Biometrics in Network Security

Noor Fathima[1*], Pallavi B N[2], Kavitha[3]

[1,2,3]Dept. of Computer Applications, DSCASC, BANGALORE, INDIA

Corresponding Author: fathimanoor98@gmail.com

Abstract— Security has been a major interest for authentication over networking. In this modern society, mobile devices have a pertained importance with hundreds and millions users. With the help of pins, passwords there are weak authentication mechanisms which allow attackers to access the stored data. By implementing various methods for key exchange cryptographic can solve the problem of security. Identity verification is a developing and mesmerizes much attention. Biometric recognition mainly relates to the automatic recognition of individuals based on their behavioral characteristics. Almost appropriate is based on vein pattern is an approach that uses the vast network of blood vessels that lie underneath a skin. Vein pattern are unique and also difficult to duplicate even twin has an unlike and unique vein structure. Biometric security devices measure unique characteristics of a person, such as voice pattern, the iris or retina pattern of the eye and finger print. In biometrics, it is very difficult for someone to break into a system. Biometric security is a mechanism which is used to prove and provide access to a facility or system based on the automatic and direct verification of a single person's physical behavior.

Keywords: Authentication, cryptography, networking.

I. INTRODUCTION

A.*Biometrics*
It is the activity and applied math analysis of people's distinctive physical and activity characteristics. .Biometrics has the capability to prove dramatically quicker, easier and safer than normal passwords; however organization got to watch out concerning the biometric information they collect. The technology is principally used for identification and access management or for distinguishing people WHO area unit underneath police work. Biometric identifiers area unit the distinctive, measurable characteristics won't to label and describe people. Biometric identifiers area unit usually classified as physiological versus activity characteristics. Physiological characteristics unit of measurement related to the shape of the body. Examples embrace, however aren't restricted to fingerprint, palm veins, face recognition, DNA, palm print, hand maths, iris recognition, animal tissue and odor/scent. Behavioral characteristics unit related to the pattern of behavior of a private, together with however not restricted to typewriting rhythm, gait, and voice. Some of the researchers have been coined the term biometrics to describe the latter class of biometrics.

Because life science will offer an inexpensive level of confidence in authenticating an individual with less friction for the user, it has the potential to dramatically improve enterprise security. Computers Associate in nursing devices will unlock mechanically once they find the fingerprints of an approved user. Server area doors will swing open once they acknowledge the faces of sure system directors. Help table systems would possibly mechanically pull up all relevant data once they acknowledge Associate in nursing employee's voice on the support line.

B.*Types of biometrics*
A biometric symbol is one that's associated with intrinsic human characteristics.
They fall roughly into 2 categories:
Physical identifiers and Activity identifiers.

• Fingerprints: Fingerprint scanners have found everywhere in recent years due to their widespread classification on smart phones.
Any device that may be touched, such as a phone screen, computer mouse or touchpad, or a door panel, has the ability to become an easy and convenient fingerprint scanner.

• Photo: If a tool is supplied with a camera, it can easily be used for authentication.
Facial recognition and retinal scans area unit 2 common approaches.

• Physiological recognition: biometric identification is that the second commonest style of authentication, according to Spice works, in place at 14 percent of companies.

Other image-based authentication strategies embrace hand pure mathematics recognition, used by 5 percent of companies, iris or retinal scanning, palm vein recognition, and ear recognition.

• Voice: Voice-based digital assistants and telephone-based service portals square measure already exploitation voice recognition to spot users and demonstrate customers.

• Signature: Digital signature scanners square measure already in widespread use at retail checkouts and in banks and square measure an honest selection for things wherever users and customers square measure already expecting
To have to sign their names.

• DNA: nowadays, DNA scans square measure used primarily in enforcement to spot suspects -- and within the movies.

II. APPLICATIONS OF BIOMETRICS

A. Airport Security
Making the journey through airfield terminals additional seamless for passengers could be a goal shared by airports round the world. Biometric technology to verify rider identities has been utilized in many giant international airports for variety of years and therefore the technology is quickly spreading to alternative locations across the globe.

In several airports, the highest biometric modality alternative for immigration management is iris recognition. In order to use iris recognition, travelers are initial registered by having a photograph of their iris and face captured by a camera. Then, their distinctive details are keep in a world info for quick, correct identification at ports of entry and exit that use iris recognition for somebody biometric authentication. When traveling, rather than waiting in long queues to be processed, passengers merely walk into a booth and appearance into associate degree iris camera. The camera then photographs the iris and a software program then matches the details with the information stored on the database.

