Volume 3, Issue 3, March 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Implementation of Secure Biometric Authentication Using Kerberos Protocol

**Shashidhar M S**[1]
[1]*Student M.Tech, Dept of CSE*
*Canara Engineering College, Mangalore*
*V.T.U university, Belgaum, India*

**Suresha D**[2]
[2]*Asst. professor, Dept of CSE*
*Canara Engineering College, Mangalore*
*V.T.U university, Belgaum , India*

***Abstract— Biometric security is concerned with the assurance of confidentiality, integrity, and availability of information in all forms, in this work we are focusing on biometric authentication along with all security assurance. Authentication of a person is an important task in many areas of day-to-day life including electronic commerce, system security and access control. We present Kerberos a client\server authentication protocol which can perform a secure communication over unsecured environments (internet). In this paper, we are proposing a Kerberos protocol to solve the problem of authentication between client and server. When authenticating using Kerberos a series of messages is exchanged between principals and the authentication server, as well as between the principals themselves (the client and server). Tickets must be obtained from the authentication server and then exchanged between the client and server to perform authentication. There is possibility of getting biometric template information by imposter and can change the information which leads to the leakage of information. If the authentication is not being done then there is compromise in security. The problem here is to authenticate using the information of the user without compromise in the security as well as the leakage of information of the individual. To overcome these problems, we are proposing biometric authentication using Kerberos Protocol. It can successfully run over public network for remote access. It can also be implemented to take care of authentication between client and server.***

***Keywords— Authentication, Biometric, Cryptography, Kerberos protocol, and Key Distribution Centre***

## I. Introduction

During remote connection we face certain challenges when it comes to security. British biometric passports have hacked by Lucas Grunewald, a consultant with a German Security Company, and discovered a method for cloning the information stored in new passport as more governments, such as India and Germany, collect more biometric data on their citizens, the security of such information will continue to be an issue [12].We are concentrating our proposed work towards this issue. Biometric authentication systems are gaining wide-spread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms [1] that make the systems both secure and cost effective. They are ideally suited for both high security and remote authentication applications due to the non-repudiate in nature and user convenience.

Most biometric systems are assumed to be secure but there are chances of getting hacked. There are two places to be attacked: (i) one is on communication link and another (ii) on server's database. In order to protect from this type of attacks we propose this system. However a variety of applications of authentication need to work over partially secured or in-secured networks such as ATM networks or the Internet. Authentication over insecure public networks or with un-trusted servers raises more concern in privacy and security. The primary concern is related to the security of the plain biometric templates, which cannot be replaced, once they are compromised. The privacy concerns arise from the fact that the biometric samples reveal more information about its owner in addition to the identity.

The biometric authentication is being used for authenticating in most of the security required scenarios. If the biometrics used in plain, there are more chances for spoofing attacks by the imposters to gain illegal access to the server to get information about the client or to gain illegal access to the client to gain information about the server, which is not desirable. The network is not secure for the server as well as for the client. Hence this is a factor of motivation for any researcher to take up a research work on the enhancement of the security to address the problem.

Authentication is the most important aspect in human life from the security point of view. Most of the existing mechanisms use the reference template for the final authentication. These templates are stored in the raw format or some encrypted format. There is possibility of getting this information by imposter and can change the information which leads to the leakage of information. If the authentication is not being done then there is compromise in security. The problem here is to authenticate using the information of the user without compromise in the security as well as the leakage of information of the individual.

Widespread use of biometric authentication also raises concern of tracking a person, as every activity that requires authentication can be uniquely assigned to an individual. The primary concern is related to the security of the plain biometric templates, which cannot be replaced, once they are compromised [2]. The privacy concerns arise from the fact

 

that the biometric samples reveal more information about its owner in addition to the identity. Widespread use of biometric authentication also raises concerns of tracking a person, as every activity that requires authentication can be uniquely assigned to an individual

Kerberos is a network authentication protocol developed by the Massachusetts Institute of Technology (MIT). Kerberos is designed to provide strong authentication for client/server applications by using secret-key cryptography. From the user point of view, it does not differ much from a normal sign-on process. Kerberos still relies on the user providing some form of credentials to verify their identity. The exchange of credentials is encrypted throughout the entire authentication process, enabling a secure authentication mechanism. The major difference is that after an identity is proven, a temporary *ticket* is issued to the client. This ticket allows the user to access other systems and applications that exist within the circle of trust, or more correctly, the *Kerberos realm*(1). The Kerberos protocol uses a unique ticketing system that provides faster authentication also provides the following security services: Mutual authentication, delegated access control, privacy and data integrity.

