IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Biometric Approach for Confidentiality in Cloud Computing

Shakir Ali[1] Pankaj Mishra[2]

Abstract: Cloud computing has revolutionized the way data and services are managed, shared, and accessed over the internet. However, with the increasing adoption of cloud services, concerns related to data confidentiality and security have become more pronounced. Traditional authentication mechanisms, such as passwords and tokens, have proven vulnerable to various attacks, leading to unauthorized access and data breaches. Currently, progress in technology has 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 databases 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 cyber safety has LED to the start of biometric security methods. 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.

Keywords— Biometric authentications, Biometric safety system, Biometrics concerns, Fingerprint reader.

I. 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 as that 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. The biometric safety system is a combination of biometric database systems and biometric identification technologies. The biometric safety system is nothing but the capture and lock mechanism to limit access to data. To entree the biometric safety system, a person wills essential need to provide their 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 people who accessed the data. The relation between the biometric and biometric safety system is also called the key and lock scheme. So, in this scheme lock is biometrics security system and key are biometrics to open that lock [5]. In the biometric security system seven different criteria are there and they are 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 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 criterion 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 universal requirements. 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 collectability requires the combination of each characteristic by the system in the pattern to verify persons identification. The next factor is performance for the system which shows how well the biometric security system works. For the biometric security system, robustness and accuracy are chief factors and these two factors will determine the performance of biometric safety system. The next parameter acceptability will be going to select fields in which biometric applications are acceptable. The circumvention parameter will conclude how simply every characteristic provided by the individual person can lead towards failure at the time of the verification process. The Deoxyribo Nucleic Acid (DNA) is the hardest characteristic that leads to the failure at the time of verification process [3]. In recent years, cloud computing has emerged as a dominant paradigm for delivering computing resources and services over the internet. It offers numerous advantages, such as scalability, cost-efficiency, and flexibility, making it an attractive choice for individuals and organizations to store and access their data and applications. However, along with the benefits, cloud computing also poses significant challenges related to data confidentiality and security. Traditional methods of authentication, such as passwords and tokens, have proven to be susceptible to various security breaches and attacks. As a result, ensuring robust confidentiality in cloud computing environments has become a critical concern. To address this issue, the biometric approach has emerged as a promising and innovative solution. Biometric authentication leverages unique physiological and behavioral traits of individuals, such as fingerprints, facial features, iris patterns, voice, and behavioral biometrics, to verify their identity. Unlike traditional authentication methods, biometrics offer a more secure and reliable way to confirm a user's identity, as these characteristics are inherently difficult to forge or duplicate. This research paper focuses on the application of the biometric approach for confidentiality in cloud computing. We explore the potential benefits of integrating biometric authentication into cloud-based systems to enhance data security and privacy. By utilizing biometric data, cloud service providers can ensure that only authorized users gain access to sensitive information and resources, significantly reducing the risk of unauthorized access and data breaches. Moreover, the paper delves into the technical aspects of implementing biometric authentication in the cloud, including the various biometric modalities, algorithms, and encryption techniques used to protect biometric data during transmission and storage. It also discusses the challenges and opportunities associated with deploying biometrics in cloud environments, such as scalability, interoperability, and compliance with privacy regulations. Furthermore, the research investigates the advancements in machine learning and artificial intelligence techniques that have improved biometric recognition systems' accuracy and robustness. These technologies play a vital role in detecting and preventing fraudulent attempts, such as spoofing or replay attacks, thereby strengthening the overall security posture of cloud-based applications. The paper also addresses concerns related to user privacy and ethical considerations associated with collecting and storing biometric data in the cloud. Balancing the need for enhanced security with the protection of user privacy is crucial to gain user acceptance and trust in biometric authentication systems.

Basic Norm for the Biometric Security System of the Parameter:

- Collectivity
- Circumvention
- Uniqueness
- Universability
- Permanence
- Acceptability
- Performance

II. RELATED WORK

The following part of the paper represents a detailed representation of the earliest work in this system.