Biometrics simplifies the airfield expertise for countless passengers traveling each day. Use of the technology additionally ensures the very best level of security and safety

B. Time and Attendance
Workforce management is another field wherever the employment of bioscience is on the increase. Fraudulent worker time and group action activities area unit a standard development in organizations throughout the globe. According to associate Yankee Payroll Association study, the typical worker reportedly steals roughly four and a 0.5 hours per week, that is such as six weeks' vacation if figure over a year. To solve this issue, firms area unit implementing biometric time clocks on their work sites.

A biometric time associated group action system is that the machine-controlled technique of recognizing a worker supported a physiological or behavioral characteristic. The most common biometric options used for worker identification area unit faces, fingerprints, finger veins, palm veins, irises, and voice patterns. When associate worker makes attempt identification by their biological traits, a biometric hardware device compares the new scan to any or all accessible templates so as to seek out a definite match.
Even government organizations currently suppose bioscience for making certain timely group action of workers and correct payroll calculations.

Law Enforcement
Organizations just like the Federal Bureau of Investigations (FBI) and international law enforcement agency are mistreatment bioscience in criminal investigations for years. Today, bioscience is wide employed by enforcement agencies across the globe for the identification of criminals. In 2008, the Chinese Police adopted an ABIS solution to allow forensic fingerprint examiners the ability to cross check inmate identities for possible matches within the database.

Biometrics is additionally wide used for jail and jail management. Biometrics provides recent details of the Jail Authority, Public Safety Departments, and Governments can safely and securely manage prisoner identities.

Access Control & Single Sign On (SSO)
II. THE PRIMARY REASON BEHIND A LOT OF AND A LOT OF ORGANIZATIONS AND PERSONNEL ACROSS THE WORLD ADOPTING BIOMETRIC TECHNOLOGY FOR ACCESS MANAGEMENT AND SINGLE CHECK IN (SSO) IS AS A RESULT OF ANCIENT AUTHENTICATION TECHNIQUES LIKE PASSWORDS ARE INSUFFICIENT FOR PERSONAL IDENTIFICATION. PASSWORDS SOLELY OFFER PROOF OR PROOF OF DATA WHEREAS BIOSCIENCE PROVIDES DISTINCTIVE BLESSINGS AS A RESULT OF IT DEPEND ON DISTINGUISHING SOMEBODY BY "WHO THEY ARE" COMPARED TO "WHAT YOU RECOGNIZE "OR "WHAT YOU HAVE."

Today, bioscience is wide used round the world for home access management, mobile phone access, vehicle access authentication and Single Sign on (SSO).

Banking – Transaction Authentication
Biometrics in banking has redoubled an excellent deal within the previous few years and is being enforced by banks throughout the globe.

As world monetary entities become a lot of digitally-based, banks square measure implementing biometric technology to boost client and worker identity management in an endeavor to combat fraud, increase dealings security, and enhance customer convenience. Customers also are fed-up with fraud and therefore the inconveniences related to perpetually

having to prove their identities. As a result, a lot of and a lot of customers area unit trying to find banks that have biometric identification in situ prompting banks to a lot of closely analysis the technology for implementation.

III. NETWORK SECURITY

It is a broad term that covers a mess of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of pc networks and knowledge victimization each software system and hardware technologies.

Every organization, despite size, trade or infrastructure, needs a degree of network security solutions in situ to guard it from the ever-growing landscape of cyber threats within today.

Today's network architecture is complex and is faced with a threat environment that is always changing and attackers that are always trying to find and exploit vulnerabilities. These vulnerabilities can exist in a broad number of areas, including devices, data, applications, users and locations.

For this reason, there are a unit several network security management tools and applications in use these days that address individual threats and exploits and additionally restrictive non-compliance.

When simply a couple of minutes of time period will cause widespread disruption and large injury to Associate in Nursing organization's bottom line and name, it's essential that these protection measures area unit In place.

How Does Network Security Work?
There area unit several layers to survey once addressing network security across a company.

Attacks will happen at any layer within the network security layers model, therefore your network security hardware, software and policies must be designed to address each area. Network security generally consists of 3 totally different controls: physical, technical and body.

Here is a brief description of the different types of network security and how each control works.

Physical Network Security
Physical security controls area unit designed to forestall unauthorized personnel from gaining physical access to network elements like routers, cabling cabinets then on. Controlled access, like locks, biometric identification and alternative devices, is essential in any organization.
Technical Network Security

Technical security controls defend knowledge that's hold on on the network or that is in transit across, into or out of the network.

Protection is twofold; it has to defend knowledge and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

Administrative Network Security
Administrative security managements contains security policies and processes that control user behavior, as well as to the infrastructure however users area unit, their level of access .