## II. Driving The Existing Systems Literature Survey

The previous work in the area of encryption-based security of biometric templates tends to model the problem as that of building a classification system that separates the genuine and impostor samples in the encrypted domain[3][4]. However, a strong encryption mechanism destroys any pattern in the data, which adversely affects the accuracy of verification. Hence, any such matching mechanism necessarily makes a compromise between template security (strong encryption) and accuracy (retaining patterns in the data). The primary difference in our approach is that we are able to design the classifier in the plain feature space, which allows us to maintain the performance of the biometric itself, while carrying out the authentication on data with strong encryption, which provides high security/privacy[6].Over the years a number of attempts have been made to address the problem of template protection and privacy concerns and despite all efforts, as Jain et al. puts it, "a template protection scheme with provable security and acceptable recognition performance has thus far remained elusive". In this section, let us look at the existing work in light of this security-accuracy dilemma, and understand how this can be overcome by communication between the authenticating server and the client. The proposed method will adopt the classification of existing works provided by Jain et al.[5] and show that each class of approaches makes the security-accuracy compromise.

Let us now analyse each of the four categories of solutions i.e., salting, non invertible transform, key binding and key generation in terms of their strengths and weaknesses. The first class of feature transformation approaches known as Salting offers security using a transformation function seeded by a user specific key. The strength of the approach lies in the strength of the key. A classifier is then designed in the encrypted feature space. Although the standard cryptographic encryption such as AES or RSA offers secure transformation functions, they cannot be used in this case. The inherent property of dissimilarity between two instances of the biometric trait from the same person, leads to large differences in their encrypted versions. This leads to a restriction on the possible functions that can be used and in salting, resulting in a compromise made between security and the performance. Some of the popular salting-based approaches are biohashing and salting for face template protection. Moreover, salting-based solutions are usually specific to a biometric trait, and in general do not offer well-defined security. Kong et al. do a detailed analysis of the current biohashing-based biometric approaches. They conclude that the zero equal error rate (EER) reported by many papers is obtained in carefully set experimental conditions and unrealistic under assumptions from a practical view point. The second category of approaches identified as noninvertible transform applies a trait specific noninvertible function on the biometric template so as to secure it. The parameters of the transformation function are defined by a key which must be available at the time of authentication to transform the query feature set.

Some of the popular approaches that fall into this category are robust hashing and cancellable templates. Cancellable templates allows one to replace a leaked template, while reducing the amount of information revealed through the leak, thus addressing some of the privacy concerns. However, such methods are often biometric specific and do not make any guarantees on preservation of privacy, especially when the server is not trusted. Methods to detect tampering of the enrolled templates help in improving the security of the overall system. Boult et al.[7] extended the above approach to stronger encryption, and proposed an encrypted minutia representation and matching scheme of fingerprints. The position information of a minutia is divided into a stable integer part and a variable increment. A Biotoken consists of the encrypted integer part and the increment information in plain. A specific matching algorithm was proposed to match the biotokens for verification. The Boult approach provides provable template security as a strong encryption is used. Moreover, the matching is efficient, and is shown to even improve the matching accuracy. However, the primary fact that encryption is applied to part of the data, which itself is quantized, may mean some amount of compromise between security and accuracy. In this method, the computed biotoken is re-encoded using a series of unique new transformation functions to generate a Bipartite Biotoken. For every authentication, the server computes a new bipartite biotoken, which is to be matched by the client against the biotoken generated by him. The method significantly enhances the template security as compared to the original protocol. Moreover, as bipartite biotoken is different for each authentication request, replay attacks are not possible. However, in the current form, the base biotoken is available in plain with the server, and if the biotoken database is compromised, a hacker can gain access to all the users' accounts until the biotokens are replaced. The method aims at securing the actual biometric template, which cannot be recovered from a secure biotoken.