I. Applications for Biometrics Technology

Physical resources contain their physical features. logical tool is techniques are used in system. Physical access control is controlled by logical tools. Physical resources provide authentication which needs people to supply physical features. It is for security purposes in various sectors such as: hospitals, police station, and the forces. The most ordinary use for physical resources is to access devices which are used in computers. This relevance is secreted and important and is responsible for a high level of security. 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 identifying long and difficult passwords with different processes. Physical resources are not producing the desired result but also safe, secure, and profitable in the organization. Logical tools contain a process to control information. These consist of secrete information from different users. Logical tools are used by the military and governments to protect their vital data with high security systems using biometric encryption technology. 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 produces the result for private information in the system. it also saves money and time [1].

II. Biometrics Solution

a) Facial Psychological feature Device

The human face is one of the simplest ways which is utilised in biometric system to recognize 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. Photographic cameras scan the user face and match it to the present database for the right result. It is very easy to install and doesn't ask for any hardware. Facial identification technology is utilised widely in various security systems. It is still not as specific because one person in one position and device is in another, so we use different parts such as retina, iris, or DNA. Hence, it is usually used with other features in the system. time contains 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 person's face and save it in the database for the coming future days. It will measure the total structure, form of user's face such as: spacing between eyes, nose, mouths, ears, size of eyes, mouth, and other contents. Facial looks are also a measurable thing to change during a user's facial recognition process. Such as smiling, crying, and lines on the face [2].

b) Fingerprint reader:

Our fingerprint is made of a few elevations and ravine on the surface of finger that are specific to each human. Elevation is the upper skin layer portion of the finger and ravine are the lower part. The elevation forms 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 forms 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 deuce chief algorithms which are used to recognize fingerprints: detailed matching and structure matching. Detailed matching will compare the details of the extract detailed to identify the difference between one user fingerprint to others. When users catalogue with the system, they will record images of finer points direction and location on the finger surface. When a person uses 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 fingers 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].

c) Voice Recognition:

There are mainly two components which make a person's voice unique. Firstly, it is a biology component which is well known as voice tract. Secondly, it is a behavioral component which is called 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 to confirm each person's identification using only the 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 a 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 users' voice more accurately. On the other side, unauthorized users can record authorized users' voices and tally it through the verification activity in order to get user access control to system. To control the hazard of unauthorized access via recording devices, the voice identification systems will ask users to restate random states which are provided by the system during verification state [1].

d) Iris Scanner and Recognition:

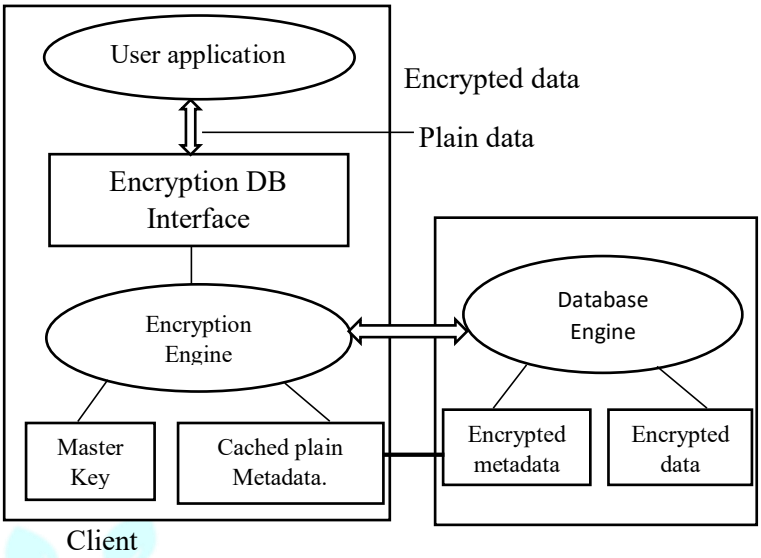
The human iris is a thin rounded structure in the eyes which is answerable for controlling the diameter and size of pupils. It also controls the amount of light which is granted through the retinal in order to protect the eye's tissue layer. Iris coloring is also changeable according to different person, each iris depending upon their genes. Iris colours will be decide by eye colour for each individual. There are various colours for iris likewise: brown (most popular and common colour for the iris), 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 other 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 wishes to access the system [1]. Iris identification safety systems are considered as one of the most faithful safety systems nowadays. The system is quite 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 between user and the system whiles the verification procedure. During the verification procedure, if the users are carrying accessories likewise: contact lenses and glasses, the system will work as naturally 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].

