Volume 6, Issue 11, November 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Based on Biometric Technology in MANET-A Comparative Study & Applications

Anubha Sharma, Ritu Patidar, Rupali Dave, Shweta Jain, Khushboo Karodiya
CSE & SVITS, Indore, Madhya Pradesh,
India

Abstract: In many areas, today Security is main issue. Mainly in various intelligent areas like Military and Defence and various other where security is priority. Here in this paper we introduce a security technique using Biometric technology. By using the biometric technique authentication can be highly achieved without any fraud. Before describe biometric techniques we explain here in this paper some very common attacks that can be occurred in many places when use Mobile ad-hoc Networks (MANET). This paper therefore present some attacks and then review of biometric techniques and advantages of using this technique in various places.

Key Terms: MANET, Authentication, Information Security, Security Attacks, Biometric techniques.

I. INTRODUCTION

Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc Network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission [13].It lacks any fixed infrastructure like access points or base stations. It lacks centralized administration and is connected by wireless links/cables. Wireless ad hoc network can be build up where there is no support of wireless access or wired backbone is not feasible[]13]. All network services of ad hoc network are configured and created on the fly. So that there are various intruders attack possible in MANET.

These attacks can be categorized into two parts as:

A. Data Traffic Attack:

Information traffic attack bargains either in hubs dropping information parcels going through them or in deferring of sending of the information bundles. A few sorts of attacks pick casualty bundles for dropping while some of them drop every one of them regardless of sender hubs. This may very debase the nature of administration and builds end to end delay. This additionally causes huge loss of imperative information. For e.g., a 100Mbps wireless link can carry on as 1Mbps association. In addition, unless there is an excess way around the inconsistent node, a portion of the nodes can be inaccessible from each other altogether [11].

B. Control Traffic Attack:

Portable Ad-Hoc Network (MANET) is intrinsically powerless against attack because of its crucial qualities, for example, open medium, conveyed hubs, self-governance of hubs cooperation in network (hubs can join and leave the network on its will), absence of brought together power Which can uphold security on the network, appropriated co-appointment and participation? The current routing protocols cannot be utilized as a part of MANET because of these reasons. Large portions of the routing protocols conceived for use in MANET have their individual trademark and principles. Two of the most generally utilized routing protocols is Ad-Hoc On Demand Distance Vector routing protocol (AODV), which depends on individual hub's participation in setting up a substantial routing table and Dynamic MANET On-Demand (DYMO) , which is a quick light weight routing protocol contrived for multi bounce networks. Be that as it may, each of them depends on trust on hubs taking an interest in network. The initial phase in any fruitful attack requires the hub to be a piece of that network. As there is no imperative in joining the network, vindictive hub can join and disturbs the network by seizing the routing tables or bypassing substantial courses. It can likewise listen stealthily on the network if the hub can set up itself as the most limited course to any goal by abusing the unsecure routing protocols. In this way it is of most extreme significance that the routing protocol ought to be as much secure as it can be. In spite of the fact that there can be different sorts of attack, for example, sticking attacks, which is not CONTROL attack[11]. They can be handled as a piece of physical layer security protocols. From now on those attacks won't be talked about as are out of extent of this paper.

II. AUTHENTICATION MECHANISM

A. Plaintext authentication

The simplest verification mechanism is PLAIN. The customer simply sends the password decoded to Dovecot. All clients support the PLAIN mechanism, however obviously there's the issue that anybody listening on the system can steal the password. Hence (and some others) different mechanisms were executed [4].

Today however many individuals use SSL/TLS, and there's no issue with sending decoded password inside SSL secured connections. So in case you're using SSL, you likely don't have to try agonizing over whatever else than the PLAIN mechanism.

Another plaintext mechanism is LOGIN. It's ordinarily used just by SMTP servers to give Outlook clients a chance to perform SMTP confirmation. Take note of that LOGIN mechanism is not the same as IMAP's LOGIN command. The LOGIN command is inside taken care of using PLAIN mechanism.

B. Non-plaintext authentication

Non-plaintext mechanisms have been designed to be safe to use even without SSL/TLS encryption. Because of how they have been designed, they oblige access to the plaintext password or their own special hashed version of it. This means it's impossible to use non-plaintext mechanisms with generally used DES or MD5 password hashes [4].

