COMPARATIVE ANALYSIS OF AUTHENTICATION AND AUTHORIZATION SECURITY IN DISTRIBUTED SYSTEM

Halima Akhter[1], Md. Ansarul Haque[2]

[1]*Computer Science and Engineering, Stamford University, Dhaka, Bangladesh*
[2]*Lecturer, Computer Science and Engineering, Stamford University, Dhaka, Bangladesh*

Abstract

In this paper different types of processes of authentication and authorization analyzed individually in a comparative way. Some time it may be seen that one process is complementary with another process so comparative analysis can detect why they are complement. Bringing a best output such as low cost, saving time, high confidentiality, adaptability etc are the results of this paper. This thesis has concluded with some recommendations that several security processes of authentication and authorization might be suitable for some in distributed system to replace the wired processes.

Keywords: *Authentication security, Authorization security, Access control, Security in distributed system.*

---***---

1. INTRODUCTION

1.1 Motivation

Distributed system is one of the modern communication technologies, which means resource sharing, openness, concurrency, scalability; transparency. The question of securities arises when some people do some unwanted job like modifying any message or source for their own motive. Especially in some large business company less of securities can be a big trouble. Now-a-days organizations are conscious about maintaining security not only in physical environment but also in virtual environment .The importance of security in distributed system is so high. The significant question of this paper is how to protect security of a distributed system. Here, come up the important point authentication and authorization processes in a distributed system. There are so many processes for authentication and authorization. In these paper different types of processes of authentication and authorization about distributed system has been analyzed individually in a comparative way. Some time it may be seen that one process is complementary with another process so comparative analysis can detect why they are complement to each other. Using a process which is chosen comparatively can bring a best output in the system. For bringing the best output such as low cost, saving time, high confidentiality, adaptability etc are the results of this paper. In a brief, comparable studies have been done among the security processes of authentication and authorization to secure the distributed system. The thesis has concluded with some recommendations that several security processes of authentication and authorization might be suitable for some in distributed system to replace the wired processes.

1.2 Research Questions

The research question of this thesis is which methods should be chosen for authentication and authorization in a distributed system.

1.3 Methodology

For securing a distributed system at authentication and authorization there are many processes have discovered by the experts. Most of the important methods have been explained with their advantages and drawbacks. So differentiation between two methods or more than two methods can easily be done. Comparative analysis clears that which method should be chosen for better/best performance in a distributed system for maximum security.

1.4 Thesis Organization

This thesis is the result of study about security for authentication and authorization in a distributed system. The introduction in chapter one is followed by the distributed system security in chapter two. The security threats in chapter three are followed by the security solutions in chapter four. Chapter four includes Encryption, Authentication security, Message Integrity and confidentiality, Authorization, Comparative analysis. A brief explanation of different methods for securing authentication and authorization in a distributed system has been explained in chapter four. In chapter five, two implemented methods of secure authentication have been showed. Finally, chapter six is the conclusion part of this paper.

2. DISTRIBUTED SECURITY SYSTEM

For creating a secure environment in distributed system we need to assure of secure in authentication, authorization, message confidentiality field because most of the security problems occur in these areas. Authentication is accepting proof of identity given by a user who has evidence that the identity is genuine. So for confirming identification of a real identity authentication performs an important role in distributed system. After permitted by authentication process a user must have some rules for using the total system. For this reason there must be authorization method for limiting user's performances. So, each of the user must be authorized. Message confidentiality is also an important part of distributed system. It secures messages from intruders.

3. SECURITY THREAT

Interception , Interruption , Modification , Fabrication are the four types of security threats . Accessing a service in distributed system by an unauthorized party is called interception. Interruption can be defined by the situation when unusable, destroyed, and unavailable of a data or services occurred. Modification defined by unauthorized change in a service or data in a distributed system. When extra data or job is produced that should not stay in normal then the situation is called fabrication.

4. SECURITY SOLUTIONS

Main solutions for security in a distributed system are encryption, authentication and authorization. By encrypting a data using encryption a non allowed user can't understand what the original meaning of that data is. Encryption provides confidentiality. To verify a claimed identity of a particular user or a particular host authentication is used. For controlling access in a service for an outsider or insider user authorization is used.

4.1 Encryption

Encryption actually is a method by which a message can be secured by encrypting .It is the process by which a plain text is encoded using keys . This encoded text can't be understand without decoding it with the keys. So a non allowed user which don't have any keys to decode it can't bring the original data.

Suppose P = plain text ; the actual message
Encrypt(P) = P_e , Encrypted message
Decrypt(P_e) = P , Decrypted message / original plain text
There are two types of encryption methods asymmetric and symmetric.

4.2 Authentication Security

Authentication security is very important for identifying a user in a distributed system. After authenticating a user can have access in the services. If an intruder become authenticated and have access in the services and its resources then it can harm the system. So, well authentication security should be used in any system. Most of the authenticating processes occurred at the time of logging. Users enter something what they know which is identified by authentication method.

4.2.1 Authentication using Password

Password based authentication is very popular for its low cost and convenient use [4]. But, at the same this vulnerable for a password guessing attacker.

Encrypted Key Exchange (EKE) Protocol

Using a combination of symmetric and asymmetric cryptography Bellovin and Merritt [15] developed a password-based encrypted key exchange (EKE) protocol against offline dictionary attacks [4].

