International Journal of Engineering Research & Management Technology ISSN: 2348-4039
March-2016 Volume 3, Issue-2
Email: editor@ijermt.org www.ijermt.org

A Review Paper on Multi-Factor Biometrics System

Ravi Kumar Gupta, Shivendra Kumar Mishra, Raushan Rituraj
Students
IIMT College of Engineering
Gr. Noida

ABSTRACT:
Security has always been a major concern for authentication over networking. Cryptographic methods solve the problem of security by implementing various methods for key exchange. Shared key is the major constraint established by Daffie Hellman Algorithm for two parties without the prior knowledge of each other over insecure communication channel. This algorithm generates the shared key with the help of receiver's public key and sender's private key. This research paper deals with the usage of finger print as the private key for generating the shared key for enhanced security.

In many parts of the world, the military has been very busy in recent times engaging in terror and other related wars. This requires that men and materials have to be located in different parts of their strategic geographic centres. And in order to ensure a fast communication with these bases, the military often deploys Mobile Ad-hoc Networks (MANETs). MANETs carry such intelligence information as: deployment information, readiness information, and order of battle plans to their various bases. The nature of these information is such that any compromise on them could be disastrous to the courses of action of the bases. This paper identifies user authentication as a key issue in strengthening security concerns in MANETs.

KEYWORDS: Military Base, Biometrics Technology, Authentication, MANET, Information security

INTRODUCTION:

"Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice."

Cryptography contains various abstraction levels of security mechanism and it builds the discipline of data encryption and decryption. Network administrator provides authorized access over the network by implementing network security and adoption of its provisions and policies to prevent unauthorized access. Authorization has always been an integral part of the security mechanism. Biometric system of identification uses unique feature of face, hands like iris, retina, finger print, structure of the face to identify a person with a unique characteristic that differentiates the concerned person from others. The system of using finger print as a parameter for authorization provides enhanced security for data transfer over the network Most military bases require the use of Mobile Ad-hoc Networks (MANETs) to establish communications between the large numbers of mobile devices deployed in the battlefield . It is therefore, instructive to state that the computer systems in military MANETs contain sensitive information, which often makes them attractive targets to unauthorised accesses. Titter, Chaplet and Stewart in provide a list of some of the sensitive information, which also includes military descriptive intelligence such as: deployment information, readiness information, and order of battle plans. Illegal access to these classes of military intelligence could compromise investigations, disrupt military planning, and threaten national security. At all times therefore, it is crucial that the computer systems in military MANETs should be protected from intruders. Consequently, this paper reviews one of the critical security protection steps that ensure that only authorised personnel gain access to the systems in the military MANETs. Consequently, we adopt the position of [1], who identifies user authentication as one of the key issues in managing security concerns in MANETs. Define a mobile ad-hoc network (MANET) as a wireless, selfconfiguring, infrastructure-less network of mobile devices, deployed oftentimes for an interim purpose. And they are important to the military because they possess the features of quick setup, takedown, and mobility features. MANETs are therefore, especially useful to the military, since they serve as channels through which they communicate in order to strategize, command, control, and operate their forces in their respective environments, in land, sea, or air . However, communications within MANET requires having legal access to the devices, as anything to the contrary will lead to information leakage on military intelligence to the opponents. And availability of military intelligence in the hands of an enemy is a bad omen for such a military base. Consequently, it becomes necessary to ensure that the identity of a person or device that attempts to gain access to the network should be authenticated. It is therefore, in line with this position that identified authentication as the first line of defence in securing MANET networks. Authentication is any process by which a system verifies the identity of a user who wishes to access it . Authentication is important in MANETs, as it ensures secure connections with a requesting entity into a network. And authentication MANETs can be based on different mechanisms. We discuss these mechanisms in the next section.

AUTHENTICATION MECHANISMS:

Allowing access to only authorised users and disallowing access to the unauthorised ones is a fundamental aspect of authentication. Authentication processes are based largely on three methods. These methods include:

1. What we know – passwords, pin codes and other personal details can be used to identify users of a particular system
2. What we have – tokens such as smartcards or key fob are also used for user authentication

3 .What we are – here, biometric features such as fingerprint scans, iris scans, palm biometrics are deploye0d for allowing access to controlled environments and .

Authentication by ‘what we know’ and ‘what we have’ increases the likelihood of identity theft as the use of passwords or tokens is not necessarily tied to the identity of the real owner of the password or token. In his study, highlights that there are consequences attributed to setting up communication with a user that has an unknown identity. A knowledge factor such as a password is not entirely secure as it can be easily guessed, intercepted or transferred to another user . In the event of User A divulging his authentication parameter such as a password to User B intentionally or accidentally, it will be difficult to capture the identity of the logged in user. More so, simple passwords can be easily guessed or cracked through brute force or dictionary attacks while complex ones can easily be forgotten. Though there are various mechanisms to protect passwords such as resetting them regularly or using passwords hints, authentication with the use of passwords is fast becoming problematic due to the sophisticated nature of technology and the pervasive Internet that allows access to all categories of information, some of which have far reaching impact on digital assets.

