A FINGER PRINT BASED SECURITY IN MOBILE ENVIRONMENT

Varun Gupta[1], Shashank Sharma[2], Vineet Kumar Disodia[3], Rajat Aggarwal[4]

[1,2,3,4] *Department Of Computer And Science Engineering, Dronacharya Group Of Institutions, Greater Noida, Uttar Pradesh, (India)*

ABSTRACT

The increasing graph of mobile and mobile network, the need of safe-keeping user information becomes more having danger. Fingers print coming out of as a powerful solution. Finger Print is a Bio-Cryptographic. This paper presents a safety which is designed for mobile general condition. In this safety fingerprint is used as user verification took care of by a Public Key base structure or popularly known as (Public Key Infrastructure) PKI, (Elliptic Curve Cryptography) ECC. The information of finger print is hidden in the vault which is the mixture of being what it seems or is said to be (genuine) and chaff features. Fingerprint features are not only used for biometric verification but also for cryptographic key stage. The safety analysis shows that the made an offer protocol can make ready a safe and safe authentication of far away, widely different mobile users over insecure network. Experimental results on public domain data base show an acceptable verification performance. Computational costs and efficiency of our protocol is also being tested on the CLDC emulator, one making an attempt to be like using Java ME earlier known as J2ME programming technology.

Keywords: Bio cryptography, Mobile Computing, Biometric, Fingerprint Authentication.

I. INTRODUCTION

Mobile apparatuses such as mobile phones have became from simple voice exchange rule electronic apparatuses to powerful digital handsets with multiple roles such as digital camera, video recorder, radio, MP3 player, net of an insect browser(web browser), gaming purposes, the last point GPS sailing person and mobile television. Lately more and more data-centric services are provided over mobile networks. Mobile devices will store much more information such as personal data and financial information than pervious handsets. Mobile users could use the services such as trading stocks, processing very small payment and managing bank accounts and using online data storage services. The able to be taken about of mobile devices and the convenience of mobile services make them increasingly good-looking. However they are also made open to the danger of information loss and not within the law use. When mobile apparatuses are lost or stolen not only the devices themselves but also the stored information may fall into the wrong hands. Such sensitive information can be a stored PIN or a cryptographic key being the property of to a client account of an e-business system. Attackers may put to use the got hand kept apparatuses and stored information to cheat for authorization. It is widely took in that current mobile computing general condition has need of higher levels of system of care for trade. In principal, biometrics can make certain true user's existence for this reason giving greater value to the authentication always-working. Biometric look, way special to a person offer three main benefits:

1. Universality i.e., every person is owner of the biometric features.

2. Specialness i.e., it is nothing like it from person to person.

3. Performance stability (doing a play without change), which means unmoving its properties keep being hard to move during one's for all ones existence.

These qualities give power biometric based authentication and identification systems to make ready higher level system of care for trade than limited by agreement knowledge based and small thing based system. Biometric and cryptography could become amount needed to make complete to each other. It is reasonable and possible to incorporate biometric into the cryptographic infrastructure. If the biometric authentication fails then an "authentication failed" note will be returned. Fingerprint based bio-cryptographic safety protocol which further reduces the vulnerability risk. The accuracy of the made an offer (proposed) protocol is valued using the public domain fingerprint knowledge-base NIST 24. In addition, we give effect to our algorithm on Java ME one making an attempt to be like(emulator) for the test of memory use and computational efficiency. Note that we take to be true that the central server is secure and computing resource rich. This assumption is practical due to following reasons :

(i). If a chief thing(central) server is often physically safe. This will significantly reduce the level of security challenge compared with the scenario such as mobile apparatus where physical way in to the attacker is let.