The third and fourth classes are both variations of Biometric cryptosystems. They try to integrate the advantages of both biometrics and cryptography to enhance the overall security and privacy of an authentication system. Such systems are primarily aimed at using the biometric as a protection for a secret key (key binding approach) or use the

 

biometric data to directly generate a secret key (key generation approach). The authentication is done using the key, which is unlocked/generated by the biometric. Such systems can operate in two modes in the case of remote authentication. In the first case, the key is unlocked/generated at the client end, which is sent to the server for authentication, which will ensure security of the template, and provide user privacy. However, this would become a key-based authentication scheme and would lose the primary advantage of biometric authentication, which is its nonrepudiable nature. In the second case, the plain biometric needs to be transmitted from the user to the server, both during enrollment and during authentication. This inherently leaks more information about the user than just the identity, and the users need to trust the server to maintain their privacy concerns. Moreover, authenticating over an insecure network makes the plain biometric vulnerable to spoofing attacks.

Biometric cryptosystem-based approaches such as fuzzy vault and fuzzy extractor in their true form lack diversity and revocability. According to Jain et al,[5] a performance degradation usually takes place as the matching is done using error correction schemes. This precludes the use of sophisticated matchers developed specifically for matching the original biometric template. Biometric cryptosystems, along with salting-based approaches introduce diversity and revocability in them. Moreover, Walter et al.[9] demonstrated a method for recovering the plain biometric from two or more independent secrets secured using the same biometric.

Nagai et al.[8] proposed the use of client side computation for part of the verification function. Their approach, termed ZeroBio, models the verification problem as classification of a biometric feature vector using a three-layer neural network. The client computes the outputs of the hidden layer, which is transferred to the server. The client then proves to the server that the computation was carried out correctly, using the method of zero-knowledge proofs. The server completes the authentication by computing the output values of the neural network. The method is both efficient and generic as it only requires computation of weighted sums and does not make any assumption on the biometric used. It also provides provable privacy to the user, as the original biometric is never revealed to the server. However, the system requires that the hidden layer weights be transferred to the server without encryption. This allows the server to estimate the weights at the hidden layer from multiple observations over authentications. Once the weights are known, the server can also compute the feature vector of the biometric, thus compromising both security and privacy. The system could also be compromised if an attacker gains access to the client computer, where the weight information is available in plain.

**Drawbacks of existing systems**

1. The plain biometric can be easily accessed by the imposter.
2. The plain biometric is sent to the server for both enrolment and for authentication, there is a much chance for the leakage of information.
3. If the user-specific key is compromised, the template is no longer secure imposter can recover the original biometric template using specific key.
4. The network is insecure in the sense that the intruder is in the network then he can gain access to the server as well as to the client.

## III. Proposed System

We are proposing Kerberos as a Biometrics authentication protocol. There is a unique way of solving problem of biometrics authentication. The encryption and biometrics with the registration server, authentication server and the token granting server makes this technique unique. We will target on strong cryptography for user's original data with the registration server, obviously the authentication should be non-reputable and also the user side attacks and the replay attacks should be taken care of, also in the cases where say the key is compromised. The high performance needed by this level of crypto-biometric system is solved by the token granting system of Kerberos.

Kerberos has been successful as an authentication protocol. What we wish to do is make it more secure by integrating it with a crypto biometric authentication system in place of the password system that Kerberos implements. The user's actual biometric data is also not available with the authenticating server. It's only submitted to the registration server. The encryption and biometrics with the registration server, authentication server and the token granting server makes this technique unique. It can guard against almost all kind of possible threats in the scenario. We take care of a) Biometric template security b) privacy of the user c) trust between user and authenticating server and d) network security related issues [5]. The proposed system follow task into three steps 1) Registration 2) Authentication 3) Ticket Granting. We will target on strong cryptography for user's original data with the registration server, obviously the authentication should be non-reputable and also the user side attacks and the replay attacks should be taken care of, also in the cases where say the key is compromised. In the proposed method we look towards the design of a classifier that also helps us to improve the performance of biometrics and we use the randomization scheme for this purpose.