IV. APPLICATIONS OF NETWORK SECURITY

A variety of popular tools that allow access to remote hosts (such as telnet, rlogin) or that provide means for file transfer (such as ftp) exchange user credentials and data in plain text. This makes them prone to eavesdropping, tampering, and spoofing attacks. Although the tools mentioned above might have conjointly been engineered upon SSL/TLS, a different protocol suite called Secure Shell (SSH) has been developed, which follows partial overlapping goals.

The SSH Transport and User Authentication protocols have options kind of like those of SSL/TLS. However, they are different in the following ways:
● TLS server authentication is ex gratia and therefore the protocol supports absolutely anonymous operation, in which neither side is authenticated. As such connections are inherently vulnerable to man-in-the middle attacks, SSH requires server authentication.

● TLS does not provide the range of client authentication options that SSH does — public-key via RSA is the only option.

● Most significantly, TLS doesn't have the additional options provided by the SSH association Protocol.
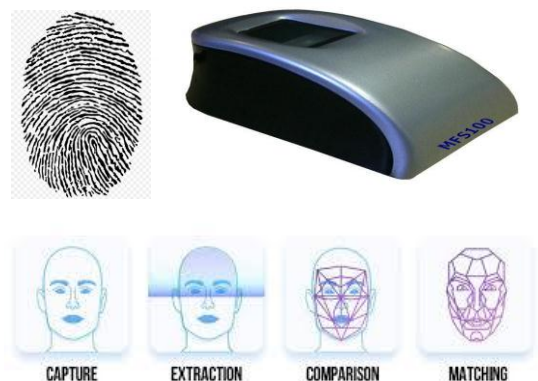

Figure 1. Image database for Biometrics

V. CONCLUSION

Biometric identification management systems offer higher security, convenience, answerableness, and correct audit trails – all attributes that encourage businesses to analysis and implement the technology for his or her own use.

We believe that as time moves forward, we are going to see implementation of biometric technology still grow and be employed in even a lot of areas that bit our lives

REFERENCES

[1]. Kirat Pal Singh Senior Project Fellow Council of Scientific and Industrial Research (CSIR) – Central Scientific Instruments Organization (CSIO) CSIR-CSIO, Ministry of Science & Technology, Chandigarh-160030

[2]. Mohammed Nasir Uddin1, Selina Sharmin2, Abu Hasnat Shohel Ahmed3 and Emrul Hasan4, Shahadot Hossain5 and Muniruzzaman6 Shanto Mariam University of Creative Technology1, 3 ,Uttara University4,5,6 IJCSNS International Journal of Computer Science and Network 16 Security, VOL.11 No.10, October 2011

[3]. SURVEY OF BIOMETRIC RECOGNITION SYSTEMS AND THEIR APPLICATIONS 1 SULOCHANA SONKAMBLE, 2DR. RAVINDRA THOOL, 3BALWANT SONKAMBLE 1Asstt Prof., Department of Information Technology , MMCOE, Pune, India 411052 2Professor, Department of Information Technology, SGGSIE&T,Nanded, India -411017 3Asstt Prof., Department of Computer Engineering, PICT, Pune, India-411043

[4]. Himanshu Srivastava Department of Computer Science & Engineering Roorkee Institute of Technology, Roorkee (U.K.), India IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013), PP 22-29

[5]. Ravi Subban and Dattatreya P. Mankame A Study of Biometric Approach Using Fingerprint Recognition Lecture Notes on Software Engineering, Vol. 1, No. 2, May

[6]. Mohammed Nasir Uddin1, Selina Sharmin2, Abu Hasnat Shohel Ahmed3 and Emrul Hasan4, Shahadot Hossain5 and Muniruzzaman6 Shanto Mariam University of Creative Technology1, 3 ,Uttara University4,5,6 A Survey of Biometrics Security System IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011

Authors Profile

Dr.Kavitha is working as a Assistant professor in dayananda Sagar College. She has publishes papers in reputed journals which includes Springer, Elsevier, Scopus, IEEE. She is the member of BOS and BOE for many universities.

Noor Fathimais currently pursuing her Bachelor's in Computer Application's. She is interested in Network and Cyber Security and interested in many other programming languages also. She is also interested in learning new technologies related to Big Data and Cloud Computing and started with certification courses.

Pallavi B N is currently pursuing her Bachelor's in Computer Application's. She is interested in Network and Cyber Security and interested in many other programming languages also. She is also interested in learning new technologies related to Big Data and Cloud Computing and started with certification courses