On the off chance that you need to use more than one non-plaintext mechanism, the passwords must be stored as plaintext so that Dovecot is ready to create the required special hashes for all the diverse mechanisms. On the off chance that you need to use just a single non-plaintext mechanism, you can store the passwords using the mechanism's own particular password scheme.

With successful/Failure Password Database (e.g. PAM) it's impractical to use non-plaintext mechanisms by any means, because they just support confirming a known plaintext password [1].

Nandini and RaviKumar in [14] 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 [2].

However, possession factors can be lost, stolen or damaged [12]. 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 concern.

III. BIOMETRIC TECHNIQUES

The biometric innovation is utilized by various methodologies that can be conveyed in the acknowledgment of biometric confirmation. Some of these, as discussed in [8] and [3] include the following:

1) Palm biometrics
2) Fingerprint authentication
3) Voice recognition
4) Signature verification
5) Iris scan
6) Facial recognition

Biometrics characteristics are a remarkable, measurable physiological or potentially behavioral quality of an individual for naturally perceiving or checking his/her personality. All human have their own one of a kind biometrics in the general human body structure. As said above, biometrics orders physiological and behavioral variables. Average physiological elements are unique mark, hand, confront, iris, and so forth. Behavioral variables incorporate keystroke, signature, voice, handwriting, and so forth. Table 1 demonstrates the characterization of biometrics [1].

Table 1 Classification of Biometric Technologies

Physiological	Behavioural
Fingerprint	Keystroke
Face	Signature
Iris	Voice
Hand	Handwriting

Not at all like different types of biometric scanners, palm vein peruses are vigorous and examine underneath the surface of the skin exhibiting a high resistance of skin surface issues, for example, dryness, unpleasantness, dampness, or scarring.

With an amazingly low false acceptance rate (FAR) and false reject rate (FRR), non-meddling contactless verification, and the most noteworthy dependability of all hand or finger based biometric validation scanners, the M2-PalmVein™ scanner is the perfect biometric acknowledgment gadget contrasted with other biometric Hardware for all situations[6].

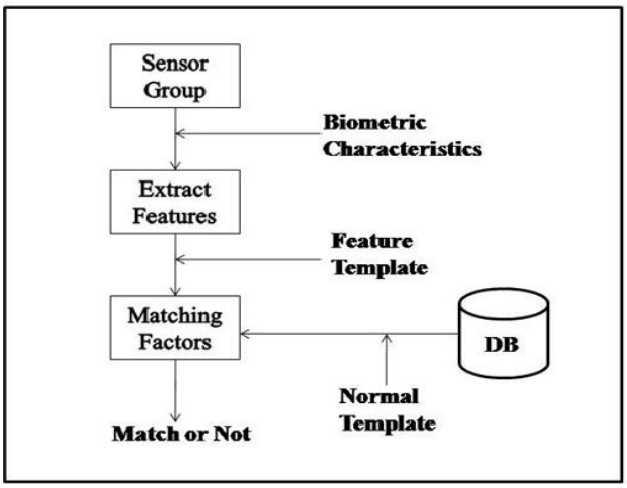

Fig 1 :-Security System Based on Biometric Technique

A. Features

- **Difficult to Forge** Since vein designs exist within the body, it is for all intents and purposes difficult to reproduce somebody's biometric format. The sensor of the palm vein scanner needs the hand and blood stream to enlist a picture.
- **Accuracy** Sophisticated back end search algorithms allow for near 100% identification accuracy. The palm vein reader has a high tolerance for skin surface problems that otherwise limit the effectiveness of other biometric modalities allowing for universal applicability and a high level of user acceptance.
- **Compatibility** Palm vein innovation can be executed in both 1:1 and 1:N coordinating situations. The new M2SYS Hybrid Server™ empowers clients to execute unique mark , finger vein, palm vein, and iris acknowledgment innovation on a similar server stage.