(ii). In many PKI systems, a belief group is also needed or taken to be true. The rest of the paper is put into order as follows. Section 2 gives the proposed bio-cryptographic protocol. The related safety analysis is presented in Section 3. Section 4 introduces experimental results and the related issues of the Java ME implementation. The

II. PROPOSED BIO-CRYPTOGRAPHIC SECURITY PROTOCOL

Mostly available biometric cryptography systems are mainly based on the idea of cryptographic key give where the biometric authentication is dissociate from the cryptographic part. The biometric part of a greater unit can only output either a say 'accept' or 'reject' (not desired) decision. If say yes or accept the cryptographic key will be given from the key managers of a business part of a greater unit. If reject (not desired), the system will not give any key. Here, biometric part of a greater unit provides a cover mechanism for the cryptographic part of a greater unit which makes the complete work system open to attack to attacks like the trojan horse. A trojan horse program may tamper with the biometric authentication module and simply inject a say 'yes' need to the key managers of a business system-part. In our protocol, biometrics and cryptography are seamlessly (not having or joined by a seams) got mixed together. The made an offer bio-cryptographic protocol is mainly of two sides (of a question) namely user the number on a list (registration) and user authentication.

2.1. User Registration

In the user the number on a list phase, user U records, lists himself/ herself into the system. The process should be attack free. It is a safe, secured and feasible way that a new user is needed to be present at the server side to successfully complete this process. User biometric template stage should be under the control of experts, such as system controlling persons in order to give support to (a statement) the high authentication accuracy. To list, at first system will as by chance produce a nothing like it part of mind given to pleasure IDu for a user U. For convenience we take to be true the length of IDube 64bits (8bytes). Then U imprints multiple fingerprint effects on mind fgi (i=1,2,..,N) where N is the total person acting for number of acquired copies of picture.

2.2. User Authentication

In the user authentication phase, a user U imprints multiple fingerprint effects on mind fpi (i=1,2,...,N) using the scanner got ready on the apparatus where N is the total person acting for number of acquired copies of picture. The biometric part of a greater unit on the mobile apparatus copies from the small points and the one only point Mi, spi from fpi. To act an into line a new order system whose place of birth is spi is put up. All small points of Mi are greatly changed based on the new order system. The new got small point makes ready are Qi, (i=1,2,...,N). A upright with bit across matching is performed between each Q i pair in order to and safe, good small points and remove false small points. It is reasonable that most safe, good and hard to move small points will come into view as multiple times in different copies of picture. After upright with bit across matching new small set Qs is acquired where in small points in Qs are the points that come into view as in at least two copies of picture. If the number of small points in Qs is less than the pre defined threshold, it is thought out as unsuccessful person to take and no further processing will be put to death. All small of Qsare made a comparison with the points of lookup table T. If there is a match, the list of words in a book number of matched point in Qs will be added to a list L0. However, in our protocol the length of L0 is being sent to the in the middle server must be capped.

III. SECURITY STRENGTH

Attacks have put forward a serious sign of danger to the current safety system especially in mobile general condition. For a bio-cryptosystem not only the cryptographic information e.g., the key but also the biometric data should be took care of against attacks. In this section we list several typical attacks and analyse how the made an offer protocol keeps from attack against them. In reality most servers have been assumed and treated as safe even though they are not perfectly secure. Sensitive information is usually stored on the server e.g., personal information, banking details, password and so on.

3.1. Trojan Horse Attack

In such type of attacks, attackers may use a Trojan horse program to put in place of the system part of a greater unit and road going past outside town its safety mechanism limited by agreement. Biometric key give systems store an at rest key in the computer and apparatus that can be against the law made prisoner by attackers via put (decision, opinion) to one side the biometric authentication part of a greater unit. Our protocol overcomes this from supporters three points:

(1). Even in the worst example that an attacker middle way the private key of the PKI which has been stored in the mobile device, it does not help break the system as the attacker has to way the biometric authentication at the in the middle server in the first place.

(2). In our protocol the meetings key K bio is produced directly from biometric point rather than false random number generator. For this reason, Kbio is not able to say for certain. If not attackers get the being what it seems or is said to be biometric data otherwise they are not simple, not hard to uncertainly have in mind out Kbio.

