BIOMETRICS AUTHENTICATION TECHNIQUE WITH KERBEROS FOR EMAIL LOGIN

Rashmi Hegde
Department of ISE, National Institute of Engineering, Mysore, India

ABSTRACT:
Advances in the field of Information Technology make Information Security an inseparable part of it. In today's world, Electronic mail or e-mail is the one that is most prone to intrusions like phishing which acquires sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. In order to deal with security, authentication like biometrics plays an important role. Biometrics technology is simply the measurement and use of the unique characteristics of living humans to distinguish them from one another to ensure that the rendered services are accessed only by a legitimate user and it is more useful as compared to passwords as they can be lost or stolen. In this paper, a method which is based on biometric recognition which would avoid any intrusion possible to the email is proposed.

KEYWORDS: *Email, biometric, Kerberos, phishing, authentication.*

I. INTRODUCTION

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security.

Biometric authentication has grown in popularity as a way to provide personal identification. Person's identification is crucially significant in many application and the hike in email hacking and identity theft in recent years indicate that this is an issue of major concern in wider society. Individual passwords, pin identification arrangement all have deficiencies that restrict their applicability in a widely-networked society. Biometric is used to identify the identity of an input sample when compared to a template, used in cases to identify specific people by certain characteristics. The advantage claimed by biometric authentication is that they can establish an unbreakable one-to-one correspondence between an individual and a piece of data.

A cryptographic protocol is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective. The whole point of using cryptography in a protocol is to detect or prevent attacks.

Electronic mail, most commonly referred to as email or e-mail since 1993,is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks.

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details

at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Email spoofing is the creation of email messages with a forged sender address - something which is simple to do because the core protocols do no authentication. Spam and phishing emails typically use such spoofing to mislead the recipient about the origin of the message.

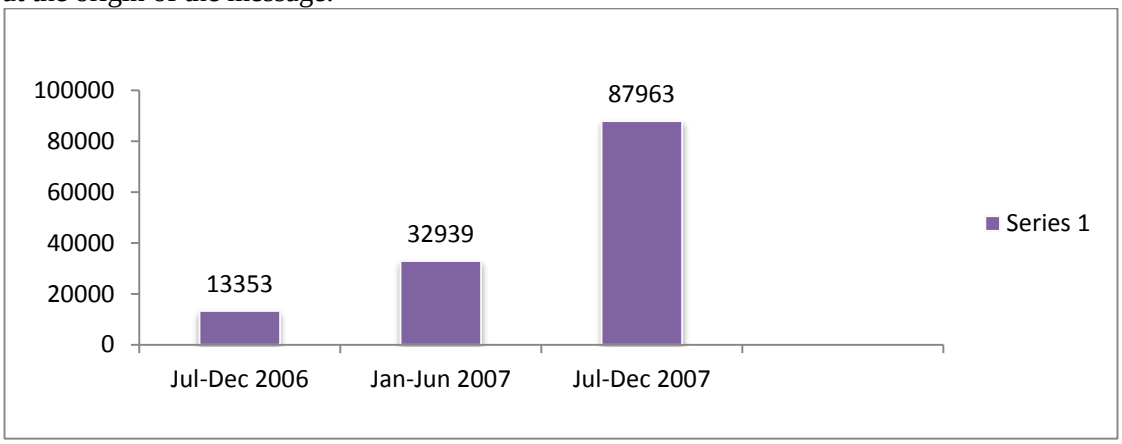

Fig 1: Rise in the number of phishing hosts

It is important to note that more than five million E-mails are identified as "verified and valid" phished E-mails almost everyday. Fig.1 shows the rise in the number of phishing hosts.[6]

Today, more common in computer network architecture is a distributed architecture consisting of dedicated user workstations (clients) and distributed or centralized servers. In this environment, network connections to other machines are supported. Thus, there is a need to protect user information and resources housed at the server. The authentication service in these environments can be achieved by using Kerberos. It is one of the most widely used authentication protocols. It addresses an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. Kerberos employs one or more Kerberos servers (the KDC: Kerberos Distribution Center) to provide an authentication service. Kerberos requires the user to prove his or her identity for each service invoked. It also requires that servers prove their identity to clients. The overall scheme of Kerberos is that of a trusted third party that uses a protocol based on that proposed by Needham and Schroeder . It is trusted in the sense that clients and servers trust Kerberos to mediate their mutual authentication. Assuming the Kerberos protocol is well designed, then the authentication service is secure if the Kerberos server itself is secure. Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.