1. A : (E_A,D_A), K_{pwd} = f(pwd). {* f is a function. *}
2. $A \rightarrow B$: A, $\{K_{pwd}\}E_A$.
3. B : Compute $E_A = \{\{E_A\}K_{pwd}\}K^{-1}_{pwd}$ and generate a random secret key K_{AB} .
4. $B \rightarrow A$: $\{\{K_{AB}\}E_A\}\{K_{pwd}\}$.
5. A : $K_{AB} = \{\{\{\{K_{AB}\}E_A\}\{K_{pwd}\}\}K^{-1}_{pwd}\}D_A$. Generate a unique challenge C_A.
6. $A \rightarrow B$: $\{C_A\}K_{AB}$.
7. B : Compute $C_A = \{\{C_A\}K_{AB}\}K^{-1}_{AB}$ and generate a unique challenge C_B.
8. $B \rightarrow A$: $\{C_A, C_B\}K_{AB}$.
9. A : Decrypt message sent by B to obtain C_A and C_B. Compare the former with his own challenge. If they match, go to the next step, else abort.
10. $A \rightarrow B$: $\{C_B\}K_{AB}$ [4].

A secret key K_{pwd} from A's password pwd is derived by A and also it generates a public/private key (E_A,D_A). Public key E_A with K_{pwd} is encrypted by A and sends it to B. The message is decrypted by B and encrypt K_{AB} using E_A and K_{pwd} ; sends it to A. To encrypt C_A (unique challenge) A uses that session key sends it to B. B generates unique challenge C_B. With the session key K_{AB} C_A, C_B encrypted by B and sends it to A. Decrypting the message C_A, C_B obtained by A and compares the former with the challenge it had sent to B. B is authenticated if they match. A encrypts C_B and send it to B. B decrypts the message to obtain C_B and to authenticate A.

Advantages

Achieving authentication using password based authentication has low cost and convenience.

Drawbacks

By building a database of possible passwords which is called dictionary and picking a password from this intruder can test it if it works. Intruder can do it for several times and if he becomes failed then he can try for login with another picked password [4].

4.2.2 Mutual Authentication

Using public-key cryptography mutual authentication can be done. Lets take a client named is Alice and Bob is a name of a server. Bob's public key is needed by Alice. Alice can ask for Bob's , as shown in the figure below message 1 , If a PKI (public key infrastructure) stays with a directory server that hands out certificates for public keys. Bob's public key is the replay in message 2 which is an X.509 certificate. Alice sends a message which is contained her identity to Bob after verifying that the signature is correct. Bob don't know whether the received message is from Alice or from intruder then he asks the directory server for Alice's public key in message 4 , which he soon gets in message 5 . After this Bob sends message 6 containing Alice's R_A (R_A is the challenge from Alice) to Alice, his own nonce , R_B (R_B is the challenge from Bob) , and a proposed session key , K_S.

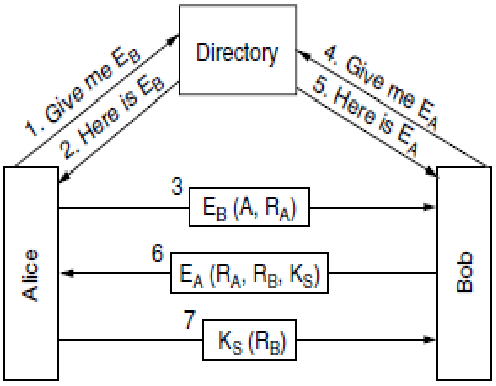


Fig 4.1 Mutual authentication using public-key cryptography [3][5]

Alice decrypts message 6 after getting it using her private key and see R_A. This message must be came from Bob because intruders have no idea about R_A. By sending back message 7 Alice agrees to the session. Bob knows Alice got message 6 and verified R_A after watching R_B which generated by him with the session key. An intruder cannot produce message 7 back to Bob because she/he does not know R_B or K_S and cannot determine them without Alice's private key [3] [5] .

Advantages of Mutual Authentication

1. Using public key cryptography security convenience is increased in mutual authentication.
2. Using public key authentication there is no chances of keeping copies of secret keys of any user, so each user has sole responsibility for protecting his or her private key.

Drawbacks of Mutual Authentication

Using public key cryptography for encryption the speed of the process become slowly

4.2.3 Authentication using Biometrics

In Biometrics authentication is done by using the measurement of physical characteristics of a user. A typical biometrics system has tow parts one is enrollment and other is identification. In enrollment process the user's characteristics are measured and the results digitized. Then important features are extracted and stored in a record associated with the user. In identification process user shows up and provides a login name. The system makes the measurement again. When the new values match with the old sampled during the enrollment time, then the login is accepted .otherwise the login is rejected [2].

Advantages of Using Biometrics

1. Biometrics allows for increased security, convenience and accountability while detecting and deterring fraud [9].
2. Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes [7].

Drawbacks of Using Biometrics

1. Biometrics authentication is costly though there is chance of security risk like every authentication methods [9].
2. Still biometrics authentication solutions are not available all over the world [9].

4.3 Message Integrity and Confidentiality

Protecting messages against hidden modifications called message integrity. The protected message can't be break off and read by any intruders is ensured by confidentiality. Confidentiality can be established by encrypting a message before sending it. RSA (Rivest,Shamir,Adleman) can be used for encrypting. Rivest, Shamir, Adleman together discovered this method at M.I.T. in 1978.It is structured by using some principle from number theory. Summary of how to use it:
1. Choosing p and q two large primes (typically 1024 bits).
2. Computing n = p*q and z = (p -1) *(q -1).
3. Choosing d is a number which is relatively prime to z .
4. Finally find out e in a way that e *d = 1 mod z.
Lets take P is a message. For encrypting P, compute $C = P^e$ (mod n) ; here e and n is needed. For decrypting C , compute $P = C^d$ (mod n) ; here d and n is needed [3][5].