B. Benefits

1) Can be deployed in a variety of implementation settings.
2) Can be used by anyone – the palm vein scanner has virtually no physiological restrictions.
3) Sophisticated algorithms allow for near 100% accuracy every time.
4) High tolerance of skin surface problems, e.g. roughness, moisture, and dirt.
5) High level of user acceptance.
6) No privacy issues.
7) More affordable than other palm vein readers in the same category.

Unique finger impression acknowledgment or unique mark validation alludes to the computerized strategy for checking a match between two human fingerprints. Fingerprints are one of many types of biometrics used to recognize people and check their character.

Unique mark handling has three essential capacities: enlistment, seeking and confirmation. Among these capacities, enlistment which catches unique mark picture from the sensor assumes an essential part. A reason is that the way individuals put their fingerprints on a reflect to sweep can influence to the outcome in the seeking and confirming procedure. Concerning confirmation work, there are a few procedures to match fingerprints, for example, connection based coordinating, details based coordinating, edge highlight based coordinating and particulars based calculation. Be that as it may, the most mainstream calculation was details based coordinating calculation because of its effectiveness and exactness.

All voice-acknowledgment frameworks or projects make blunders. Shouting youngsters, woofing puppies, and boisterous outer discussions can create false info. Quite a bit of this can be kept away from just by utilizing the framework as a part of a calm room. There is likewise an issue with words that sound alike yet are spelled diversely and have distinctive implications - for instance, "listen" and "here." This issue may some time or another be to a great extent conquer utilizing put away relevant data. Notwithstanding, this will require more RAM and speedier processors than are at present accessible in PCs.

Signature confirmation is a method utilized by banks, insight organizations and prominent establishments to approve the personality of a person. Signature confirmation is frequently used to think about marks in bank workplaces and other branch catch. A picture of a mark or an immediate mark is encouraged into the mark confirmation programming and contrasted with the mark picture on record. Signature confirmation is a sort of programming that analyzes marks and checks for validness. This spares time and vitality and forestalls human mistake amid the mark procedure and brings down odds of extortion during the time spent verification. The product generates a certainty score against the mark to be confirmed. Too low of a certainty score implies the mark is in all probability a phony.

Signature verification software has now become lightweight, fast, flexible and more reliable with multiple options for storage, multiple signatures against one ID and a huge database. It can automatically search for a signature within an image or file.

Iris acknowledgment is a mechanized strategy for biometric recognizable proof that utilizations scientific example acknowledgment methods on video pictures of either of the irises of an individual's eyes, whose mind boggling random examples are extraordinary, stable, and can be seen from some separation. Any individual who has seen the TV show "Las Vegas" has seen facial acknowledgment software in activity. In any given scene, the security office at the anecdotal Montecito Hotel and Casino utilizes its video reconnaissance framework to pull a picture of a card counter, criminal or boycotted person. It then runs that picture through the database to discover a match and distinguish the individual. Before the hour's over, all awful folks are escorted from the club or tossed behind bars. Be that as it may, what looks so natural on TV doesn't generally decipher also in this present reality.

In 2001, the Tampa Police Department installed police cameras equipped with facial recognition technology in their Ybor City nightlife district in an attempt to cut down on crime in the area. The system failed to do the job, and it was scrapped in 2003 due to ineffectiveness. People in the area were seen wearing masks and making obscene gestures, prohibiting the cameras from getting a clear enough shot to identify anyone.

IV. APPLICATIONS

Biometric innovation can be utilized for an extraordinary number of uses. Odds are, if security is included, biometrics can make operations, exchanges and regular day to day existence both more secure and more helpful. Here you will discover a rundown of the numerous zones of sending for biometrics and the organizations that give relevant personality arrangements.

A. Border Control and Airport Biometrics

A key range of utilization for biometric innovation is at the outskirt. Any individual who's gone via air can let you know security checkpoints fringe intersections are the absolute most baffling spots to need to travel through. Gratefully, biometric innovation is robotizing the procedure. Trusted traveller screening activities and computerized e-Gates and stands are making the universal travel encounter less demanding on travellers while increasing the effectiveness for government offices and keeping outskirts more secure than at any other time.

