ISSN 2277-3061

International Journal of Computers & Technology
Role of Biometric Security For The Enhancement of Data Security

Kapil Chauhan
Student, (AIIT) Amity University
Sector-125, Noida, Uttar Pradesh, India
Dr. Himanshu Gupta
Senior Faculty Member, AIIT
Sector-125, Noida, Uttar Pradesh, India

ABSTRACT

In today's society, data security is the big problem for every business organization or an individual. Most found threat is theft of personal data and information. With time digital data become more prevalent, personnel try to secure their information by using highly encrypted passwords and authentication identities. But, the misuse and theft of these security measures are rising in lot of theft cases. Taking advantage of security flaws in authentication identities ends up in cards being duplicated or counterfeited and hence misused. This increasing fight with cyber security has been the sole reason of making biometric security systems, the important area of concern is that how do one can implement the biometric security for increasing of data security. First unique feature which is found different in every human is Fingerprints, Humans have used fingerprints for personal identification. Presently, most of the organisation use fingerprint recognition for authentication process it is one of the oldest and most commonly used biometrics, with high accuracy & generally easy and efficient and fast. In this paper we propose the idea to use fingerprint recognition along with the user authentication password or to access the data or information. Since the only person who can access information is the person linked to it, no thief can gain access. It also makes your data, very hard for cyber criminals to hack into.

Indexing terms/Keywords

Biometric System; Face Recognition, Voice Recognition; Security of Data; Fingerprint Recognition

Academic Discipline And Sub-Disciplines

Information Technology, Data Authenticity, Data Integrity, Confidentiality, Security.

SUBJECT CLASSIFICATION

Biometric Security, Multifactor Authentication.

TYPE (METHOD/APPROACH)

Multifactor authentication requires biometric scan to gain the access to the confidential data, this authentication requires the physical presence of the user before allowing the access to the data. By designing an API (Application Program Interface) that will implement multifactor authentication to provide data integrity and data security. Due to increase in Cyber Crime, data is vulnerable and we need a strong mechanism to avoid unauthorized access to the sensitive data.

With the help of multifactor authentication this API will ensure that the data is accessible only by the authorized user. This API will also eliminate the threat of Cyber Theft.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol. 14, No. 10
www.ijctonline.com, editorijctonline@gmail.com

ISSN 2277-3061

INTRODUCTION

Biometrics is defined as the system of automated recognition of individuals based on biological or behavioural characteristics. Common forms of biometrics used for physical and logical access control includes fingerprints, facial, iris, retina, voice, hand geometry, keystrokes, and handwriting recognitions . Unique human characteristics are used to identify an individual or to verify an identity. Biometric authentication generally involves the latter—verifying or authenticating a user's claim to identity is based on a one-o-one evaluation and comparison of the used biometric credentials to the registered enrolled biometric.

BACKGROUND AND DEVELOPMENT

The term biometrics comes from the combination of the Greek words 'bios', which means life, and 'metrikos', which means measuring. Biometrics is the "automated recognition of individuals based on their biological characteristics". Biometric technology has numerous applications involving the identification of persons or verification of the identity of a person. The authentication is used for government systems, to fraud prevention, to time and attendance, to physical access control, to automobile locks/ignitions. Biometric can also be used for "logical access control", that is use for biometric user authentication as part of a computer, network, or software application logon process. Biometric technologies aim primarily at identifying a person's unique features of physiological. Examples of physiological biometrics are fingerprints, iris patterns, hand geometry, DNA and facial image, while signatures, keystroke dynamics and mouse movements belong to behavioural biometrics.

Within the larger area of information security, a key element is user identification and authentication. Confidence in the identity of the user is required before authorization (access privilege) decisions are implemented. Biometric authentication is based on physical or behavioural traits of a (human) individual and depends on the ability of the applicant to present a biometric characteristic from the same source as that which was previously registered. By comparison, its "procedural strength" is high compared to traditional methods where a password may be shared or written down because it is too hard to remember.

It can also be used as an additional factor when used with other authentication technologies (such as a PIN/password, smartcard, and/or cryptographic token) in a multifactor authentication environment. As an example, the NIST EAuthentication Guidelines identify the use of biometrics as the means of authentication to release a cryptographic secret within a hard or soft certificate that is then used within a traditional authentication protocol. Multifactor authentication is often required at higher security levels, where a higher confidence in the validity of the asserted identity is required. When biometrics are used as part of the user authentication process, the biometric data must be protected when in transit and at rest. In addition, key biometric components used in the process should be trusted. At each point, threats and counter measures are identified. It is noted that these threats vary depending on the biometric architecture used (e.g., where the storage and matching are located and where physical boundaries exist).