➢ **Digital Signatures:**
Digital Signatures can be performed by two ways one is symmetric key signatures and other is public key signatures. Symmetric key signature is a method where have to trust one central authority that knows everything. Central authority hands a secret key which have to choose each user. Public key signatures are better than Symmetric key signatures because trusting one central authority is not a good way.

4.4 Authorization

For controlling access rights authorization processes are used in a distributed system.

4.4.1 Access Control Security

Access control means identifying access rights and authorization means granting access rights.

Protection Domain: Protection domain is defined by a set of pairs (object, access rights). Operations are performed by a given object and each pair specifies this. When a subject requests an operation to be performed by an object then the reference monitor first search the protection domain corresponded with that request. Whether the request is allowed to be performed, it is checked by the given domain and reference monitor afterward [1][6].

Advantages of Protection Domain

Protection domain can be used as roles. In role based access control an user has a specific role. The protection domain is identified by user's role in which he will operate [1].

Drawbacks of Protection Domain

Looking for a member's access control through the database is costly for a large collection.

➢ **Firewalls:**
Every incoming and outgoing packet are inspected by firewall. Here , firewall works as a packet filter. Those packets that full fill some criterion described in protocols structured by the network administrator are passed normally. Failed packets are dropped. For keeping track of connections firewalls map packets to connections and use TCP/IP header fields [1].

Packet-Filtering Gateway

Based on the source and destination address as contained in the packet's header packet filtering gateway firewall operates as a router and makes decisions as to whether or not to pass a network packet[1][6].

Application-Level Gateway

Proxy gateway is a special kind of application level gateway. It ensures that only those messages are passed that have certain eligibility and works as front end [1] [6].

Advantages of Firewalls

1. Incoming and outgoing internet traffic must pass through a single check point. Thus unauthorized traffic is banned.
2. Yet it is the one which is not easy for hacking on the internet.

Drawbacks of Firewalls

1. It is expensive and don't provides foolproof for protections [8].

➢ **Java Security:** Security of distributed system can also be done by java. For this purpose developers need to create programs that are executed on remote distributed systems.

Sandbox Security Model

In order to have all applets run in a protected environment the sandbox security model was developed. Code run locally would have full access while applets that run from a remote site would be permitted only limited access to the system. If the remote applet is signed and trusted, then it can run with full local system access. A security policy that allows the administrator to define how the applets should be run is settled for permissions.

Advantages of using Agent

1. Mobile agent moves computation code to data, and the intermediate results passing are reduced. The network bandwidth consumption is reduced [12].
2. Agent operates asynchronously and autonomously, and the user doesn't need to monitor the agent as it roams in the Internet. This saves time for the user, reduces communication costs, and decentralizes network structure [12].

Drawbacks of using Agent

Need to protect mobile code against malicious host and more important is that need to protect host against malicious mobile code.

Comparative Analysis

Differentiation can be found when we comparison one process with others. All of the authentication/authorization process wouldn't have same advantages. So, comparative analysis can play an important role in this case.Based on the described authentication processes in chapter 4, security solutions; differentiated the processes of authentications here.

Table 4.1 Comparative Analysis of Authentication

Authentication using password	**Mutual authentication**	**Authentication using biometrics**
1.User pick a password .which can be mixed of integers , alphabets or any symbol [4].	1.It refers two users authenticating with each other at the same time. This users can be client and server[3] [5].	1.In Biometrics authentication is done by using the measurement of physical characteristics of a user [2].
2.Using password based authentication can be utilized for login , registration in a distributed system [4].	2.Mutual authentication Can be done using symmetric encryption and asymmetric encryption [3] [5].	2.It is divided in two parts . one is enrollment and other is identification [2].
3.Achieving authentication using password based authentication has low cost and convenience. It is also easy to remember [4].	3.Using public key cryptography security and convenience is increased in mutual authentication. Using public key authentication there is no chances of keeping copies	3.Biometrics allows for increased security, convenience and accountability while detecting and deterring fraud [9]. Biometrics occurred the

	of secret keys of any user, so each user has sole responsibility for protecting his or her private key [3] [5].	possibilities automatically to know “who” did “what”, “where” and “when” [7].

Authentication using password is very popular and easy to remember. The process of password based authentication is simpler than biometrics authentication. But there are some risks using password based authentication. Intruders can keep eyes when typing the password on the keyboard. Advanced intruders like crackers can do dictionary attack. For this reason the combination of the password should be very hard. In replacement of using password biometrics can be used. Using biometrics there are no any troubles about memorizing a password for entering in a distributed system. Biometrics authentication is done by using the measurement of physical characteristics of an user. The system makes the measurement again at the time of entering in the system. When the new values match with the old sampled during the enrollment time, then the login is accepted [2].So in this case an intruder can’t attack using possible password’s dictionary. But the cost of biometrics authentication is so high where using password based authentication’s cost is low comparatively.

Mutual authentication is just for two end users. It is done with using encryption and decryption which can be the reason slowing the process.

Based on the described authorization methods in chapter 4, security solutions; I differentiate the methods of authorizations here.