The information and analysis of a report based on on-going primary research conducted by The Radicati Group, Inc. consists of information collected from a variety of surveys, carried out on an on-going basis. Secondary research sources have also been used, where appropriate, to cross-check the information collected. These include company annual reports and market size information from various market segments of the computer industry. Table 1 shows the statistics of email.

Typical corporate email user sends and receives about 105 email messages per day. Despite spam filters, roughly 19% of email messages that are delivered to a corporate email user's inbox are spam. [6]

Table 1 : Statistics of Email

Business Email	2011	2012	2013	2014	2015
Average Number of Emails Sent/Received Per User/Day	105	110	115	120	125
Average Number of Emails Received	72	75	78	81	84
Average Number of Legitimate Emails	*58*	*62*	*65*	*68*	*71*
*Average Number of Spam Emails**	*14*	*13*	*13*	*13*	*13*
Average Number of Emails Sent	33	35	37	39	41

Corporate Email Sent and Received Per User Per Day, 2011-2015

In this paper, a detail description on Biometric Authentication, Kerberos and how these can be implemented to provide higher security is presented. The organization is as follows: Related works to the topic are mentioned in section 2. Detail, techniques and technologies that are used is described in section 3. Then, there is a brief overview of the proposed system in section 4. After that, feasibility study is seen in section 5. While in section 6, system features will be discussed. Finally, we will summarize the conclusions and the future work in section 7.

II. RELATED WORK

Massachusetts Institute of Technology (MIT) developed Kerberos to protect network services provided by Project Athena. Several versions of the protocol exist; versions 1–3 occurred only internally at MIT. Many members of Project Athena contributed to the design and implementation of Kerberos [7].Security of Kerberos has been analyzed in many works, e.g. [8], [9], [10], [11], [12], [13] and [14]. Most commonly analyses identify certain limitations of Kerberos and sometimes propose fixes. This leads to the evolution of the protocol when a new version patches the known vulnerabilities of the previous versions. The current version Kerberos V5 is already being revised and extended [15], and [16]. A. Boldyreva and V. Kumar at 2007 take a close look at Kerberos' encryption and confirm that most of the options in the current version provably provide privacy and authenticity [17]. Kerberos is also used in wireless applications. M. Erdem proposed a high speed 2G wireless authentication systems based on kerberos [18]. He used DES, 3DES and AES as secret-key crypto algorithms. He also used SHA-1 message digest algorithm to hash the message blocks. Besides, A. Pirzada and Chris McDonald discuss how kerberos is used for authentication in mobile ad-hoc networks [19]. Kerberos is also introduced to be used in IPv6 networks. S.Sakane, N. Okabey, K. Kamadaz, and H. Esakix describe a method to establish secure communication using Kerberos in IPv6 networks [20]. Hussein Khalid Abd-alrazzq, Mohammad S. Ibrahim and Omar Abdulrahman Dawood describe Secure Internet Voting System based on Public Key Kerberos[21]. Sanjay Kumar, Manpreet Singh show a secure electronic voting system using fingerprint technique[22]. Development of a Student Attendance Management System Using RFID and Face Recognition was proposed by Unnati A. Patel and Dr. Swamynarayan Priya [23].

III. DETAIL, TECHNIQUES AND TECHNOLOGIES

3.1 BIOMETRICS

There exist two kind of biometric characteristics. So, techniques for biometric authentication have been developed based on these characteristics. Details of different techniques are discussed below.