**The advent of proposed systems**

1. The authentication is done using the encrypted data set. Hence no identity of the client or the server is revealed to each other.
2. The computations are carried out in the randomized Manner .Hence no imposter can gain the biometric of the client in plain.
3. It provides provable protection against replay and client-side attacks

## *IV* ARCHITECTURAL FOCUS

The overall authentication procedure as explained is divided into the following three major steps in fig 2 shown below i.e., registration, authentication and ticket granting. A remote client first registers himself, i.e., enrolls himself with the

 

first server. Then it authenticates himself with authentication server proceeding further with the tickets and session keys.

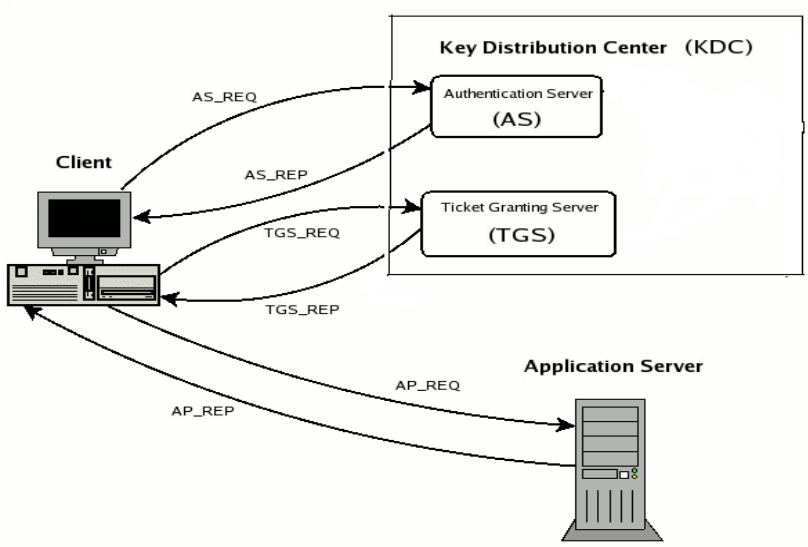


Fig 1: working principal of Kerberos protocol

**A) Registration Server :**

This is the basic step of registering the user with the main registration server that has the templates of biometrics provided by all users. The registration server is trusted server here. We are here assuming that this third party server i.e., the registration server is already safe enough for us. K is the public key of Alice that it tells the server. During the registration, the client/ Alice sends samples of her biometric data to the registration server, which generates the classifier for Alice. The Biometric sample from Alice to registration server was digitally marked by the client and encrypted using the public key of the server to protect it hence making it secure. Finally what we send to the authentication server is the Alice's identity, her public key, the encrypted parameters and the threshold value.

**B) Authentication Server:**

Now we need to compute a value w, x that requires multiplication. We can consider simple scalar multiplication and then addition of the values obtained. Over here we are calculating x based on the vector values $y_i$ that we may obtain from the biometrics. For the sake of simplicity we convert this vector to a finite quantity and single x rather than dealing with I values of a single vector derived from the biometric. x can be the mean of the vectors or note that we are using RSA in this method, we know that it follows homomorphism for multiplication[6].