Table 4.2 Comparative Analysis of Authorization

Protection Domain	**Using Agent**	**Firewalls**
1.It is a set of object and access rights . objects and access rights both together is called pairs. This pairs specify for a object exactly which operations should be done [1] [6].	1. An agent is actually a computer program that acts as a security agent in a distributed system to protect securities for a user [1] [6] .	1. Firewall is a special kind of reference monitor which control the external access of any part of a distributed system [1] .
2. Different uses of protection domains exist. Such as access control matrix, construct groups of users. Where the exact operations for a object are defined [1][6].	2.Agent is actually a code. They protect themselves from vulnerabilities and also protect users from malicious code [1] [6] .	2. Every incoming and outgoing packet are inspected by firewall. Here , firewall works as a packet filter. Those packets that full fill some criterion described in protocols structured by the network administrator are passed normally. [1] .

In protection domain process a pair of object and access rights specify the exact operations which should be done by the object. But looking for a member’s access control through the database is costly for a large collection. So in that case we can use agent using security services. An agent is actually a computer program which acts as a security agent. For protecting a user from malicious codes and vulnerabilities at first the agent should protect itself properly. After that it can protect users from vulnerabilities. Agent operates asynchronously and autonomously, and the user doesn't need to monitor the agent as it roams in the Internet. This saves time for the user , reduces communication costs, and decentralizes network structure [12].But If the agent can’t protect itself from modifying by an outsider or an outside’s malicious code then it can’t protect the user rather causes corrupts. Though Firewalls also don’t provide foolproof protection but it is full of robust. It is one of the most effective forms of protection yet developed against hackers operating on the internet. But it is costly for a small company.

5. IMPLEMENTATION

5.1 Implementation of Mutual Authentication Using RSA Algorithm

This project is a out put of RSA method implementation . It is specially between two nodes one is server and another is client. Both of them can send messages to each other which is encrypted and decrypted by RSA method.

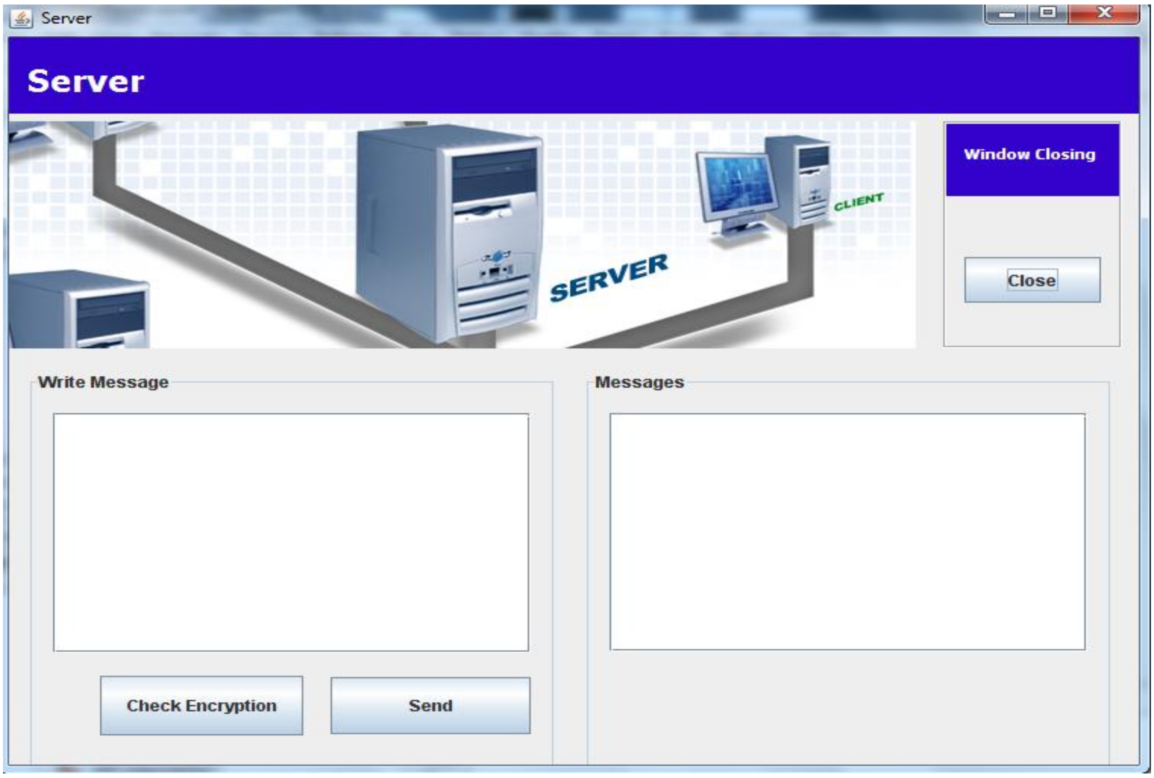


Fig 5.1 Running Server

In this figure the server is running.