3.1.1 Techniques

A. Finger Print Technology

A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal ". The traditional method uses the ink to get the finger print onto a piece of paper. This piece of paper is then scanned using a traditional scanner. Now in modern approach, live finger print readers are used .These are based on optical, thermal, silicon or ultrasonic principles. It is the oldest of all the biometric techniques. Optical finger print reader is the most common at present. They are based on reflection changes at the spots where finger papilar lines touch the reader surface. All the optical fingerprint readers comprise of the source of light, the light sensor and a special reflection surface that changes the reflection according to the pressure. Some of the readers are fitted out with the processing and memory chips as well.[3]

The size of optical finger is around 10*10*15. It is difficult to minimize them much more as the reader has to comprise the source on light reflection surface and light sensor. The finger print obtained from an Optical Fingerprint Reader is shown in figure 2.

Figure 2. Fingerprint Bitmap.

Optical Silicon Fingerprint Sensor is based on the capacitance of finger. Dc-capacitive finger print sensor consists of rectangular arrays of capacitors on a silicon chip. One plate of the capacitors is finger, other plate contains a tiny area of metallization on the chips surfaces on placing finger against the surfaces of a chip, the ridges of finger print are close to the nearby pixels and have high capacitance to them. The valleys are more distant from the pixels nearest them and therefore have lower capacitance. Ultrasound finger print is newest and least common. They use ultrasound to monitor the figure surfaces, the user places the finger on a piece of glass and the ultrasonic sensor move and reads whole finger print. This process takes 1 or 2 seconds. Finger print matching techniques can be placed into two categories. One of them is Minutiae based and the other one is Correlation based. Minutiae based techniques find the minutiae points first and then map their relation placement on the finger. Correlation based techniques require the precise location of a registration point and are affected by image translation and rotation.

B. face recognition technology

A facial recognition technique is an application of computer for automatically identifying or verifying a person from a digital image or a video frame from a video source. It is the most natural means of biometric identification. Facial recognition technologies have recently developed into two areas and they are Facial metric and Eigen faces. Facial metric technology relies on the manufacture of the specific facial features (the system usually look for the positioning of eyes, nose and mouth and distances between these features), shown in figure 3 and 4.[2][3]

Figure 3. Recognition of face from Body.

The face region is rescaled to a fixed pre-defined size (e.g. 150-100 points). This normalized face image is called the canonical image.

Then the facial metrics are computed and stored in a face template. The typical size of such a template is between 3 and 5 KB, but there exist systems with the size of the template as small as 96 bytes. The figure for the normalized face is given below.

Figure 4. Normalized Face.

The Eigen Face method (figure 5) is based on categorizing faces according to the degree of it with a fixed set of 100 to 150 eigen faces. The eigen faces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern shows how different features of a face are singled out. It has to be evaluated and scored. There will be a pattern to evaluate symmetry, if there is any style of facial hair, where the hairline is, or evaluate the size of the nose or mouth.

Figure 5. Eigen Face.

Other eigen faces have patterns that are less simple to identify, and the image of the eigen face may look very little like a face. This technique is in fact similar to the police method of creating a portrait, but the image processing is automated and based on a real picture. Every face is assigned a degree of fit to each of 150 eigen faces, only the 40 template eigen faces with the highest degree of fit are necessary to reconstruct the face with the accuracy of 99 percent. The whole thing is done using Face Recognition softwares.

C. iris technology

This recognition method uses the iris of the eye which is colored area that surrounds the pupil. Iris patterns are unique and are obtained through video based image acquisition system. Each iris structure is featuring a complex pattern.

This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings. The iris pattern is taken by a special gray scale camera in the distance of 10- 40 cm of camera. Once the gray scale image of the eye is obtained then the software tries to locate the iris within the image. If an iris is found then the software creates a net of curves covering the iris. Based on the darkness of the points along the lines the software creates the iris code. An IRIS Image shown in figure 6.