Nandini and Ravi Kumar in describe ‘what users have’ as knowledge based authentication also called possession factors. Possession factors have found widespread usage in recent times, as they have added another level of security to authentication. Most of ‘what users have’ technologies are based on a two factor authentication mechanism, with PINs or passwords as secondary authentication features. Using a smart card or key fob, for instance, is a great way to enhance privacy. Most of the smart cards have the user’s information engraved in them with peculiar attributes that maps the identity of the user to the card. Though this creates a sense of security for the numerous users across the globe, the use of tokens is subject to replay and active attacks . However, possession factors can be lost, stolen or damaged . In such a situation, replacing them is necessary. But there is the possibility of using them to commit crime before they can be retrieved. This can create problems for the owner. Since a card owner may have his name engraved on a card, using it by a malicious user, if lost, will still record a transaction against the card owner. This is a serious security.

APPLICABLE BIOMETRIC TECHNOLOGY:

The biometric technology is leveraged by a number of methodologies that can be deployed in the realisation of biometric authentication. Some of these, as discussed and include the following:

a. Palm biometrics
b. Fingerprint authentication
c. Voice recognition
d. Signature verification
e. Iris scan and
f. Facial recognition
g. DNA
All of these are necessary. However, this paper focuses on the first three above: palm biometrics, fingerprint authentication and voice recognition.

A. PALM BIOMETRICS:

Palm biometrics is based on the use of biometric traits extracted from the palm (curvature of the palm, width of the palm, length of fingers, thickness of the palm, principal lines, wrinkles, delta points etc [7]) to verify the identity of a person in a controlled environment. The use of palm biometrics, on itself, cannot guarantee an efficient user identification system without being augmented by other identification methods such as the use of personal identification numbers (PIN) as the human hand is not unique. The reliability provided by palm biometrics in the context of verification and authentication is considerably high. Non repudiation is enhanced as a user cannot deny that a physiological trait such as a palm print image does not belong to him/her once logged in. Tracking users' access and the use of resources can be controlled. Also, there is more convenience for users and system administrators as incidences of password or identification card theft or loss may not be obtainable thereby enhancing efficiency. Some of the key weakness of palm biometrics is that the sensor data, if used independently of other biometric

B. FINGERPRINT AUTHENTICATION:

There is a proliferation in the use of fingerprint authentication in recent times . This can be seen in most mobile phone service providers. The use of fingerprints for identification and verification is borne out of the fact that the patterns of ridges and furrows that characterise an individual's finger (most especially the surface of the fingertip) are unique to each individual. Fingerprint devices allow a user to access a controlled environment through fingerprint scans. Podio in maintains that the user merely places his finger tip on the appropriate device to be identified and authenticated. This paves way for secure access control and network authentication mechanism. However, fingerprint biometrics can be given to the weaknesses of palm biometrics especially when there is an accumulation of skin oils or dirt on the surfaces of sensor plates. The resultant effect may be false rejection in which case a valid user fingerprint scan is rejected as illegitimate. False acceptance can also be obtainable here where an invalid fingerprint scan is accepted as valid for a given user transaction [7].

C. VOICE RECOGNITION:

Voice recognition is based on the distinct rate and pitch of sounds produced by the human voice [9], as well acoustic features of speech including the shape of the throat, speaking style and size of the mouth [3]. Kounoudes et al in [2] mention that voice authentication is preceded by the extraction of voiceprints, which are stored during the enrolment phase and matched with raw speech data captured by voice recognition devices such as a voice speaker or microphone.

Xiao in [5] identifies two types of technologies for voice biometrics namely voice scans and speech recognition. The main distinction between the two technologies is that while voice scans use a pre-stored voice sample of the user to authenticate and verify the identity of the user, speech recognition depends on words and sentences from an audio signal, which form the input to a voice recognition device.

Zhang and Abdulla in [10] proposed a voice biometrics technique based on human auditory models and independent component analysis. The auditory models were found to achieve better identification rates with high robustness to noise. Furthermore, Rashid et al in [9] implemented a security system that allows for voice patterns as the access control key thereby enhancing the accuracy of the authentication process since voice patterns as seen to be distinct per individual. The design of the proposed auditory models, access control mechanism, and voice recognition system is suitable for deployment in military controlled environments.

One major advantage of voice biometrics is that it does not require physical contact with the authenticating device though it can be subject to background noise, which may lead to a high rate of false rejection [2]. However, voice templates, as highlighted in [1] are small in size basically less than 16 kilobytes and can be represented using neural networks, decision trees, pattern matching algorithms and hidden Markov models.

D. IRIS:

It is the annular region of the eye surrounded by the pupil and the sclera on either side. During the first two years of life, the visual texture of the iris is formed. A fully developed iris carries very unique information useful for personal recognition. But the system might be expensive and usage might be complex .

E. DNA:

Deoxyribonucleic acid (DNA) is the unique code for identifying an individual except for the fact that it's same for identical twins. It is mostly used in forensic applications for person recognition. The major limitation is that a DNA sample can easily be stolen from a person without getting noticed

F .FACE RECOGNITION:

Facial images are the most common Biometric characteristic. Humans are personally recognized through their face. The most popular approaches for face recognition include the location and shape of facial attributes like eyes, eyebrows, nose, lips, chin, and their spatial relationships [9].