(3). we do not store any at rest like in size key at either mobile client side or server side. In our protocol, the biometric and cryptography are seamlessly got mixed together.

3.2. Brute Force Attack

In cryptanalysis, an brute force attack is a way of breaking a cryptographic scheme by systematically trying a great number of possible states. The safety power of an algorithm cannot be greater than its key length. In our protocol Kbio is produced from a group of small points. Three properties x, y and z of a minutia are used for the design of Kbio. Since the mobile general condition is quite open, attackers may capture the Kbio. There exists a risk that attackers trace Kbio back to the first form biometric data. To put a stop to it, we use a not invertible cancellable greatly changed account of biometric data to produce the Kbio. By the purpose of computational efficiency we act a simple great change.

3.3. Biometric Template Attack

In our protocol Kbio starts from fingerprint data, i.e. minutiae coordinates and angles. It is observed that one fingerprint can only contain limited number of small points. If attackers become owner of small o minutiae information successfully they can narrow down the look for range of Kbio. In other words the cryptographic key space made come into existence by 20-40 precise points is small. There have existence two solutions to get answer to this hard question. One of the solution is increasing the total number of minutiae. The other is increasing the difficulty for attackers to capture the precise information. In our protocol the second solution is adopted. We insert a large amount of chaff points fake minutiae into a template T so that genuine minutiae and fake minutiae are mixed giving in the look up table. In our protocol the number of chaff points is greater than 200. A mobile device only stores T without any indication of which nodes are genuine. The safety power of a lookup table is significantly made up one's mind by how we mix the put in chaff points and true minutiae. When the overall point distribution general direction to be be equal the greatest point information entropy is achieved i.e. the template is with strongest safety. To get done this end, purpose we division into parts a fingerprint area into several small rooms. As an outcome of that the how probable of each point being made uncertain statement out is the same giving in the greatest point randomness safety power of a template.

3.4. Replay Attack And Man-In-The-Middle Attack

Replay attack is prevented by the adoption of time stamps in our protocol. The system is breakable only when an attacker has obtained the private key as well as previous transmitted notes. This L' will be broken. Even when this happens, the damage to future news is limited. This is because there are many different L' lists. Again and again of the same L' or a grouped in twos of L's will be easily sensed by the in the middle server which can apparatus to start in motion a danger sign of safety com undertaking. We can also produce a not clear template T based on cancellable template technology. This will make it in feasible to forming of word from another true minutia from L' list which also gives list cancellable experiment.

IV. EXPERIMENT

The experiment of our made an offer protocol is chiefly of two stages. At first the finger print verification algorithm used in our protocol was implemented in Matlab and tested on a PC with public domain knowledge-base. The main purpose is to value the operation of authentication accuracy. In stage two we value the ECC design on Java ME one making an attempt to be like general condition in order to research, its able to be done useable thing request and computational go quickly.

4.1. Verification Accuracy

The fingerprint sample sets we tested are from the

(1) NIST Special Database 24

(2) FVC 2002 DB2 Database

4.1.1. Experiment On NIST 24

In this experiment an a division of five finger subjects was selected from the distortion group each having 150 different copies of picture. This results in 750 person fingerprints in our experiments . In NIST Special knowledge-base 24, the live took a look at every part in turn fingerprints are got from a to do with the eye or seeing scanner of resolution 500dpi with original dimension of 720x480 pixels. For convenience, the selected fingerprints were first rightly planted downsized through normalizing and zero thick material to a new size of 256x256. We use four training copies of picture to produce one tem-plate. Firstly we got into line training copies of picture according to their one only points. Then we take the coming together of minutiae in four training copies of picture as the template T. Three test copies of picture will be has at need to generate one test minutiae set Q. The procedure of minutiae group is different from the way of producing template. Here we cross match the three question copies of picture to find all matched minutiae. Q only includes the matched minutiae so unmatched minutiae are put out as of no use. This try to make certain only the safe, good minutiae can take part in the supporters matching process. For each person or subject, 100 templates were produced through selecting different groups of training images. For each template, we as by chance selected 40 copies of picture from the same person as true test and 160 copies of picture from the rest four subjects (40 impressions from each) as imposter test. As an outcome of that, a total of 100×40×5=20000 genuine tests and 100×160×5=80000 imposter tests were performed. The authentication accuracy of a biometric system can be value put on by several metrics. Two commonly used ones are false bill of exchange rate FAR(false acceptance rate) and false not-taking rate FRR(false rejection rate). Normally, FAR is defined as the relation of the number of wrongly taken tricker tests to the total number of impost or tests. FRR is the ration of the number of incorrectly put back (not desired) being what it seems or is said to be tests to the total number of true tests.