B. Consumer and Residential Biometrics

Late developments in portability and availability have made a demand for biometrics in the homes and pockets of purchasers. Cell phones with unique mark sensors, applications that take into consideration facial and voice acknowledgment, portable wallets: these are the inexorably prevalent ways that shoppers around the globe are discovering biometric in their lives. Presently, on account of the ascent of the Internet of Things and associated auto innovation, biometrics are discovering their way into the car and into our homes. And why not? Cutting edge security and comfort are prepared for standard appropriation.

C. Financial Biometrics

Late developments in portability and availability have made a demand for biometrics in the homes and pockets of purchasers. Cell phones with unique mark sensors, applications that take into consideration facial and voice acknowledgment, portable wallets: these are the inexorably prevalent ways that shoppers around the globe are discovering biometric in their lives. Presently, on account of the ascent of the Internet of Things and associated auto innovation, biometrics are discovering their way into the car and into our homes. And why not? Cutting edge security and comfort are prepared for standard appropriation.

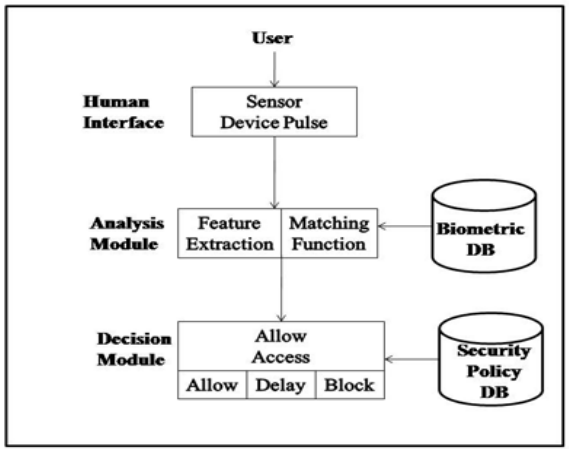

Fig 2:- Design View Biometric Signal based Structure

D. Biometric Locks

On the off chance that you have something worth ensuring why not give it the star treatment? Biometric physical get to control arrangements are more grounded verification techniques than keys, scratch cards and PINs for a basic reason: they're what you are, not what you have. While a key can be lost or stolen and utilized by an unapproved individual, your fingerprint is something special that lone you have. Unique mark biometric locks are ideal for keeping entryways shut to everything except those approved to utilize them.

E. Biometrics in Healthcare

Biometrics bring security and comfort wherever they're conveyed, however in a few examples they likewise bring expanded association. In the field of social insurance this is especially valid. Wellbeing records are probably the most significant individual archives out there, specialists require access to them rapidly, and they should be accurate. A slip by in security and legitimate bookkeeping can mean the contrast between an auspicious and accurate determination or empower wellbeing misrepresentation. Biometrics tackles those issues.

F. Justice and Law Enforcement Biometrics

Biometric innovation and law requirement have a long history, and numerous imperative character administration advancements have grown from this helpful relationship. Today, law implementation biometrics are genuinely multimodal; unique mark, face and voice acknowledgment all assume their own one of a kind part in upgrading open security and finding needed people.Whether it's a portable answer for in-field utilize, a period and participation following framework, or biometric programming that can help in the investigation of a lot of rich media, the merchants beneath have you secured.

G. Mobile Biometrics

It is hard to exaggerate the gigantic effect that the cell phone has had on all parts of life. As we turn out to be progressively associated awesome advantages in productivity open up, however without the correct security said efficiencies can get to be vulnerabilities. Because of biometric programming the influences standard portable equipment, and in addition developments in sensor producing that have prompt to the ascent of the unique mark filtering cell phones. Wearable tech is ended up being a comparative territory of chance for biometric applications similar to the developing Internet of Things.

In many parts of the world, the military has been extremely occupied lately captivating in dread and other related wars. This requires men and materials must be situated in various parts of their vital geographic focuses. Also, keeping in mind the end goal to guarantee a quick correspondence with these bases, the military regularly sends Mobile Ad-hoc Networks (MANETs). MANETs convey such insight data as: arrangement data, preparation data, and request of fight arrangements to their different bases. The way of these data is with the end goal that any bargain on them could be tragic to the game-plans of the bases. This paper recognizes client verification as a key issue in fortifying security worries in MANETs. The papers promote embraces biometrics advances as the inclining choices with the end goal of acquiring a more genuine impression of the characters of the clients of specially appointed systems. This paper hence, surveys different biometrics innovation execution techniques accessible, and prescribes the selection of one, or a mix of them by army installations.