BIOMETRICS BASED AUTHENTICATION SYSTEM:

Biometrics characteristics are a unique, measurable physiological and/or behavioural trait of a human being for automatically recognizing or verifying his/her identity. All human have their own unique biometrics in the overall human body structure. As mentioned above, biometrics classifies physiological and behavioral factors. Typical physiological factors are fingerprint, hand, face, iris, etc. Behavioral factors include keystroke, signature, voice, handwriting, etc., Table 1 shows the classification of biometrics

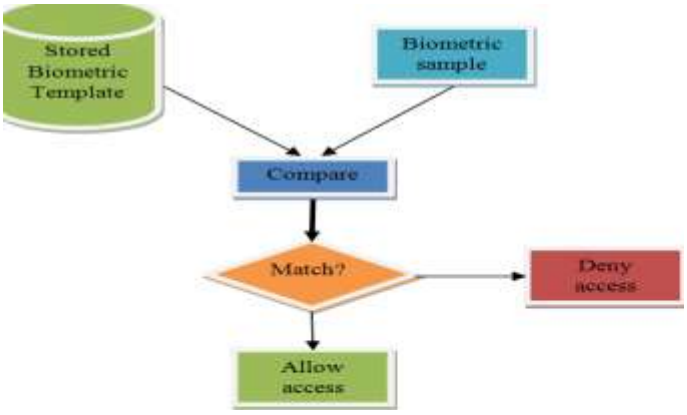
CLASSIFICATION OF BIOMETRICS:

Biometric	Classification			
Physiological				
	Fingerprint	Face	Iris	Hand
Behavioral				

	Keystroke	Signature	Voice	Handwriting

BIOMETRIC AUTHENTICATION PROCESS:

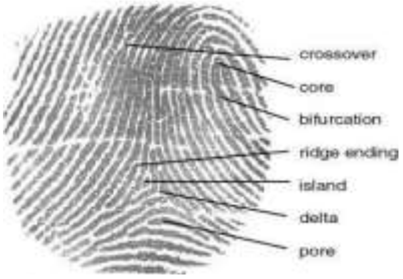
Biometric authentication is preceded by an enrolment procedure. The enrolment process requires the initial capture of the biometric traits. As stated in [3] and [7], the captured traits are pre-processed for feature extraction and stored as templates in the authenticating device or database. The performance of the biometric sample during authentication is dependent on the quality of the captured template. Figure 1 is a representation of a Biometric Authentication Process.



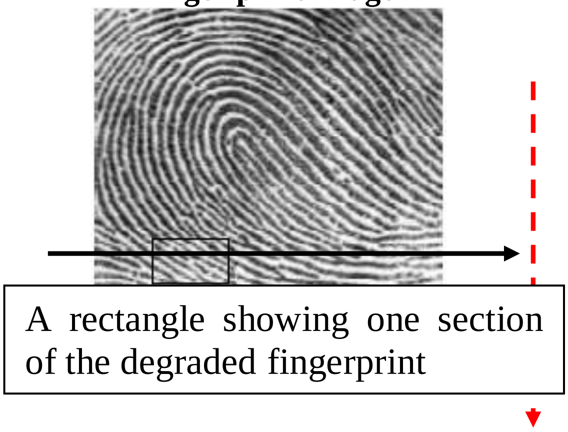
Representation of a Biometric Authentication process

Verification is an indispensable aspect of biometric authentication [6]. A user whose biometric sample has been enrolled can only be allowed access to a system such as during a login session by verification. During verification, the stored biometric template is compared with the sample presented by the user at the point of authentication. Access is allowed when a match is found and in the event of a mismatch, access is denied. Verification leads to identification and usually involves a one-to-many or one-to-one matching of the stored template in the database with the captured sample [9].