For biometric authentication to be performed in either a physical or logical access control system, the biometric must be provisioned into the system. This involves an enrolment process - where the biometric information is captured from the individual and securely stored for future comparison. It may also involve the production and issuance of a credential, such as a smartcard that contains the biometric data. The integrity of the enrollment process is also critical. Enrollment should include an "identity proofing" step to ensure that only known, eligible persons are enrolled. Also, the binding of the biometric data to the identity must be trust worthy.

ROLE OF FINGERPRINT AUTHENTICATION

Fingerprint biometrics is largely regarded as an accurate biometric recognition method. Today, fingerprint scanners are available at low cost and increasingly integrated in laptops and other portable ICT devices. Most fingerprint recognition systems analyze the unique pattern of ridges and valleys, and the arrangement of small unique marks on the fingerprint, which are known as minutiae. They can be recognized and distinguished by their type, by x- and y-coordinates, and by their direction. Fingerprint scanners can operate with touch-based or touchless optical systems. The former is to be found in laptops and works in a similar way to digital cameras by capturing a digital image of the fingertip using visible light. While this type of sensor provides a cheap and simple solution, it comes with some drawbacks: when a finger touches or rolls on the scanner surface, the elastic skin deforms. The quality of the captured image strongly depends on amount and direction of pressure applied by the user and the fingerprint may appear different in every cap-ture.

By emitting light on or through the finger and capturing the reflected or transmitted signals, fingerprints can be taken without contact between skin and scanner. To avoid fake-finger at-tacks, some systems employ so-called liveness detection technology, which takes advantage of the sweat activity of human bodies. High-magnification lenses and special illumination technol-ogies capture the finger's perspiration and pronounce the finger dead or alive. Application planners need to take into account that fingerprints of a small part of the population cannot be utilized for biometric recognition. This can be due to age (thin skin or senile atrophy of friction skin), accidents, genetic reasons, environmental or occupational reasons (e.g., construction workers may have worn fingerprints or a large number of cuts and bruises on their fingerprints that keep changing).

