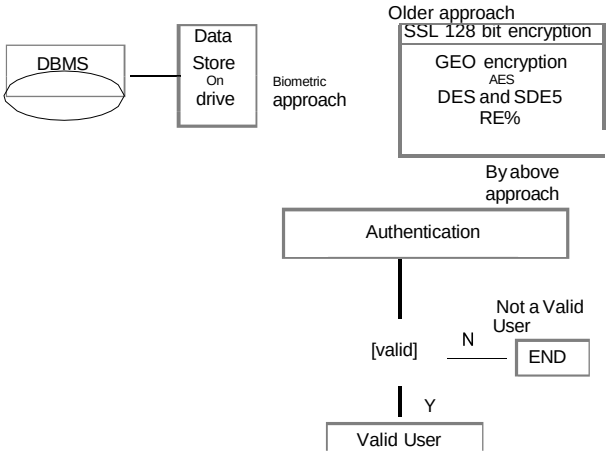

Fig.2: Authentication Process in Cloud

In this architecture we use biometric approach. The system certifies a user using some encryption techniques like AES,DES etc. If user is authorised then apply the biometric approach and store that data on the drive and then store in the database. If user is not valid then end the process. This process is done in cloud for database security and protect data form attacker.

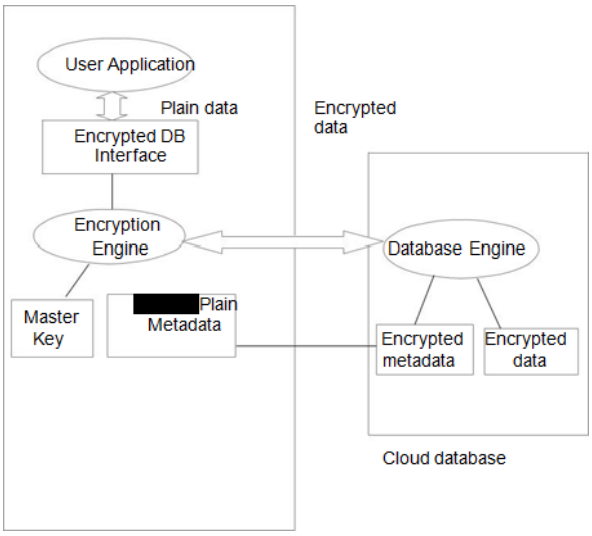

Fig.3: Authentication process in cloud

In this architecture there is connection between client cloud database. User request for the service to the cloud server. User enters the plain data through encrypted database interface it goes to the Encryption Engine. This engine consists of master key and cached plain meta data. Cloud database consist of database engine which has two parts encrypted meta data and encrypted data. When client request for the service that time encryption engine and database engine interact with each other.

4. FUTURE SCOPE

Nowadays, biometrics methodology is well known thought of the top-quality security methods of user information, database etc. Normally, biometrics method will collect and measure database of human biology and actions. There are various structure to collect and measure database of users likewise: scanning the particular characteristics of the person/user (tissue layer, facial-expression, finger-print) and examine the particular action of user likewise: signature.

The primary intention of biometric system is to determine and confirm a user‟s identification. Biometrics technology is easier than other security technologies of identification validation. For example, Identity card (student identity card in collage) is one of the examples to certify a person‟s identity. If you don‟t remember users identity card at home, then user will not be capable to entree the collage building. In such situation, biometrics device will be more dynamic and useful due to chances that you remembering your eyes or fingers at home are not possibly convincing .With biometrics safety system, we just need to authenticate our identification by using the unique characteristics, which we are carrying always with us reducing the possibility of misplace Identity cards and another identifying accessories. Likewise, identity cards can be duplicated, it increase the hazard of unapproved users achieve access to import database. With user‟s

own specific characteristics and action‟s, it will be difficult to make copies.

Biometrics security system has larger applications in lives and in current years. Scientists have developed higher stages of recognising a user‟s identity. Our main application is fingerprint identification technology. With this technology, we are able to identify any user in the overflow groups so that, we are able verify the person‟s identification. We are also able to use this method of biometrics technology to find past recognised criminals and terrorists in our society. This will help us to cut down the criminal actions in the world. Biometrics technology is applied in a different of ways and different fields of practice. it is use in healthcare facility to insure the identification of patients and to defend their secrecy. Biometrics technology has been utilised at airports to insure the identification of people. By using this technology, it helps keep record of people going away and out of country. It also helps in determing vicious people and terrorists.

5. CONCLUSION

Biometrics technology is a fresh technology for most of us because it has only been implemented in public for short time period. There are many another utilities and result of biometrics technology utilised in security systems. It has much benefit which can modify our lives like wise: better security and effectiveness, decreased fraud and password administrator costs, simplicity of use and makes live more homely.

Even though the biometrics security system still has many related concerns likewise, information isolation, physical privacy and religious protest. Users can‟t neglect the reality that this new technology will change our lives.

REFERENCES

[1] Lifeng Lai, Sui Wai Ho and H. Vicent Poor “Privacy Security Trade-Offs in Biometric Security Systems - Part 2:Multi Use Case” [Lai. 2011] EEE Transactions on Information Forensic and Security, Vol 6, No.1, March 2011

[2] Paul Reid, “Biometrics for network security”, Pearson Education Inc [Reid, 2011], ISBN 0131015494.

[3] Sandra Maestre, Sean Nichols “DNA Biometrics”, 2009

[4] Massimo Tistarelli and Marks Nixon, “Advances In Biometrics”,[Tistarelli, 2009] Springer-Verlag Berlin Heidelberg 2009.

[5] Jain, A.K.; Ross, A.; Pankanti, S., “Biometrics: a tool for information security”[Jain, 2006] Volume: 1 Issue: 2,Issue Date:June 2006, page(s): 125 – 143.

[6] Khalid Saeed-Jerzy Pejas-Romuald Mosdorf, “Biometrics, Computer Security, Systems and Artificial Intelligent Applications”,[Mosdorf, 2006],S pringer-Verlag Berlin Heidelberg 2006, ISBN 0387362320.

[7] Nalluri, S. K., & Parasaram, V. K. B. (2015). Automating Software Builds with Jenkins: Design Patterns and Failure Handling. International Journal of Technology, Management and Humanities, 1(01), 16-33. https://doi.org/10.21590/ijtmh.01.02.03

[8] Nalluri, S. K., & Parasaram, V. K. B. (2015). Automating Software Builds with Jenkins: Design Patterns and Failure Handling. International *Journal of Technology, Management and Humanities,* 1(02), 16-33.

[9] Lorrie Faith Cranor, Simson Garfinkel, “Security and usability: designing secure systems that people can use” [Cransor, 2005], O‟Reilly Media, Inc., 2005, ISBN 0596008279.

[10] Jain, A.K.;Ross, A.;Prabhakar, S.;”An introduction to biometric recognition” [Jain, 2004],Volume: 14 Issue: 1 Issue Date:Jan. 2004, on page(s): 4 – 20.

[11] Michael E. Schuckers, “Some Statistical Aspects of Biometric Identification Device Performance”, 2001

[12] John D. Woodward (Jr.), United States. Army, Arroyo Center “What concerns do biometrics raise and how do they differ from concerns about other identification methods?”,[Woodward, 2001],Army biometric applications:identifying and addressing sociocultural concerns, 2001.

[13] New Mexico, Department of Health “Fingerprint Techniques Manual what.pmd”http://dhi.health. state. nm. us/elibrary/ cchspmanual/fingerpr int_manual.pdf