6. Fingerprint identification process



Finger print image



A rectangle showing one section of the degraded fingerprint

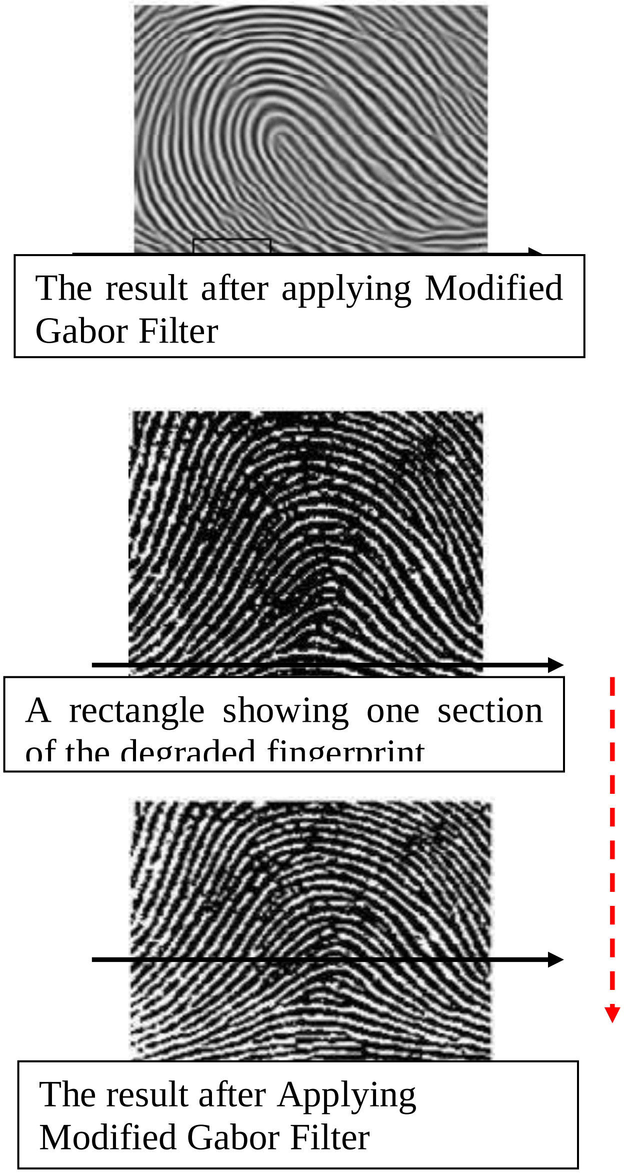
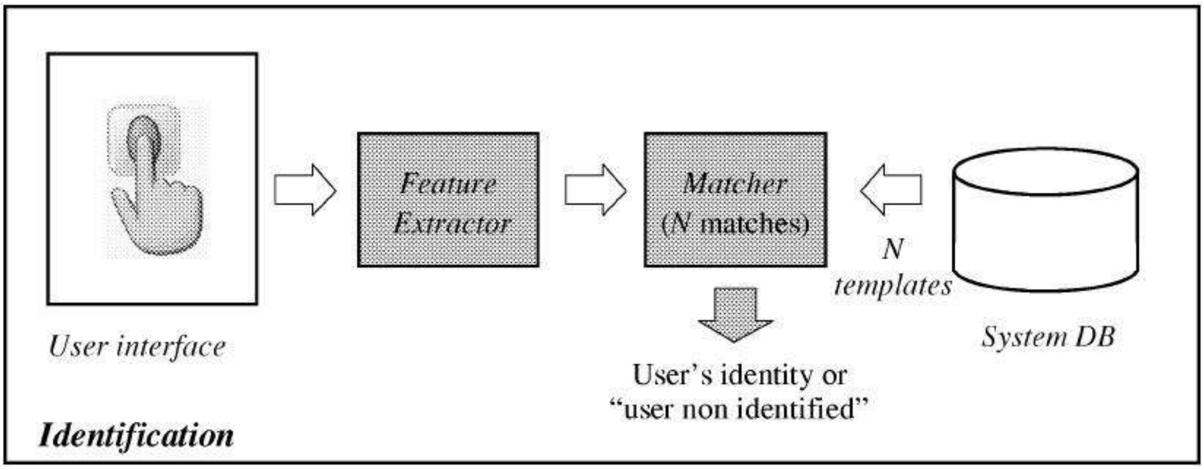

The result after applying Modified Gabor Filter
A rectangle showing one section of the degraded fingerprint
The result after Applying Modified Gabor Filter

Fig. 3. Images (a) and (c) are real-life fingerprints with distortion and misalignment; images (b) and (d) are the enhanced fingerprint

BACKGROUND:

OPERATION OF A BIOMETRIC SYSTEM:

To understand the obstacles and their solutions, the basic understanding of a Biometric system is essential. Any Biometric system typically operates in three phases- Enrolment and Identification/Verification. In the enrolment stage, a person provides an identifier (e.g. Passport, Driving License) and his/her Biometric is linked to the identifier provided [4]. This Biometric is stored in the form of a template. The Quality Checker or the Sensor module captures the Biometric data of an individual from the user interface. From this information, the salient features that are uniquely used to identify an individual are grabbed by the Feature Extraction module. The System Database Module is then used to store the Biometric templates. During the Verification or Identification phases, a Matcher module is used to determine whether the user is valid.



DECIDING TO USE A BIOMETRIC TECHNOLOGY:

There sure are many advantages of biometrics. It doesn't change over time and cannot be lost or forgot. It is next to impossible to forge a Biometric. It provides a very strong access control security solution satisfying confidentiality, integrity, authentication, and non-repudiation. Aspects like accuracy, reducing costs, user friendly devices, and universality add to the advantages. The user need not remember or carry anything with him which is a great reason to use Biometrics. However, a lot of parameters are to be evaluated before adopting or changing to Biometric system.

A detailed cost-benefit analysis should be performed [4]. All the estimated costs for installing, deploying, and educating the people should be accounted. The different kinds of benefits should be documented. The system should be adopted only if the benefits outweigh the costs. An organization should discuss with their employees, about the effects on privacy and convenience. Everything should be transparent. An employee will accept the system only if he/she has a clear idea of what's going on. Since user acceptance is the major challenge, educating the people about the technology and making them confident should be the company's top priority.

The organizations and public are slowly leaning towards using Biometrics due to the security breaches and inefficiency of the current security measures. Many surveys are being conducted to know the public perceptions about the usage of Biometrics in common places like office, ATM, and for computer logon. The following are the results obtained by Janette Moody in her survey .