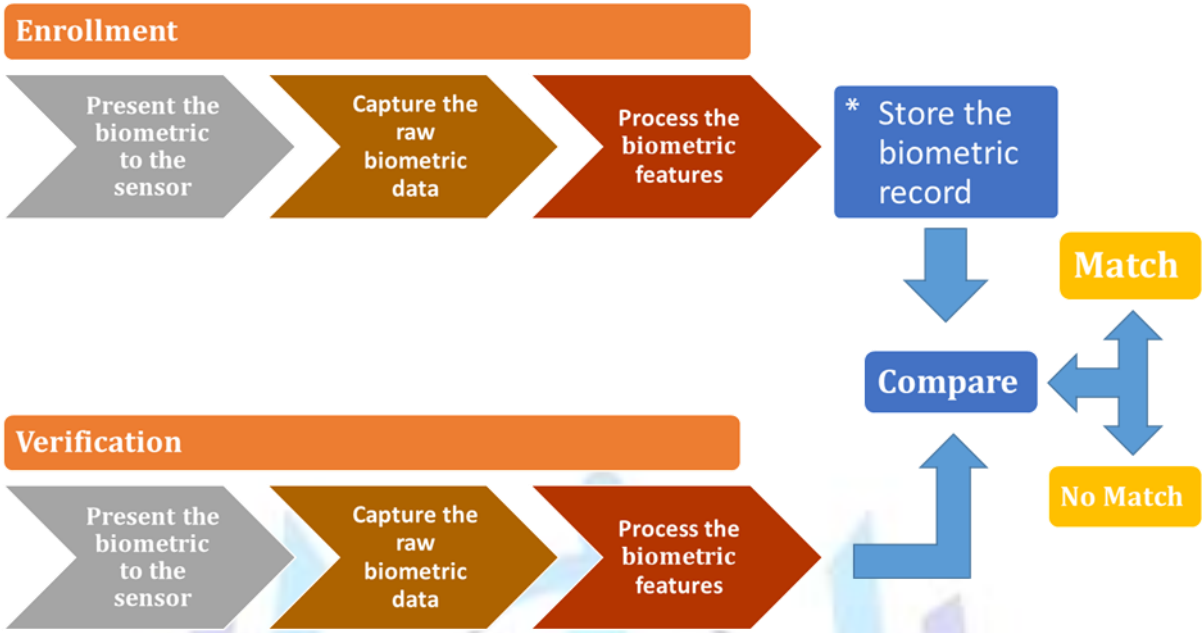

Figure 1.1: OVERVIEW OF BIOMETRIC AUTHENTICATION

Figure 1.2 BIOMETRIC AUTHENTICATION COMPONENTS

OVERVIEW OF THE PROPOSED TECHNIQUE

Multifactor authentication or two-factor authentication is the requirement of a second piece of information before allowing access to an account. By adding another authentication step when logging in, it is required that the user enter two forms of data – typically something the user knows, like a username and password, and then something the user has physical access to, like a fingerprint authentication that scan a fingerprint of the user to access and an app on a mobile phone that generates one-time codes (For those that does not have fingerprint enable device). The concerned database is required to store the user's fingerprint along with the user name and password and API that one can work with to interface with it and acquire the fingerprint images directly via the concern database. If someone system does not have the fingerprint recognition device, so users can easily add the device in the system. If someone compromises your master password, they can't gain access to your account without the second form of authentication.

Middleware and software for biometrics security system provides the link between services and instructions through the use of multiple processes, used by the biometrics system form an integral part to the efficiency and effectiveness of the whole biometrics security system. It provides system, the flexibility to bind all the applications which are located at the database/server to any biometric devices at the verification location.

The database will include biometric data, private data and application data. Capture, loss or alteration of this data is a security concern which will impact on both data integrity and confidentiality. The above proposed idea is feasible and can easily implement on the present scenario just to add an additional API (Application Programming Interface) with the authentication process.

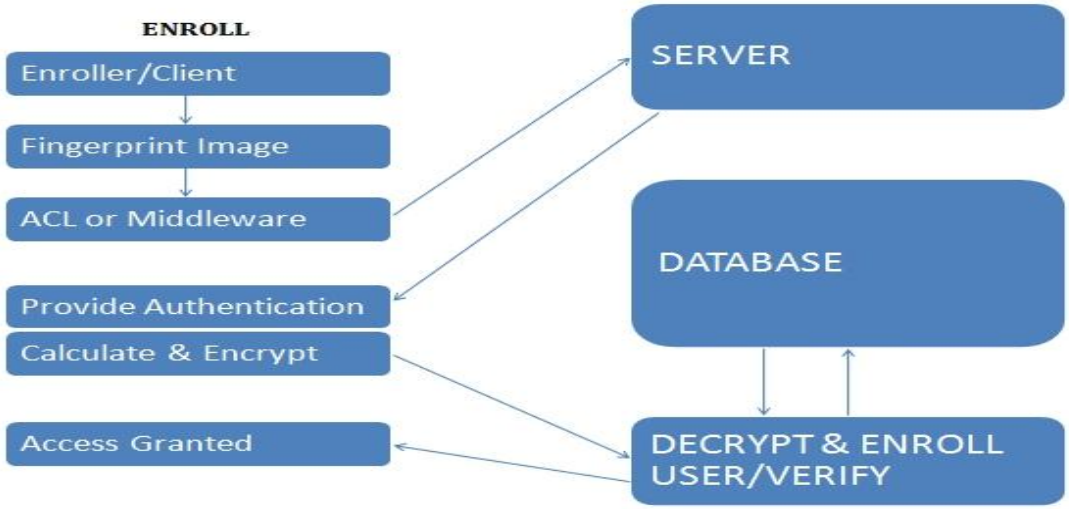

Figure 1.3: BIOMETRIC AUTHENTICATIONS

FUTURE SCOPE

Biometrics technology provides us with great number of new inventions which improves both the quality and the longevity of our lives. Nowadays, biometrics technology is considered one of the best protection methods of user information, data etc. The main purpose of biometric system is to identify and verify a person's identity. Biometrics technology is more convenient than other protection technologies of identity authentication.

While biometrics retina scan is the future and only viable measure to be used in authentication systems with fingerprints using the double check or barrier will make it extremely impossible to hack into system given an exception there is equivalently possibility of very early detection which makes future secure than ever in digital world.