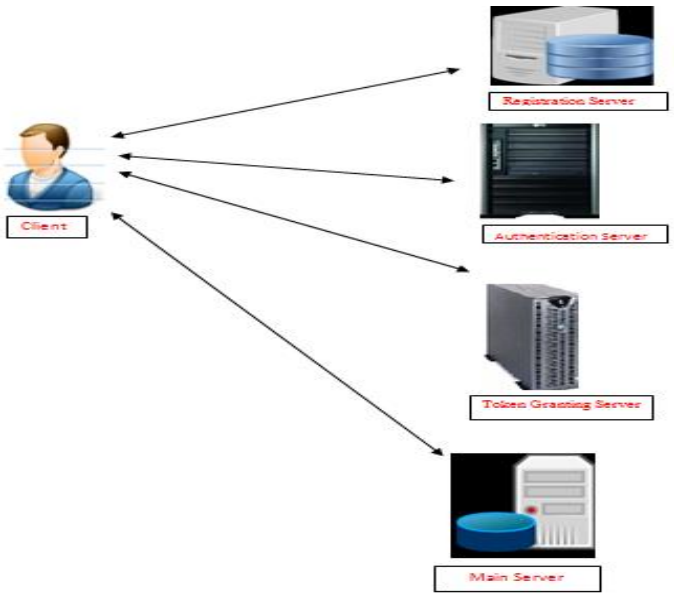


Fig 2: Architectural overview

Hence we can compute K (w x)=K(w)K(x) at the server side because of this property of homomorphism that RSA follows. Though we cannot add the results to compute the authentication function making it safe. Sending the product answers to Alice to do the addition actually reveals the classifier parameters to the Alice, which obviously we do not want. We are using a randomization technique for this purpose. We generate the parameter $r_i$ by such randomization. It makes sure that the Alice can do the summation computing while it is not able to decipher any information from the product that she can get hands on. The randomization is done in a way such that the server can compute the final sum to

 

be compared with the value of threshold that was decided earlier. The server here carries out all of its computation in the encrypted domain, and hence does not get any information about the biometric data(x) or classifier parameter (w). No one can guess our classifier parameter from the products as they are randomized when multiplied with $r_j$. The server is able to compute the final sum S because of the imposed condition on $r_j$ and tjS.

**C) Token Granting :**

1. Now TG server sends two tickets containing
2. $K_s$ (Bob, $K_{AB}$) and $K_b$( Alice, $K_{AB}$)
3. Alice sends Bob's ticket timestamp encrypted by $K_{AB}$ i.e., $K_{AB}$( T) and $K_B$( Alice , $K_{AB}$) it received from TG.
4. Bob confirms with Alice by a response such as K AB (T+1) and confirms the success in ticket granting. Hence once this ticket is granted no need to authenticate again and again and we can thus increase the performance of the biometrics.

**D) Minutiae extraction from finger print:**

Step 1: plain finger print image has been taken.
Step 2: It has to be subjected to pre-processing unit
- 2.1. Image size has been altered to323x352 pixels.
- 2.2. Clarity of image has been maintained.
- 2.3. Image has been converted to bit map format.

Step 3: core of the finger print has been identified.
- 3.1Cut of 50,50, 50,50,pixels in the four sides.
- 3.2 Find centre point which is having 270 degree or more curvature angle
- 3.3. Note the X&Y co-ordinate values.

Step 4: Chain link algorithm is used to give continuity if Image contains some impurities.
Step 5: Hit and miss algorithm is used to give width stroke in One pixel.
Step 4: calculate ridge ending, bifurcation, and island distances from core and store X&Y co-ordinate values of each.

## IV. Conclusion

Authentication is critical for the security of computer systems. Without knowledge of the identity of a principal requesting an operation, it is difficult to decide whether the operation should be allowed. Traditional authentication methods are not suitable for use in computer networks where attackers monitor network traffic to intercept passwords. The use of strong authentication methods that do not disclose biometric data is imperative. The Kerberos authentication system is well suited for authentication of users in such environments.

If we talk about the unprotected environment, any Client can apply to any server for service. This has a Security risk of impersonation. An opponent can pretend to be another client and obtain unauthorized privileges on server machines. In the above scheme the transaction will be highly secured in the sense that Authentication server creates a ticket which is further encrypted using the Asymmetric key shared by the server and authentication Server. This ticket then sends back to client. Because the ticket is encrypted, it cannot be altered by client or by an opponent. The primary advantage of the proposed approach is that we are able to achieve classification of a strongly encrypted the proposed work is extremely secure under a variety of attacks and it can be used in various biometric traits.