Figure 3.1. Acceptable Biometric for ATM

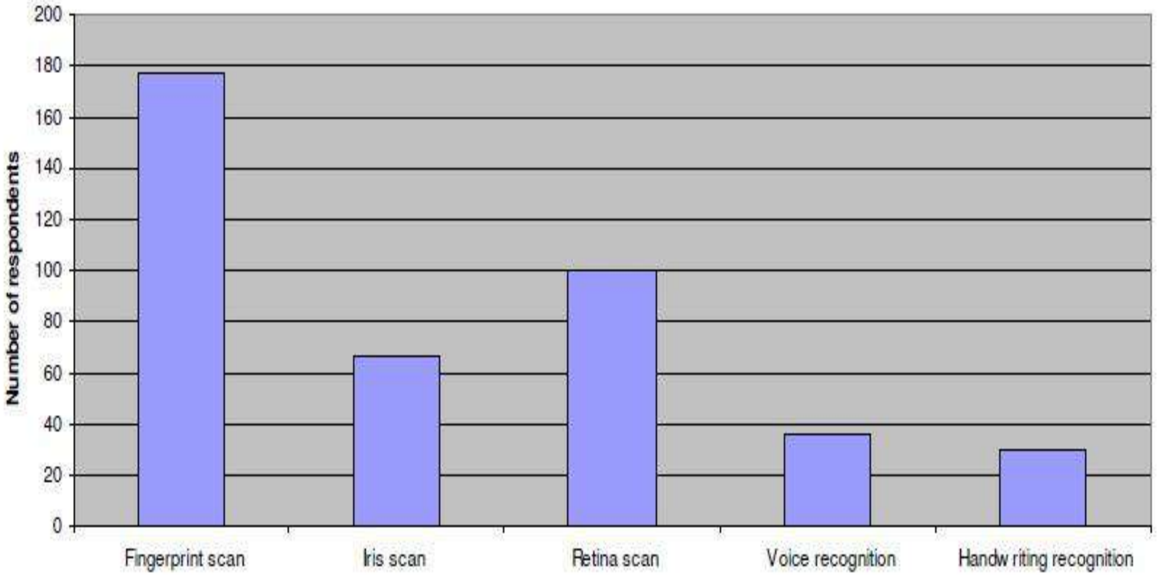


Figure 3.2. Acceptable Biometric for Computer Logon

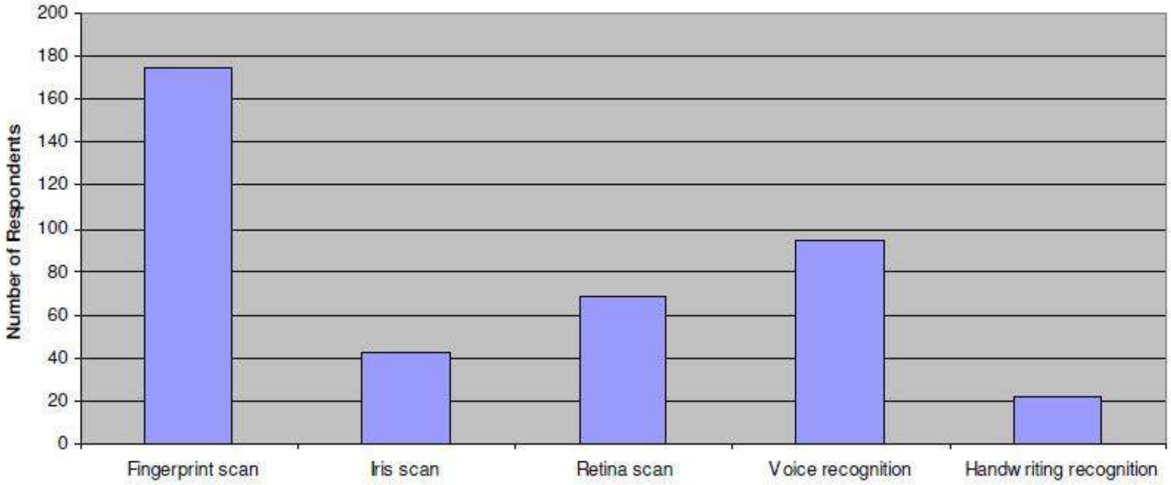
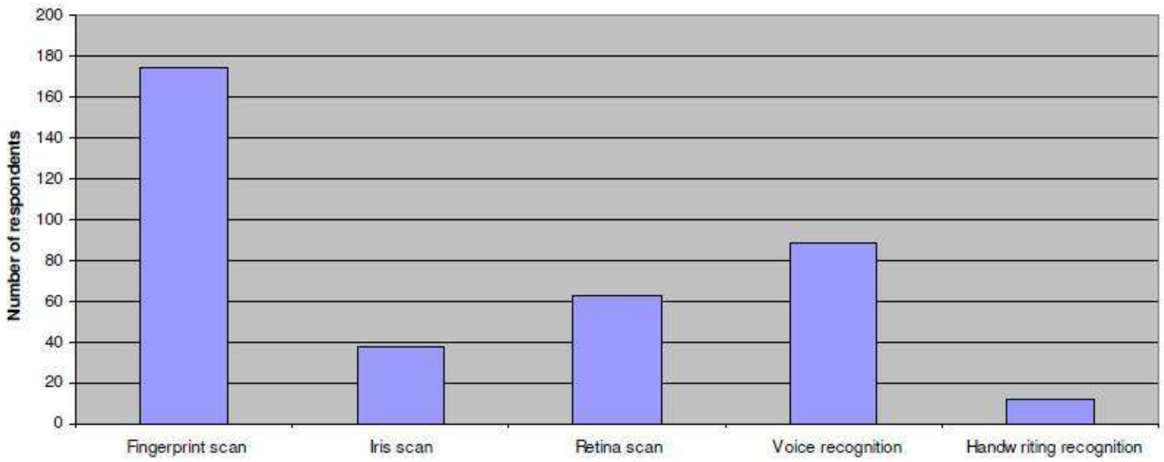