e) Veins Recognition:

One of the modern biometric technologies invented is the vein recognition system. Nervous are blood vessels that transfer blood to the heart. Each person's nervousness has specific physical and behavioral traits. Taking benefit of this, biometrics uses special characteristics of the nervous as a method to identify the persons. The vein recognition method is mainly concentrated on the nervous in the users hands. Each finger on a human hand has nervousness which links directly with the heart, and it has its personal physical traits [2]. Pare down to the other biometric methods, the user's nervous are situated inside the human body. Therefore, the identification method will be acquiring images of the nervous structure at inner side of users' 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 nervous 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 access power is improved. The level of accuracy utilised in nervous identification systems is amazing and reliable by the examination of the recorded data to that of the present database. Furthermore, it too has 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]

III. METHODOLOGY

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



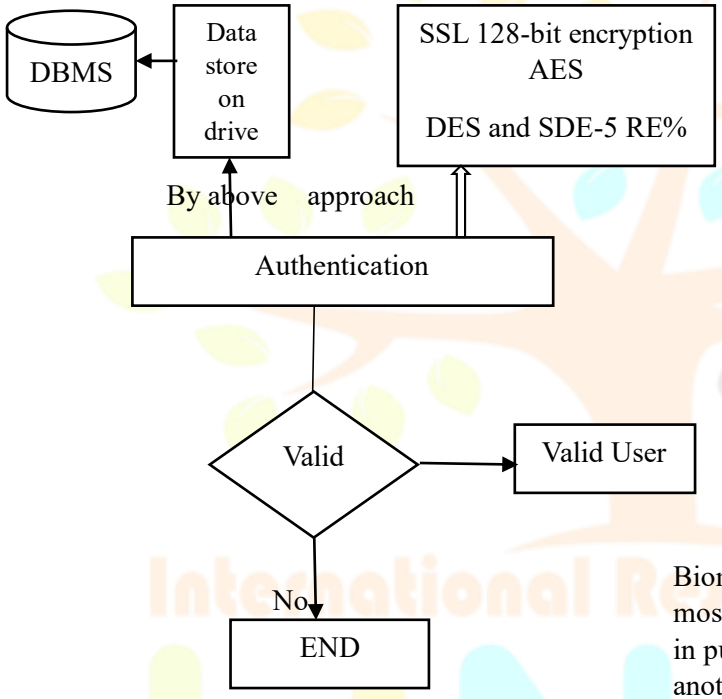


Figure-1: Authentication process of cloud

In this architecture there is a connection between client cloud databases. 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 caches plain meta data. Cloud databases consist of database engines which have 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.

IV. Conclusion

Biometrics technology is a fresh technology for most of us because it has only been implemented in public for a short time period. There are many another utilities and results of biometrics technology utilised in security systems. It has many benefits which can modify our lives, provide better security and effectiveness, decrease fraud and password administrator costs, simplicity of use and makes life 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 for the better.

V. 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], Springer-Verlag Berlin Heidelberg 2006, ISBN 0387362320.

[7] Mishra, P., & Singh, D. R. (2018). Biometric Approach for Confidentiality in Cloud Computing. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 10(01), 65-70.

[8] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001

[9] 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

[10] New Mexico, Department of Health "Fingerprint Techniques Manual what.pmd"http://dhi.health.state.nm.us/elibrary/cchspmanual/fingerpr int manual.pd

[11] Padma, P., & Srinivasan, S. (2016, August). A survey on biometric based authentication in cloud computing. In 2016 International Conference on Inventive Computation Technologies (ICICT) (Vol. 1, pp. 1-5). IEEE.

[12] Yadav, B. P., Prasad, C. S. S., Padmaja, C., Korra, S. N., & Sudarshan, E. (2020, December). A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing. In IOP Conference Series: Materials Science and Engineering (Vol. 981, No. 2, p. 022043). IOP Publishing.