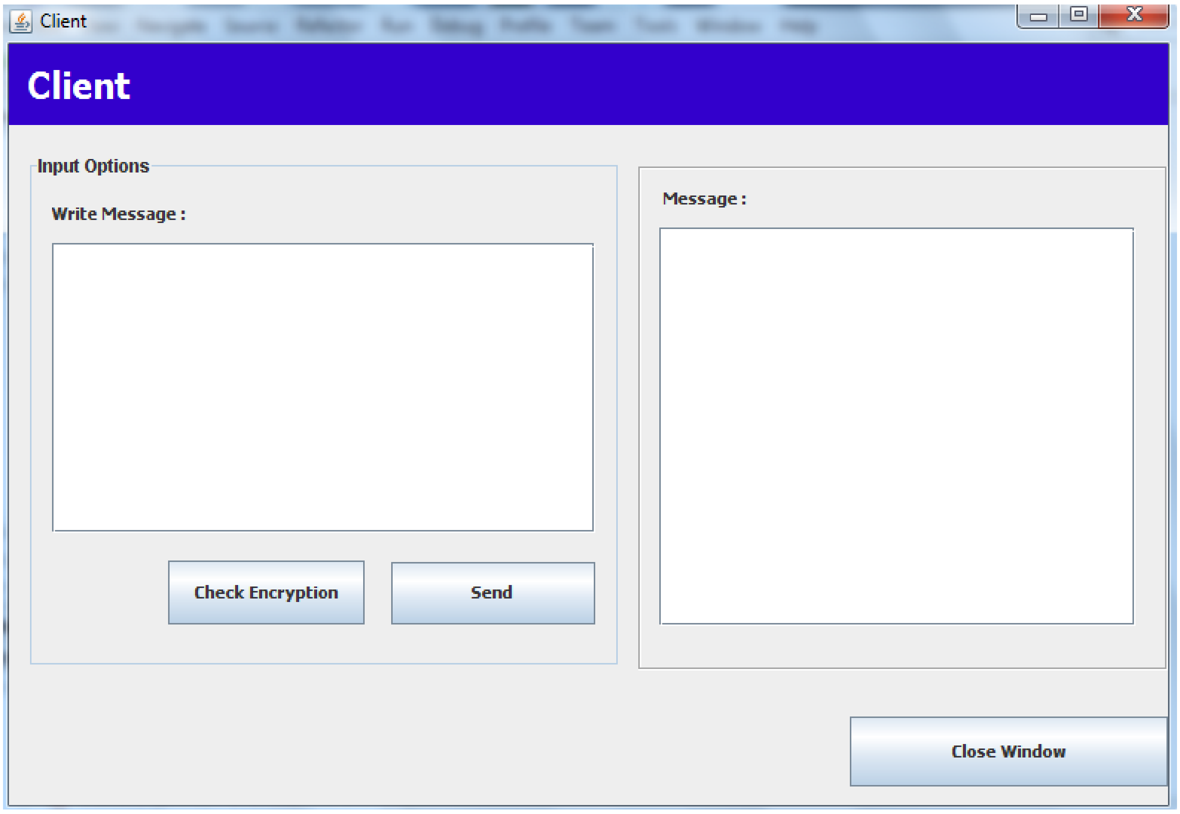
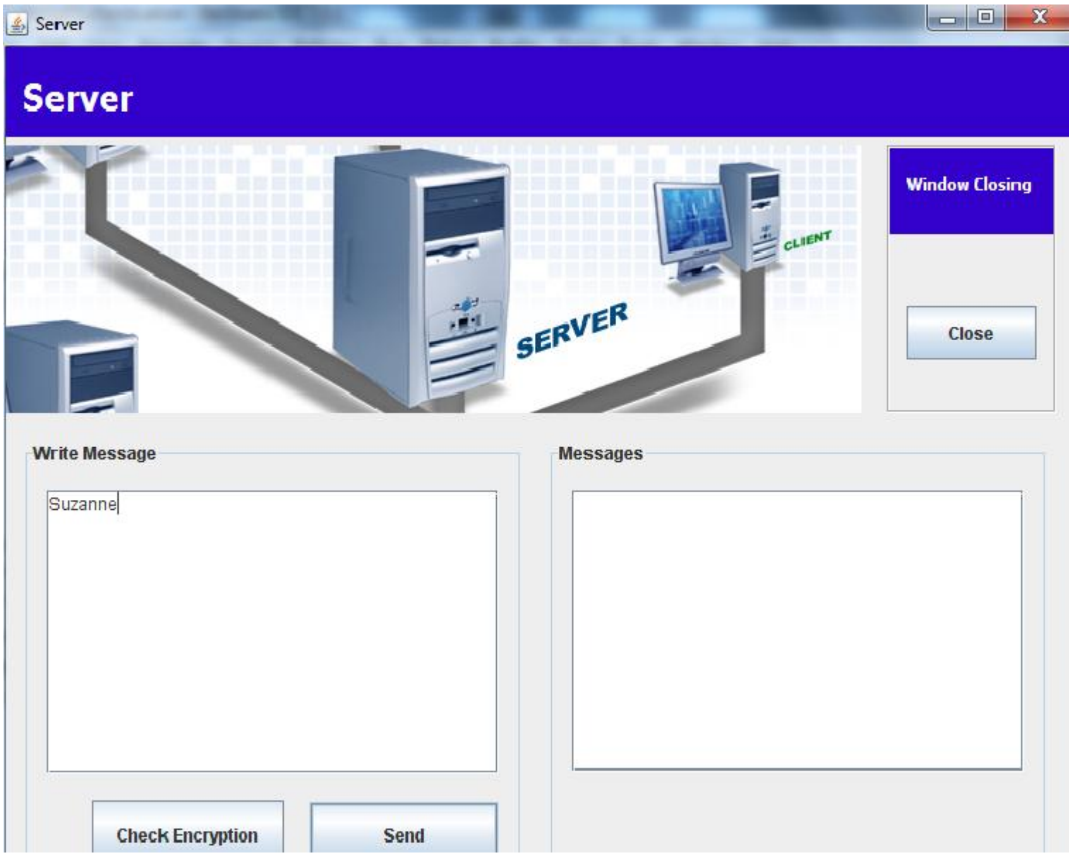