Figure 3.3. Acceptable Biometric for Office Access



From the information present in the above bar charts, it is evident that people are more comfortable using Fingerprint scan in the environments mentioned in the survey. This might be because of the public perception that it is the most easy-to-use Biometric recognition. It is also the most famous and oldest known Biometric. On the other hand, it is easy for the organizations to implement Fingerprint scan because of its accuracy and low expense.

Gone are the days where Handwriting is used for recognition. It is easy to forge and fake. So, there is no surprise that people are not comfortable in using it as a security control. They are also not interested in using iris scan and retina scan. This might be because of their perception that it is complex and that it might cause health problems or blurred vision if used regularly.

CHALLENGES FACED:

PRIVACY AND PUBLIC CONFIDENCE:

Public acceptance is the main reason obstructing the growth of Biometrics. There exists fear among people that usage of Biometrics may lead to invasion of their Privacy (freedom from observation). Different organizations store the information about different Biometric identifiers of people in their databases. They are afraid that some organizations might use this information to track their movements and behaviour and also share this information with other organizations for various reasons.

FAKE BIOMETRICS:

It is difficult to fake Biometric identifiers but not impossible. Behavioural Biometrics like signature and voice can easily be stolen compared to physiological Biometrics. Although signature is seldom used for security, a person's voice is commonly used. Voice can be mimicked. Fingerprint scanners can be tricked with a silicone finger. A mold or cast of hand can be used to fake hand Biometrics. An image/photo of the face and iris can be used to deceive the Biometric scanning systems. Iris can be faked using a contact lens also. All these techniques of faking

THEFT OF BIOMETRIC DATA:

Theft of Biometric data is another serious problem. The advantage in using Biometrics is that the Biometric identifiers don't change over time. Ironically, the advantage of Biometrics can become its greatest disadvantage. Biometric data once compromised can be a serious issue through the life time of an individual because it is difficult to replace a Biometric unlike a password or a credit card. Biometric is nothing but a binary file which is stored in the database and can be stolen by a hacker like any other file.

EASE OF USE:

This problem is closely related to the public acceptance of Biometric devices as security systems. One advantage of Biometrics is that a person need not remember or carry anything with him/her. But, user acceptance can only be obtained if the Biometric devices are convenient to use and operate. This convenience should not be provided at the cost of security .

PHYSICAL FACTORS:

There might be a case where the user might be unable to enroll in the Biometric device due to some disability or limitations in physical characteristics. This is called Failure to Enroll (FTE) . In case of diseases like arthritis, where motion of the body parts is limited, a person might not be able to place his/her hand on the device . People with wounds or bruises on their skin might also be denied access because of the inability of the scanner to scan.

SOLUTIONS:

EDUCATING PUBLIC ABOUT BIOMETRICS – SOLVES PUBLIC ACCEPTANCE AND EASE OF USE PROBLEM:

As with the introduction of any new technology, user participation and acceptance is essential. Organizations deciding to install Biometric devices would be well served if they conduct a survey on their employees in advance, to determine where their misperceptions and apprehensions might exist, if any. After extracting the facts from this information, an education program could be undertaken to specifically address their concerns. Prior to investing in any new technology, it is sensible to determine not only if it is financially and technologically viable, but also if it is functionally appropriate. Educating the public about Biometrics will help greatly to solve many problems and help in the growth of this industry. The society's misconceptions about the security, privacy and working of the technology can be eradicated through providing adequate education regarding the technology.

ENCRYPTION, CENTRALIZATION, MULTIMODAL BIOMETRICS AND REVISING ALGORITHMS – SOLVES THE PROBLEM OF THEFT:

The fact that a Biometric cannot be changed makes the theft of Biometric data a problem of top priority. Certain algorithms are used by organizations to convert the Biometric into a Binary file which is stored in a database. There should be people supervising and safeguarding the Biometric Devices and databases. These databases should be placed in inaccessible locations. Even if an attacker has the data, the corresponding Biometric cannot be regenerated with this data unless the algorithm is known. Once the attacker gets the algorithm used for conversion, he can make use of the stolen information.