Figure 6. Image of IRIS.

Here, two influences have to take into account. First, the overall darkness of image is influenced by the lighting condition so the darkness threshold used to decide whether a given point is dark or bright cannot be static, it must be dynamically computed according to the overall picture darkness. Secondly, the size of the iris changes as the size of the pupil changes. Before computing the iris code, a proper transformation must be done.

In decision process, the matching software takes two iris codes and compute the hamming distance based on the number of different bits. The hamming distances score (within the range 0 means the same iris codes), which is then compared with the security threshold to make the final decision. Computing the hamming distance of two iris codes is very fast (it is the fact only counting the number of bits in the exclusive OR of two iris codes). We can also implement the concept of template matching in this technique. In template matching, some statistical calculation is done between a stored iris template and a produced. Depending on the result decision is taken.[2][3]

3.1.2. Evaluation

When it is time to use the biometric authentication, the degree of security is concerned. In this paper, the various types of biometric authentication techniques is discussed. In this section, we will evaluate different techniques and find degree of security.
There are various parameters with the help of which we can measure the performance of any biometric authentication techniques. These factors are described below.
Table 2 shows the evaluated vales of various evaluation techniques.[3]

IV. FACTORS OF EVALUATION

- **False Accept Rate (FAR) and False Match Rate (MAR):** The probability that the system incorrectly declares a successful match between the input pattern and a nonmatching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.
- **False Reject Rate (FRR) or False Non-Match Rate (FNMR):** The probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percent of valid inputs being rejected.
- **Equal Error Rate (EER):** The rates at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly. When quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

V. RESULTS OF EVALUATION

The evaluations of various techniques using the above parameters are presented in a tabular format in table 2.[3]

Table 2. Evaluation of Biometric Techniques

Biometric	EER	FAR	FRR	Subjects	Comments
Fingerprint	2%	2%	2%	25000	rotation and exaggerated skin distortion
Face	NA	1%	10%	37437	varied light, indoor /outdoor
Iris	.01%	.94%	.99%	1224	Indoor environment

- **Finger Print Technology:** The finger print bit map obtained from the reader is affected by the finger moisture as the moisture significantly influences the capacitance .This means that too wet or dry fingers do no produce bitmaps with sufficient quality and so people with unusually wet or dry figures have problems with these silicon figure print readers.
- **Face Recognition Technology:** The accuracy of face recognition systems improves with time, but it has not been very satisfying so far. There is need to improve the algorithm for face location.. The current software often doesn't find the face at all or finds "a face" at an incorrect place .This makes result worse. The systems also have problems to distinguish very similar person like twins and any significant change in hair or beard style requires re – enrollment .glasses also causes additional difficulties .It doesn't require any contact with person and cab be fooled with a picture if no countermeasures are active The liveness detection is based most commonly on facial mimics. The user is asked to blink or smile .If the image changes properly then the person is considered "live".
- **Iris Technology:** The artificial duplication of the iris is virtually impossible because of unique properties .The iris is closely connected to the human brain and it is said to be one of the first parts of the body to decay after the death. It should be therefore very difficult to create an artificial iris to fraudulently bypass the biometric systems if the detection of the iris liveness is working properly.

3.2 Kerberos

3.2.1 Purpose

The main objective in the proposed technique is to have the highest impact, and acceptance among average applications. Hence, a kerberos frame work which can be easily integrated into any client server application is being proposed. For wider acceptance the simple and user friendly user interface is being made.

The proposed technique will work with any average application using encrypted ticket based communication without compromising on security.