Fig 5.2 Running Client

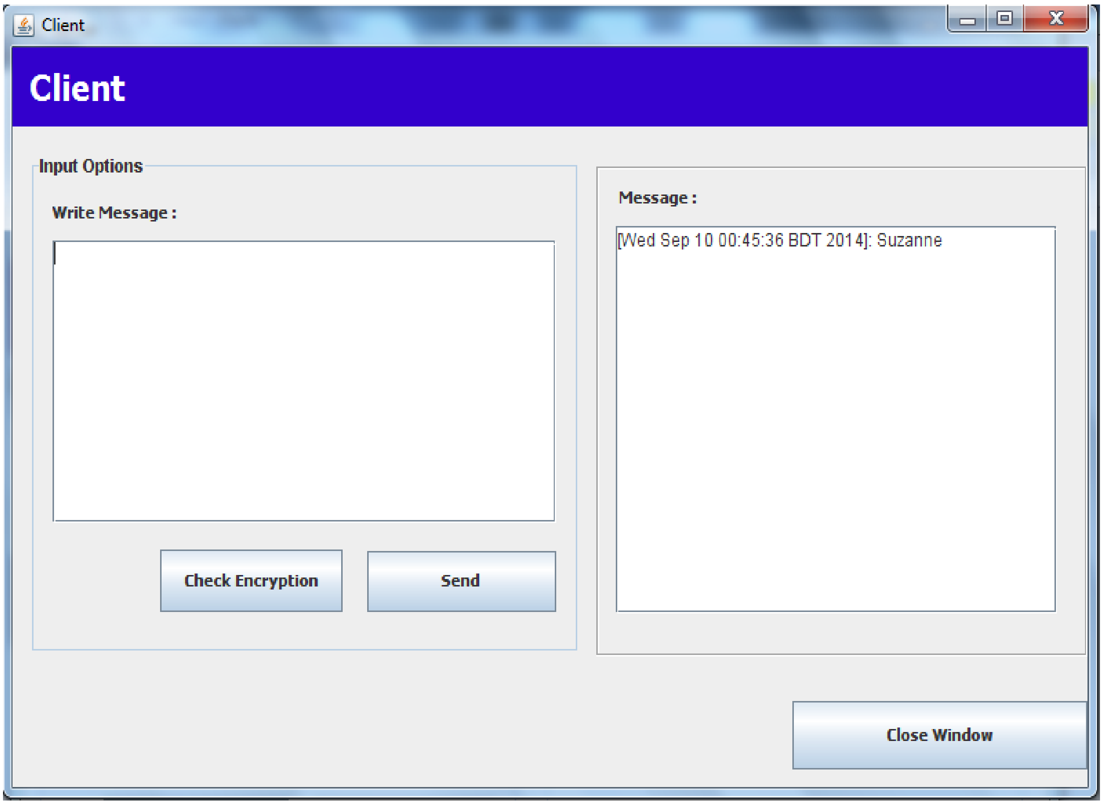
Client is running.



Suzanne

Fig 5.3 Server sending message to client

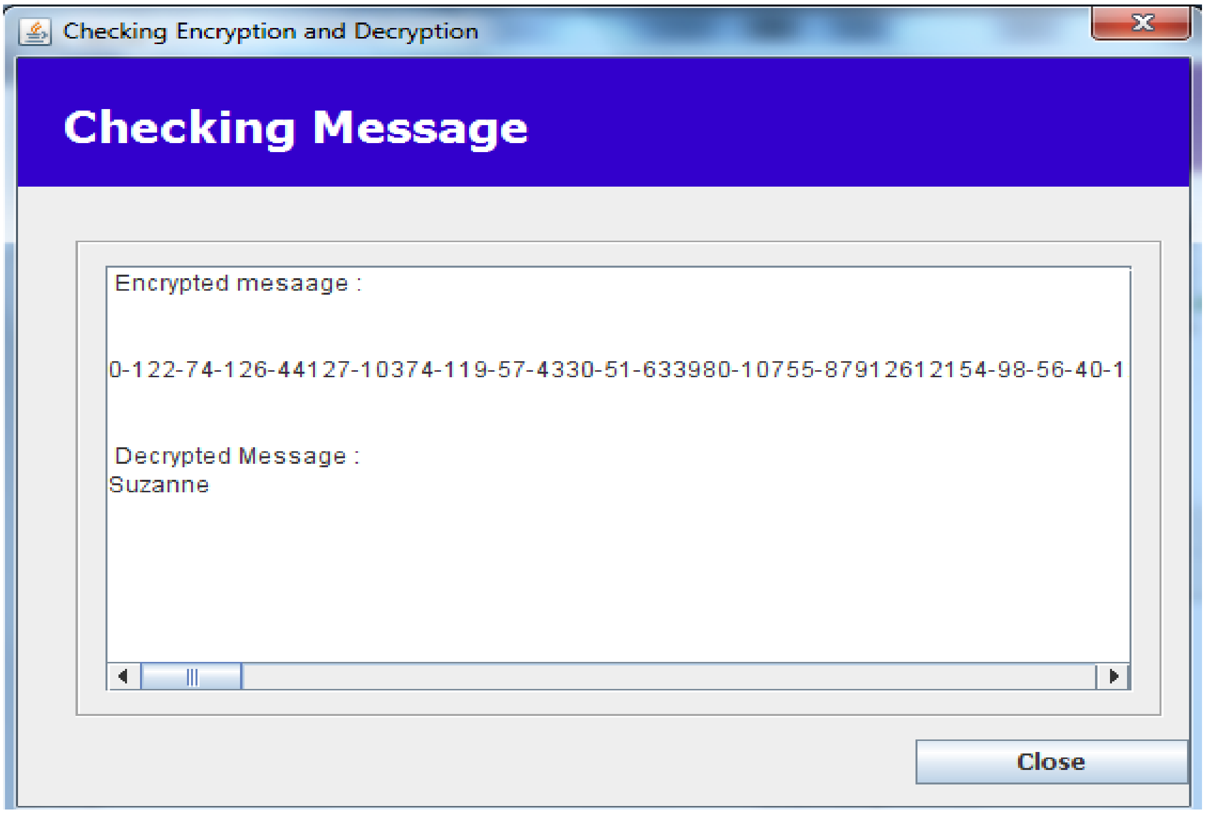
Server write message and send it to the client.