H. Authentication Using Biometric Technique:

In this PC driven period, wholesale fraud and the misfortune or revelation of information and related protected innovation are developing issues. We each have numerous records and utilize different passwords on a continually expanding number of PCs and Web destinations. Keeping up and overseeing access while securing both the client's character and the PC's information and frameworks has turned out to be progressively troublesome. Key to all security is the idea of confirmation - checking that the client is who he claims to be.We can confirm a character in three courses: by something the client knows, (for example, a secret key or individual ID number), something the client has (a security token or savvy card) or something the client is (a physical trademark, for example, a unique finger impression, called a biometric). Biometric validation has been generally viewed as the most idiot proof - or possibly the hardest to fashion or farce. Since the mid 1980s, frameworks of recognizable proof and verification in light of physical qualities have been accessible to big business IT. These biometric frameworks were moderate, meddlesome and costly, but since they were for the most part utilized for guarding centralized server get to or confining physical section to generally couple of clients, they demonstrated workable in some high-security circumstances. A quarter century, PCs are much quicker and less expensive than any time in recent memory. This, in addition to new, cheap equipment, has recharged enthusiasm for biometrics.

V. CONCLUSION

Biometric Authentication is any procedure that approves the personality of a client who wishes to sign into a framework by measuring some inborn normal for that user. Biometric tests incorporate fingerprints, retinal outputs, confront acknowledgment, voice prints and not withstanding writing patterns. Biometric Authentication relies on upon estimation of some one of a kind trait of the client. They assume that these client attributes are special, that they may not be recorded and procreation gave later, and that the inspecting gadget is carefully designed.

VI. FUTURE WORK

The work can be extended for multi-factor authentication scheme.

REFERENCES

[1] R. Awasthi and R. A. Ingolikar, “A Study of Biometrics Security System”, J. Innovative Research &Development, vol. 2, Issue 4, (2013), pp. 737-760.

[2] S. P. Cheon, J. M. Kang, M. W. Park and J. H. Eom, “The Scheme of 3-Level Authentication Mechanism for

Preventing Internal Information Leakage In", The 4th International Conference on Digital Information and Communication Technology and its Application, (2014), pp. 154-157.

[3] N. Dahiya and C. Kant, "Biometrics Security Concerns In", The 2nd International Conference on Advanced Computing & Communication Technologies, IEEE Press, New York, (2012), pp. 297-302.

[4] "Biometrics Security Considerations", www.nsa.gov/snac.

[5] J. Wayman, A. Jain and D. Maltoni, Eds. "Biometric Systems", Technology, Design and Performance Evaluation. Springer-Verlag, (2005).

[6] S. Rane, Y. Wang, S. C. Draper and P. Lshwar, "Secure Biometrics", IEEE Signal Processing Magazine, IEEE Press, (2013).

[7] "The application and Problems of Biometrics", http://www.kipo.go.kr.

[8] W.-H. Yang and S.-P. Shieh, "Password Authentication Schemes with Smart Cards", J. Elsevier Computers & Security, vol. 18, no. 8, (1999), pp. 727-733.

[9] E.-J. Yoon, "Cryptanalysis of RSA based Password Authentication Scheme with Smart Card In", The International Summer Conference on IEIE, (2012), pp. 866-869.

[10] T. Ye-wei, S. Xia, Z. Hui-xiang and W. Wei, "A Biometric Identification System Based on Heart Sound Signal In", The 3rd International Conference on Human System Interaction, IEEE Press, New York, pp. 67- 75, (2010).

[11] Julius N. Obidinnu ,Ayei E. Ibor,S. O. O. Duke ,"Improving the Security of MANETs Oriented Military Intelligence using Biometrics Authentication Technologies",Scientific Research Journal (SCIRJ), Volume 2, Issue 1, January 2014 .ISSN 2201-2796

[12] Jung ho Eom,"The Design of Robust Authentication Mechanism using User'sBiometrics Signals",International Journal of Security and Its Applications Vol.8, No.6 (2014), pp.71-80