ENSURING CLEANLINESS BEFORE USING A BIOMETRIC DEVICE – MITIGATES ENVIRONMENTAL FACTORS:

People should be educated about the conditions in which a Biometric device can be used. An instructor should be present at the location where the scanning is being done and should ensure trouble free scanning. In the jobs involving usage of chemicals, construction work, or mechanical works, a person's hand will be smeared with dirt or grease. He should clean his hands before fingerprint or hand scanning.

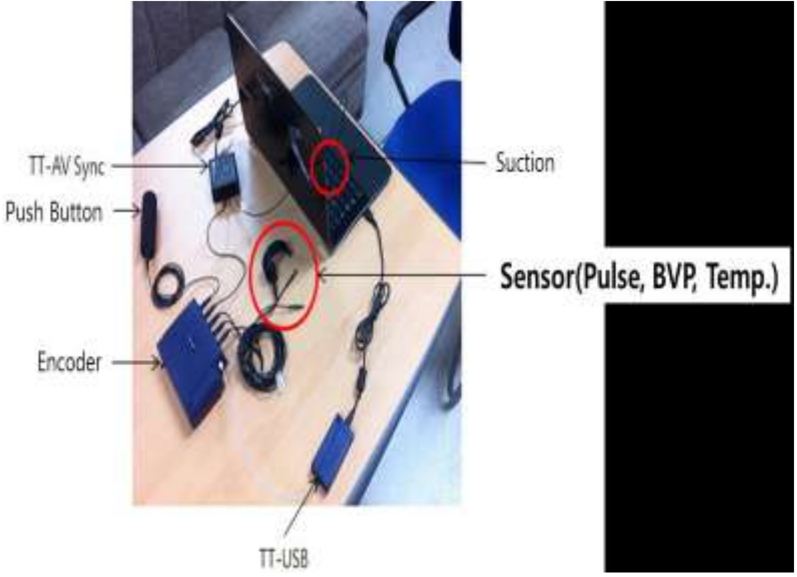
Notices and instructions can be put in an obviously visible position so that the user can go through them before moving forward for scanning

SOLVING THE PROBLEM OF PHYSICAL FACTORS:

There is no solution except to exclude a physically challenged person from the authentication process. He/she should be provided with some other means of authentication. It is important for the organization to make differently abled people comfortable so that they won't feel alienated. An alternative authentication process should also be installed for people with minor physical damages like bruise or wounds.

APPLICATION:

Biometrics signals measurement system is composed of sensor, encoder and software made in Thought Technology. A BVP (Blood Volume Pulse) sensor can measure heart rate, pulse, temperature, and skin temperature. In this research, we use only pulse. BioGraph Infiniti program [11] presents biometrics signals and reaction times. The following Figure 4 shows the components of hardware.



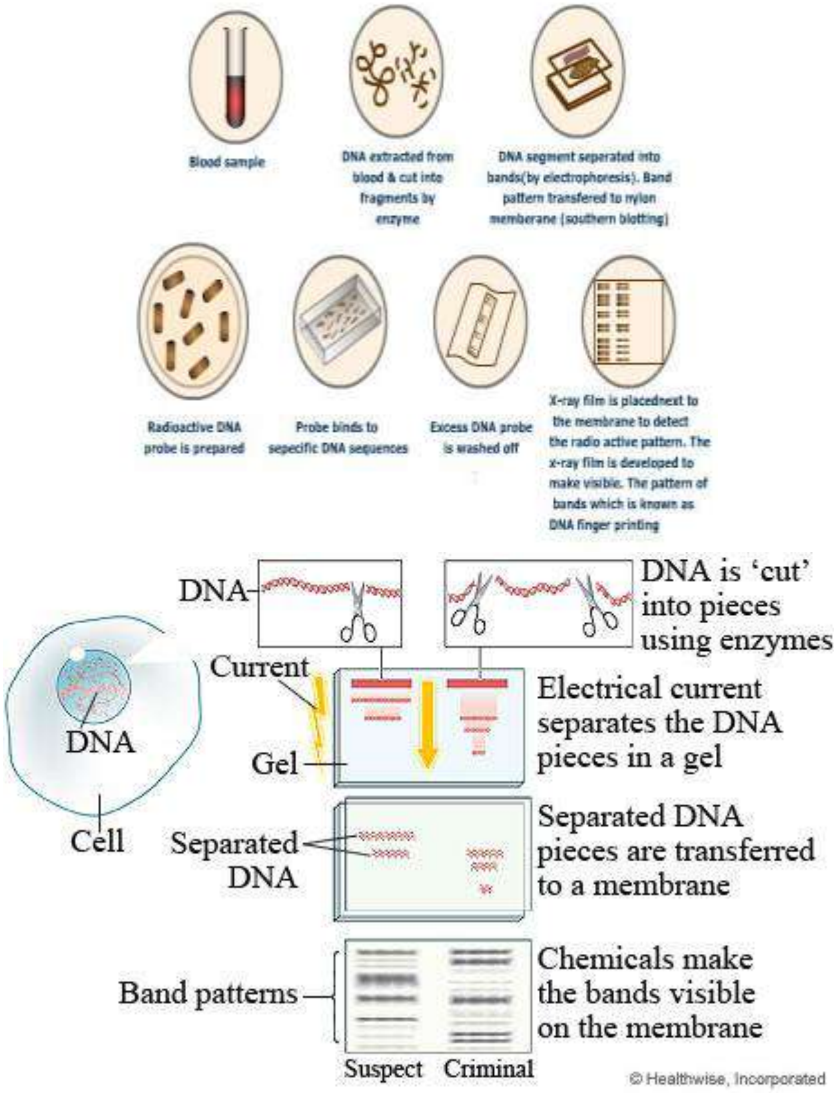
The Biometrics Signals Measurement System