[Wed Sep 10 00:45:36 BDT 2014]: Suzanne

Fig 5.4 Client got the message after decrypting.

Client got the message.



Encrypted mesaage :

```
0-122-74-126-44127-10374-119-57-4330-51-633980-10755-8791261215 4-98-56-40-1
```

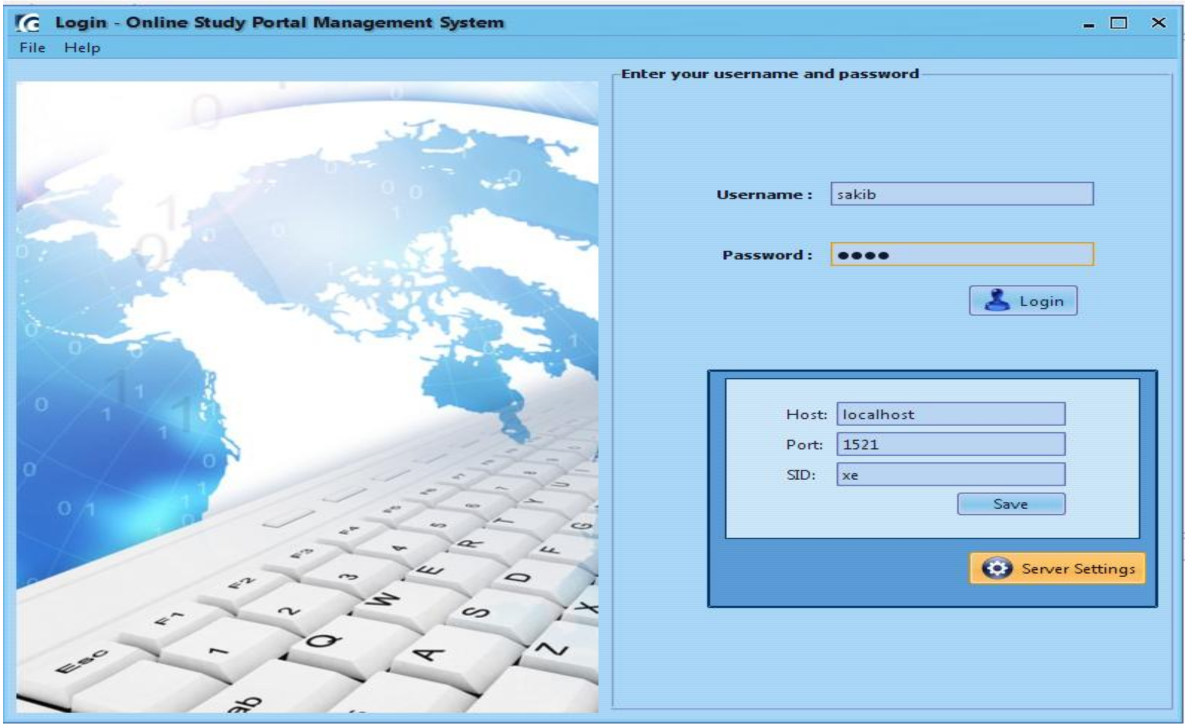
Decrypted Message :
Suzanne

Fig 5 5 Server or Client can check the encrypted message.

Server can check the message to be sure of encrypting by clicking “Checking Encryption” Button.

In the same way client also can send message to the sever and also can check it’s encryption in the checking encryption and decryption dialogue.

5.2 Implementation of Password based Authentication



Login - Online Study Portal Management System
File
Help
Enter your username and password
Login
Save
Server Settings