3.2.2 Architecture

Fig. 7 shows the architecture of the Kerberos protocol.[4]

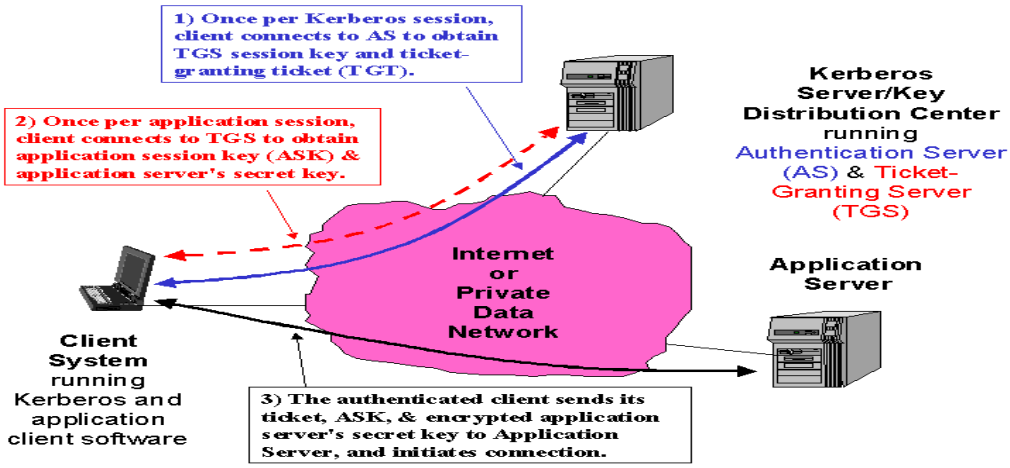

Fig. 7 Architecture of kerberos protocol

3.2.3 Mathematical model[1][5]

Problem statement: To build an application helps user to have secure authentication by using ticket based communication.

Problem description:

Let S1 be the set of user/controller in our system.
S1= { C , AS , TGS , V}
C = Client
AS = Authentication Server
TGS = Ticket Granting Server
V = Server on which we want to access the service

Let S2 be the set of objects in our system.

S2 = { IDc , IDTGS , TS , KC , KV , lifetime , ADC , TicketTGS , TicketV }
IDC = ID of client
IDTGS = ID of Ticket Granting Server
KC = Key of client
KV = Key of Server
AD = Address

TicketTGS = E(KTGS [KTGS || IDC || ADC || IDTGS || TS2 || lifetime])
TicketV = E(KV [KC.V || IDC || ADC || IDV || TS4 || lifetime])
Authenticator = E(KC,TGS [IDC || ADC || TS])

Working:

There are three stages in our problem solving.

A] Authentication service exchange to obtain Ticket Granting Ticket (TicketTGS)
1. C -> AS : IDC || IDTGS || TS1
2. AS -> C : E(KC[KC,TGS || DTGS || TS2 || lifetime || TicketTGS])
In the above stage client request AS for Ticket(access) to TGS Server.
AS checks client authenticity and sends TicketTGS to Client.

B] Ticket granting service exchange to obtain server granting Ticket(TicketV)
3. C -> TGS : IDV || TicketTGS || Authenticator C
4. TGS -> C : E(Kc,TGS [KC,v || IDV || TS4 || TicketV])
In the above stage client sends the ID and TicketTGS to TGS to authenticate itself.
The TGS replies with a TicketV (Ticket to Server).

C] Client|Server Authentication Exchange to obtain service
5. C -> V : TicketV || Authenticator
6. V -> C : E (KC,V [TS5+1]) For mutual authentication
In the above stage client sends TicketV to server to authenticate and access service.
Thus we see from above solution that in our problem solving there are no unknown stages or unpredictable branching. Thus we can conclude that the problem is a P(Polynomial Time) Problem as it is deterministic in solving.