CONCLUSION:

One of the key issues in managing a user's access to critical resources is the ability to allow only the authorised users of a system to such resources. Over the years, identity spoofing, man in the middle, replay and active attacks have left most military bases prone to the leakage of classified information and intelligence as well as the circumvention of established security procedures. The consequences of security breaches are grave and can lead to loss of lives, property and revenue. As seen in most third world counties, where terrorism is on the increase, leakage of sensitive information can cripple the bedrock of an economy. To this end, providing adequate and enhanced authentication mechanisms to controlled environments cannot be overemphasised.

The above research paper is proposed for enhanced network security. For this analysis, Diffie Hellman algorithm has been implemented which is based on shared key concept. The usage of finger print instead of random number as a private key in the algorithm provides better security for data transfer over the network with high confidentiality. In future to avoid high level security threats we can upgrade the system by having multi parameter security mechanisms such as hybrid combinations of Deoxyribonucleic Acid (DNA) with finger print or with retina (Figure- 12).

Figure 12: Analysis of DNA and retina with finger print


Blood sample
DNA extracted from blood & cut into fragments by enzyme
DNA segment seperated into bands(by electrophoresis). Band pattern transfered to nylon memberane (southern blotting)
Radioactive DNA probe is prepared
Probe binds to sepecific DNA sequences
Excess DNA probe is washed off
X-ray film is placednext to the membrane to detect the radio active pattern. The x-ray film is developed to make visible. The pattern of bands which is known as DNA finger printing
DNA
DNA is 'cut' into pieces using enzymes
Current
DNA
Gel
Electrical current separates the DNA pieces in a gel
Cell
Separated DNA
Separated DNA pieces are transferred to a membrane
Band patterns
Chemicals make the bands visible on the membrane
Suspect
Criminal
© Healthwise, Incorporated

ACKNOWLEDGMENTS:

It is a matter of great pleasure by getting the opportunity of highlighting fraction knowledge, acquired during my technical education through this paper. This would not have been possible without the guidance and help of many people. This is the only page where I have opportunity of expressing my emotions and gratitude from the care of my heart to them. This paper would not have been successful without enlightened ideas; timely suggestion and keen interest of my respected Guide **Prof. Dipesh Das** and Co-Guide **Prof. Parvin Rai** without his best guidance this would have been an impossible task to complete.

REFERENCES:

1. Althobaiti, O.; Al-Rodhaan, M.; Al-Dhelaan, A., (2012) "Biometric access control for wireless nodes," Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on , vol., no., pp.167,174, 21.
2. Balfanz, D., Smetters, D. K., Stewart, P., and Chi Wong, H. (2002). Talking To Strangers: Authentication in Ad-Hoc Wireless Network, Proceedings of Network and Distributed System Security Symposium 2002 (NDSS'02), San Diego, CA, February, 2002.
3. Chetty, G.; Wagner, M., (2006) "Multi-Level Liveness Verification for Face-Voice Biometric Authentication," Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session, vol., no., pp.1,6.
4. Darwish, A.A.; Zaki, W.M.; Saad, O.M.; Nassar, N.M.; Schaefer, G., (2010) "Human Authentication Using Face and Fingerprint Biometrics," Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference on , vol., no., pp.274,278
5. Dong-Ju Kim; Kwang-Seok Hong, (2008) "Multimodal biometric authentication using teeth image and voice in mobile environment," Consumer Electronics, IEEE Transactions on , vol.54, no.4, pp.1790,1797

6. Hitachi ID Systems Inc. (2014). Definition of Authentication. Available at: http://hitachi-id.com/concepts/authentication.html (Accessed: 12 January 2014)
7. Yan, H. & Long, D. (2008) "A Novel Bimodal Identification Approach Based on Hand-Print," Image and Signal Processing, 2008. CISP '08. Congress on , vol.4, no., pp.506,510
8. Ichino, M.; Yamazaki, Y., (2013) "Soft Biometrics and Its Application to Security and Business," Biometrics and Kansei Engineering (ICBAKE), 2013 International Conference on , vol., no., pp.314,319
9. Isa, M.R.M.; Yahaya, Y.H.; Halip, M.H.M.; Khairuddin, M.A.; Maskat, K., (2010) "The design of fingerprint biometric authentication on smart card for PULAPOT main entrance system," Information Technology (ITSim), 2010 International Symposium in , vol.3, no., pp.1,4
10. Yang, J. (2010) "Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System," Management of e-Commerce and e-sGovernment (ICMeCG), 2010 Fourth International Conference on , vol., no., pp.405,410.