**ACKNOWLEDGMENT**

First of all I would like to express my heartfelt thanks to **Asst. prof**. **Suresha D** for their highly appreciable encouragement and support. Their guidance has been the constant driving force behind my preparation to this Paper. I would also like to thank my lecturers who have been instrumental in inspiring and motivating me with all career guidelines. I am grateful to all the suggestions and hints they have provided with respect to project. Finally, I would thank all my friends who have helped me in collecting the related materials and who have been responsible for improving the quality of this paper by discussing and providing me with the extra information related to the paper. I'm glad to admit that the paper has been a great learning experience and I would certainly look forward to future opportunities like this.

**REFERENCES :**

[1] A.K. Jain , A. Ross and S. Prabhakr " An introduction to Biometric recognition", IEEE trans. Circuit systems , Video Technol., Vol 14, nol,pp 4-20,jan2004
[2]Lawrence O' Gorman, Avaya Labs, Basking Ridge " Comparing Passwords, Tokens, and Biometrics for User Authentication" Proceedings of the IEEE, Vol. 91, No 12,Dec 2003
[3] N.K. Ratha , J.H Connell and R.M Bolle, "enhancing security and privacy in biometric based authentication systems", IBM syst. J. ,vol 40, no.3, pp.614-634,mar 2001.
[4] Upmanyu, M.; Namboodiri, A.M.; Srinanthan, K.; Jawahar, C.V. "Blind Authentication: A Secure Crypto Biometric Verification Protocol" ;; Information Forensic s and Security, IEEE Transactions on. Vol 2. Issue 2, June 2010:pp 255
[5] R. Rivest, A. Shamir, and L. Adelman, " A method for obtaining digital signatures and public key cryptosystems", Commun ACM, Vol 21, no 2 , pp. 120-126, 1978.
[6] B. Clifford Neuman and Theodore Ts'o. " Kerberos: An Authentication Service for Computer Netwotks", IEEE Communications Magazine, Volume 32, Number 9, pages 33-38, September 1994..
[7] S.P. Miller, C. Neuman., J.I.Schiller, " Kerberos authentication System" Project Athena Technical

 

[8] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP*, vol. 8, no. 2, pp. 1–17, 2008.
[9] Prof R.P. Arora, Garima Verma, ―Implementation of Authentication and Transaction Security based on Kerberos‖, IJITCE, Feb 2011
[10] Dr. S. Santhosh Baboo, K. Gokulraj, ―A Secure Dynamic Authentication Scheme for Smart Card based Networks‖, International Journal of Computer Applications, Number 8- Article 2, pp. 1605-2157, 2010
[11] K. Aruna et. al (2010), ―A new collaborative trust enhanced security model for distributed systems‖. International Journal of Computer Application, No-26
[12] Hongjun liu et. al(2008), ―A distributed expansible authentication model based on Kerberos‖ Journal of Network and Computer Application, Vol.31, Issue 4
[13] Dr.Mohammad N. Abdullah & May T. Abdul-Hadi, ―A Secure Mobile Banking Using Kerberos Protocol‖, Engg & Technology Journal, Vol 27, No 6, 2009.
[14] MIT Kerberos Website, http://web.mit.edu/kerberos/www.
[15] William Stallings, ―Cryptography and Network Security‖, Third Edition.

**AUTHORS PROFILE**

Shashidhar M S was born in 1986. He received Bachelor's Degree in computer Science and engineering and pursuing Master's degree in CSE from Canara engineering college, Mangalore. He is pursuing his Master's thesis under supervision of my M. Tech guide Asst. Prof. Suresha D.

Suresha D was born in 1980. He received Bachelor's Degree in Computer Science and engineering and received Master's degree in Computer Networks. He is currently working as Assistant Professor in the Department of Computer Science and engineering in Canara Engineering College Mangalore. He has published research papers in International Journals and presented his work at conferences

 