VI. PROPOSED SYSTEM

When the user likes to login to his email account, he has to prove this authenticity through the biometric system. The password in the form of biometric, for example fingerprint, is unique and is stored in the client while registration. Through this, the user ID and unique password (biometric factor) is known to the client module. The client module C in the user's workstation requests the user's authenticity and then sends a message to the AS. The AS checks its database to see if the user has supplied the proper password for this user ID and whether this user is permitted access to server V. If both tests are passed, the AS accepts the user as authentic and must now convince the server that this user is authentic. To do so, the AS creates a ticket that contains the user's ID and network address and the server's ID. This ticket is encrypted using the secret key shared by the AS and this server. This ticket is then sent back to C. Because the ticket is encrypted, it cannot be altered by C or by an opponent.
With this ticket, C can now apply to V for service. C sends a message to V containing C's ID and the ticket. V decrypts the ticket and verifies that the user ID in the ticket is the same as the unencrypted user ID in the message. If these two match, the server considers the user authenticated and grants the requested service.
The ticket is encrypted to prevent alteration or forgery. The server's ID (*IDV*) is included in the ticket so that the server can verify that it has decrypted the ticket properly. *IDC* is included in the ticket to indicate that this ticket has been issued on behalf of C. Finally, *ADC* serves to counter the following threat. An opponent could capture the ticket transmitted in message , then use the name and transmit a message from another workstation. The server would receive a valid ticket that matches the user ID and grant access to the user on that other workstation. To prevent this attack, the AS includes in the ticket the network address from which the original request came.
Now the ticket is valid only if it is transmitted from the same workstation that initially requested the ticket.

VII. FEASIBILITY STUDY

Feasibility study is performed to determine the possibility or probability of either improving the existing system or developing a completely new system. Following are the feasibilities, which are considered for the development of the application:

● Operational Feasibility: It means to estimate whether it is required to the train the user to handle the system. In this case there is only training of interaction with user interface. Since the users are computer literate it would not to be difficult to adapt to new system.
● Technical Feasibility: Technical feasibility is to estimate whether it is possible to develop the proposed system with the available hardware and software and network resources. Since all proposed hardware, software and network requirements are easily available; the development of the application is feasible.
We can prove that our system is P-Complete because in our system the most complex module is kerberos module but it is implemented in polynomial time. So our can be considered as P-Complete.
From above mathematical model we can see that in our problem solving there is no unknown stages or unpredictable branching. Thus we can conclude that the problem is a P(Polynomial Time) Problem as it is deterministic in solving.

VIII. SYSTEM FEATURES

A. Functional Requirements
● **Client:** Client sends Client id and Server id over the network to Kerberos for authentication.
● **Remote Computer: -** The Remote Computer will consist of Web browser that will contain log-in interface.
● **Biometric system: -** The hardware installed on host to scan the biometric factors.
● **Kerberos**: - Kerberos consist of AS and TGS.AS receives request from client, it verifies and sends TGS address back to client along with TGT specifications. TGS than receives request from client for server access .TGS verifies and sends back Session specifications to client and server.
● **Server**: -Server receives access to service from client along with Session specifications. Server verifies Session information and gives service to client
B. Non-functional Requirements
● Secure access of confidential data (user's details). SSL can be used.
● 24 X 7 availability.
● Better component design to get better performance at peak time.
● Flexible service based architecture will be highly desirable for future extension
● Ease of Use- Few clicks, intuitive, flexibility, performance and installing/download.
● Security- Privacy, Confidentiality, Integrity, Authentication, Verification/Non-repudiation.
● Technical Acceptability- Integration Effort, Interoperability, Scalability, Remote Access, Performance.

IX. CONCLUSION AND FUTURE WORK

While biometric authentication can offer a high degree of security, they are far from perfect solution. Sound principles of system engineering are still required to ensure a high level of security rather than the assurance of security coming simply from the inclusion of biometrics in some form.
In this paper an authentication framework, considering the security issues over the network during authentication process is proposed. The proposed protocol framework not only satisfies the need of authentication that is generally required in the protocol, it also provides the better security as the trusted third party is involved. This method which is based on biometric recognition and Kerberos would avoid any intrusion like phishing possible to the email.
As a future work, this method can be used for many social sites to prevent intrusion from happening. The algorithms can be changed according to the network needs in the future. The framework is secure and scalable. Kerberos is currently available for the various operating systems, databases, and other vendored applications. Kerberos will be seen to support mobile devices in future.