4.2. Resource Demand And Speed In Java ME

Java flat structure, Micro Edition (Java ME) is one of most pleasing to all mobile application development technology designed for mobile apparatuses such as mobile phones. A Major Advantage of Java ME is its cross platform nature which means the same source code can be did, gave effect to on all flat structures without modification. The Java ME platform has two accounts, one for general mobile apparatuses, named the connected limited apparatus trick configuration CLDC, and the other one for more able mobile devices like smart-phones and set top boxes, named the Connected Apparatus Profile (CDC). Our attention to is put out based on CLDC because CLDC is more pleasing to all and is widely supported by nearly all Java-gave power mobile phones. We were using Sun Java radio Toolkit (WTK) 2.5. One making an attempt to be like as the development and test flat structure. WTK provides an errorless support to the latest Java me CLDC technology and Mobile Information Apparatus Profile (MIDP 2.0).

V. CONCLUSIONS

We have presented a bio-cryptographic safety signed agreement between nations designed for client-server authentication in mobile computing general condition. Different from having existence key cord used to put

together and key give designs, user authentication of our protocol is guided from far at the computer side. The made an offer design takes to be true that the computer is safe which is a common experience in most client-server requests. In order to grip different types of attacks, we designed or took up different safety apparatuses: ECC PKI is used to keep safe (out of danger) authentication process. Not clear template is made an offer to safe the true biometric point against attacks. The bio-key, with motion produced from fingerprint, is designed to keep safe (out of danger) exchange between client and computer after good authentication. Doing a play put value on NIST 24 knowledge-base shows a reasonable matching having no error has been got done. The putting into effect on Java me one making an attempt to be like gets knowledge of the made an offer approved design satisfies the resource constrained mobile devices. Future work includes adopting more sophisticated fingerprint matching algorithm and cancellable biometric template system of care for trade designs.

REFERENCES

[1] Shaw K. Data on PDAs mostly unprotected. Network World Fusion. Available from www.nwfusion.com2004.

[2] Rivest RL, Shamir A, Adleman L. A method for obtain- ing digital signatures and public-key cryptosystems. Communications of the ACM 1978; 21(2): 120--126.

[3] Koblitz N. Ellipticcurve crypto systems, Mathematics of Computation 48, 1987; 203--209.

[4] Miller V. Use of elliptic curves in cryptography, CRYPTO 85, 1985.

[5] Maltoni D, Maio D, Jain AK, Prabhakar S. Handbook of Fingerprint Recognition. Springer-Verlag: New York, 2003.

[6] Soutar C, Roberge D, Stojanov SA, Gilroy R, Vijaya Kumar BVK. Biometric encryption - enrollment and verification procedures. Proceedings of SPIE, Optical Pattern Recognition IX 1998; 3386: 24--35.

[7] Soutar C, Roberge D, Stojanov SA, Gilroy R, Vijaya Kumar BVK. Biometric encryption using image processing.Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques II, 1998; 3314: 178--188.

[8] Soutar C, Roberge D, Stojanov SA, Gilroy R, Vijaya Kumar BVK. Biometric encryption. In ICSA Guide to Cryptography Nichols RK (ed.). McGraw Hill, New York, 1999.

[9] Teoh A, GohA, NgoD. R and ommultispacequantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Transactions on Pat-