Iris recognition security systems are considered as one of the most accurate security system nowadays. It is unique and easy to identify a user. Even though the system requires installation equipment and expensive fees, it is still the easiest and fastest method to identify a user. There should be no physical contact between the user and the system during the verification process. During the verification process, if the users are wearing accessories such as glasses and contact lenses, the system will work as normal because it does not change any characteristics of the user's iris. Theoretically, even if users have eye surgery, it will have no effect on the iris characteristics of that individual.

CONCLUSION

In this report, we presented a new approach for online security that allows users to secure access to their accounts. The presented approach uses fingerprints which provide a better and stronger factor of authentication. Authenticating users based on what they are instead of what they know or what fingerprint recognition have provides an interface that users can access with a more effective, convenient, and secure way to access their account and messages. There are many applications and solutions of biometrics technology used in security systems. It has many advantages which can improve our lives such as: improved security and effectiveness, reduced fraud and password administrator costs, ease of use and makes live more comfortable. Even though the biometrics security system still has many concerns such as information privacy and physical privacy, users cannot deny the fact that this new technology will change our lives for the better. While biometrics technology provides a strong user authentication solution, there are other variables to be considered in the authentication protocol. When a high level of security is needed, it is recommended that you combine other authentication factors with biometrics. When you combine what you know, what you have, and what you are, you will have achieved the highest level of security across multiple applications and systems.

ACKNOWLEDGMENTS

I am highly indebted to my guide, Mr. Himanshu Gupta for the continuous support, supervision motivation and guidance throughout the tenure of my research paper. He helped me in clarifying the concepts, requiring knowledge, perception and methods for evaluating problems.I extend my gratitude to Amity University for giving me this opportunity.

I would also like to express special thanks to my friends who have helped me on every issue and problems that I faced.

REFERENCES

[1] D.Santhadevi, "Biometric Authentication, Access-Control and Encryption For Cyber Security and Privacy".

[2] Tomko, G. (1998), “Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?” Privacy Laws & Business, 9th Privacy Commissioners/Data Protection Authorities Workshop, Spain.

[3] Potter, E. J. (2002). "Customer Authentication: The Evolution of Signature Verification in Financial Institutions."

[4] Catherine J. Tilton, " The Role of Biometrics in Enterprise Security" February 2006. Available: http://www.dell.com/downloads/global/power/ps1q06-20050132-Tilton-OE.pdf.

[5] ITU-T Technology Watch Report, "Biometrics and Standards " December 2009. Available: http://www.itu.int/dms_pub/itut/oth/23/01/T230100000D0002PDFE.pdf

[6] QuestBiometrics, "Biometrics Access Control", 2005. Available: http://www.questbiometrics.com/biometric-access-control.html

[7] Chien Le, "A Survey of Biometrics Security Systems" November 28, 2011. Available: http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet.pdf

[8] PBWORKS, "Advantages and Disadvantages of Technologies" Available: http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies.

Author' Biography

AUTHOR 1

Kapil Chauhan is a Post-Graduate student of Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh, India.

He is pursuing M.Sc in Networking Technology and Management. He is having degree in Bachelor of Computer Application (BCA) and certification of Software Engineering from NIIT. He has attended many conferences and seminar held by EC Council and Cisco.

AUTHOR 2

Dr. Himanshu Gupta is associated with academics and research activities since last ten years. He is working as a Senior Faculty Member in Amity Institute of Information Technology, Amity University, Noida.

Dr. Himanshu Gupta is having specialization in Network Security & Cryptography. He is having prestigious membership in various reputed International Technical and Research Organizations as IEEE Computer Society (USA), TIFR (India), CSI (India), CSTA (USA), IACSIT (Singapore), CRSI (India), UACEE (Australia) and World Association of Young Scientists (Paris). He has successfully completed a patent titled as "A Technique & Device for Multiphase Encryption" under the domain area of Network Security & Cryptography in the field of Information Technology and many more patents have been filed in same domain.

Dr. Himanshu Gupta has attended many National and International Conferences, Seminars and Workshops and presented many research papers in the field of Information Technology. He has visited to Malaysia, Singapore, Thailand, Cambodia, Vietnam and Indonesia for his academic and research work. He has delivered many technical sessions on —Network Security & Cryptographyll in the field of Information Technology in various reputed International Conferences, World Summit and other foreign universities as an Invited Speaker. He has many Research Papers and Articles in the field of Information Technology, which have been published in various reputed Conference Proceedings and Journals.

ISSN 2277-3061