ACKNOWLEDGEMENT

I am greatly thankful to my family and friends for the continuous support that has provided a healthy environment to drive me to do this project.

REFERENCES

[1]. William Stallings(2007),"Cryptography And Network Security ". Edition 5,Pearson publications.
[2]. Smita S. Mudholkar , Pradnya M. Shende , Milind V. Sarode , "Biometrics Authentication Technique" , International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012
[3]. Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A, and Minkyu Choi, "Biometric Authentication: A Review**",** International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009
[4]. Sanket Bhat , " KERBEROS: An Authentication Protocol*",* International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 2, February 2014
[5]. Eman El-Emam**, "**A Network Authentication Protocol Based on Kerberos **",** IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009
[6]. Nina Godbole & Sunit belpure , *Cyber Security*, Wiley Publishers
[7]. C. Neuman and Ts'o. Theodore, "Kerberos: An Authentication Service for Computer Networks". IEEE Communications Magazine. September 1994.
[8]. S. Bellovin & M. Merrit, "Limitations of the Kerberos Authentication System," SIGCOMM Comput. Commun. Rev., 20(5):119–132, 1990.
[9]. G. Bella and E. Riccobene, "Formal analysis of the Kerberos authentication system". Journal of Universal Computer Science, 3(12):1337–1381, 1997.
[10]. G. Bella and L. Paulson, "Kerberos version IV: Inductive analysis of the secrecy goals". In ESORICS '98. Springer, 1998.
[11]. J. Kohl, "The use of encryption in Kerberos for network authentication". In CRYPTO '89. Springer, 1989.
[12]. S. Stubblebine and V. Gligor. "On message integrity in cryptographic protocols". In Symposium on Security and Privacy '92. IEEE, 1992.
[13]. T. D. Wu. "A real-world analysis of Kerberos password security". In NDSS '99. The Internet Society, 1999.
[14]. T. Yu et al. "The perils of unauthenticated encryption: Kerberos version 4". In NDSS '04. The Internet Society, 2004.
[15]. K. Raeburn. "Encryption and Checksum Specifications for Kerberos 5". Network Working Group. Request for Comments: 3961. Available at http://www.ietf.org/rfc/rfc3961.txt, 2005.
[16]. K. Raeburn. "Advanced encryption standard (AES) encryption for Kerberos 5". Network Working Group. Request for Comments: 3962. Available at http://www.ietf.org/rfc/rfc3962.txt, 2005.
[17]. A. Boldyreva and V. Kumar, "Provable-Security Analysis of Authenticated Encryption in Kerberos". IEEE Symposium on Security and Privacy (SP'07). May 2007.
[18]. M. Erdem, "High-speed ECC based Kerberos authentication protocol for wireless applications". Global Telecommunications Conference. GLOBECOM. IEEE Volume 3, (Dec 2003).
[19]. A. Pirzada and C. McDonald. "Kerberos Assisted Authentication in Mobile Ad-hoc Networks". The 27th Australasian Computer Science Conference, conferences in Research and Practice in Information Technology. 2004.
[20]. S. Sakane et al. "Applying Kerberos to the Communication Environment for Information Appliances", Symposium on Applications and the Internet Workshops (IEEE SAINT-w'03), 2003.
[21]. Hussein Khalid Abd-alrazzq, Mohammad S. Ibrahim and Omar Abdulrahman Dawood, "Secure Internet Voting System based on Public Key Kerberos", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.
[22]. Sanjay Kumar, Manpreet Singh, "design a secure electronic voting system using fingerprint technique", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013
[23]. Unnati A. Patel and Dr. Swamynarayan Priya, "Development of a Student Attendance Management System Using RFID and Face Recognition", IJARCSMS, Volume 2, Issue 8, August 2014

AUTHOR

Rashmi Hegde was born in Mysore, India (1993). She obtained B.E. in 2014. She is presently a student of M.Tech at National Institute of Engineering, Mysore in Computer Network Engineering.