Username : sakib

Password : ●●●●

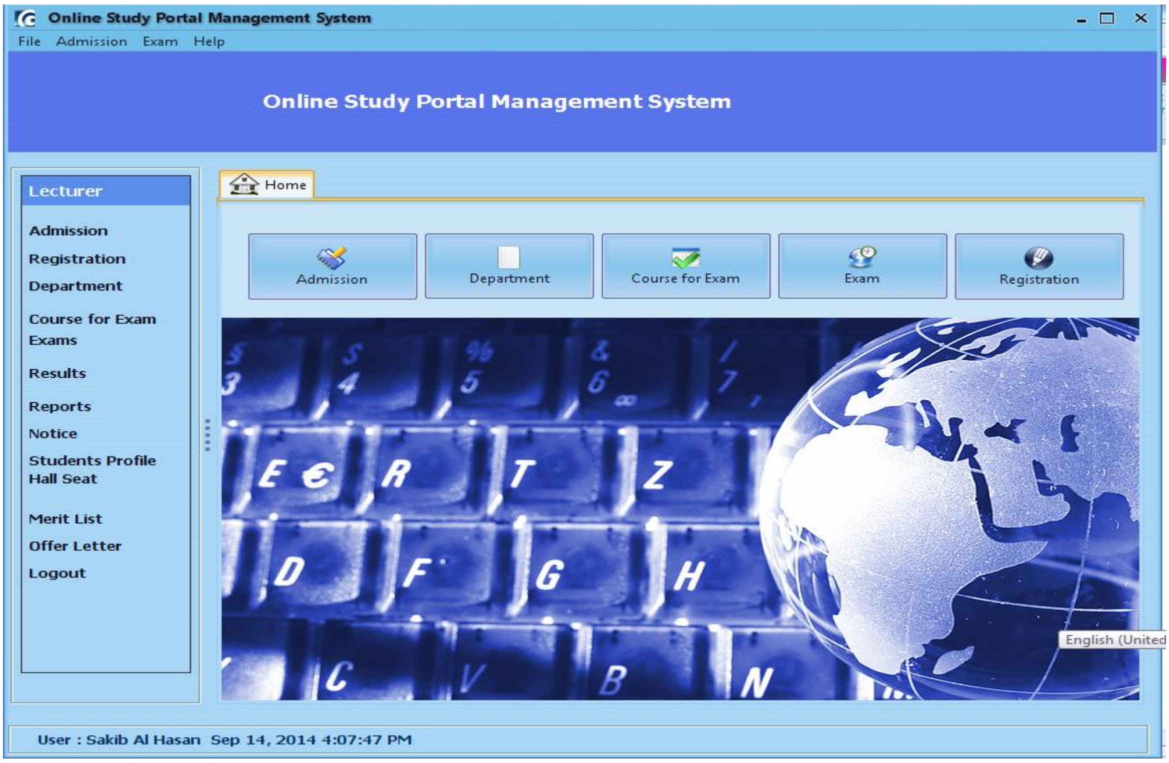
Host: localhost

Port: 1521

SID: xe

Fig 5.6 Entering in the server by logging

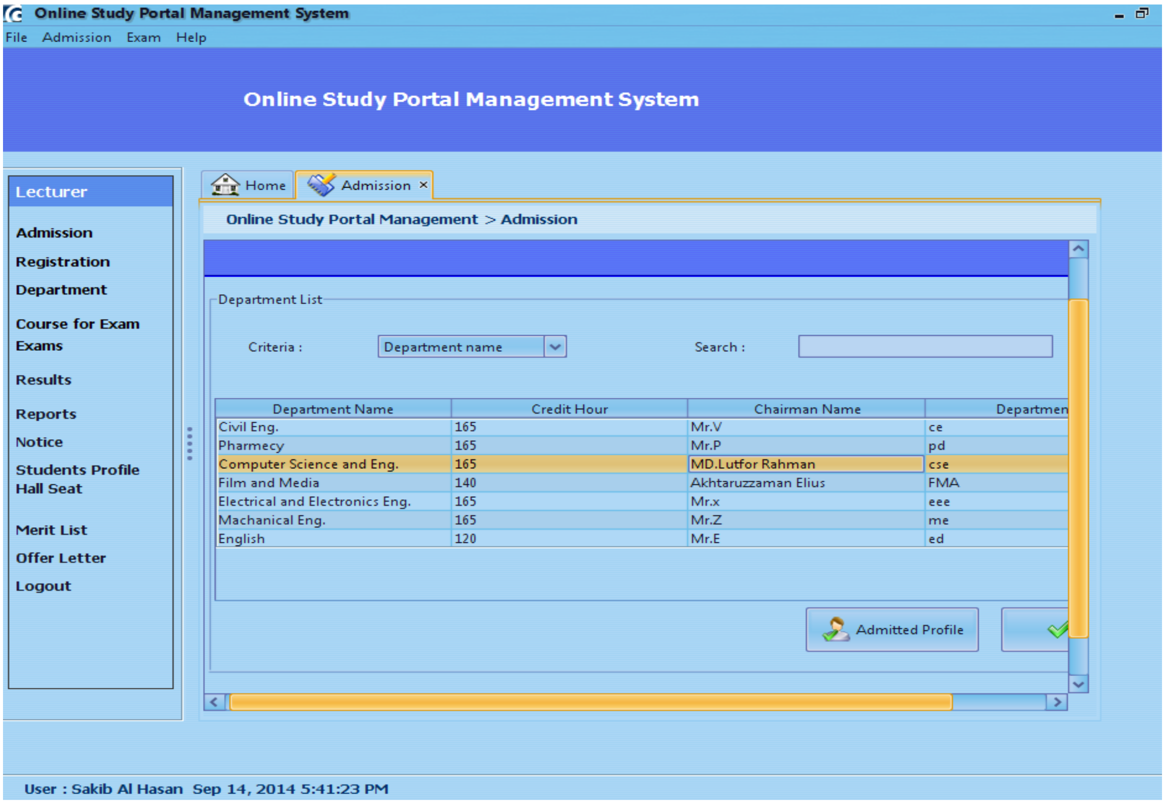
Logging in a Server for example online study portal. This login is based on password authentication . Users type username and password to enter the server for online study portal.



User : Sakib Al Hasan Sep 14, 2014 4:07:47 PM

Fig 5.7 The home of the server

After login enter the server.



Department Name	Credit Hour	Chairman Name	Departmen
Civil Eng.	165	Mr.V	ce
Pharmecy	165	Mr.P	pd
Computer Science and Eng.	165	MD.Lutfor Rahman	cse
Film and Media	140	Akhtaruzzaman Elius	FMA
Electrical and Electronics Eng.	165	Mr.x	eee
Machanical Eng.	165	Mr.Z	me
English	120	Mr.E	ed

User : Sakib Al Hasan Sep 14, 2014 5:41:23 PM

Fig 5.8 An user can perform particular functions

When clicking the Admission one can get admitted.

5.3 Graphical Presentation of Mutual Authentication and Password based Authentication

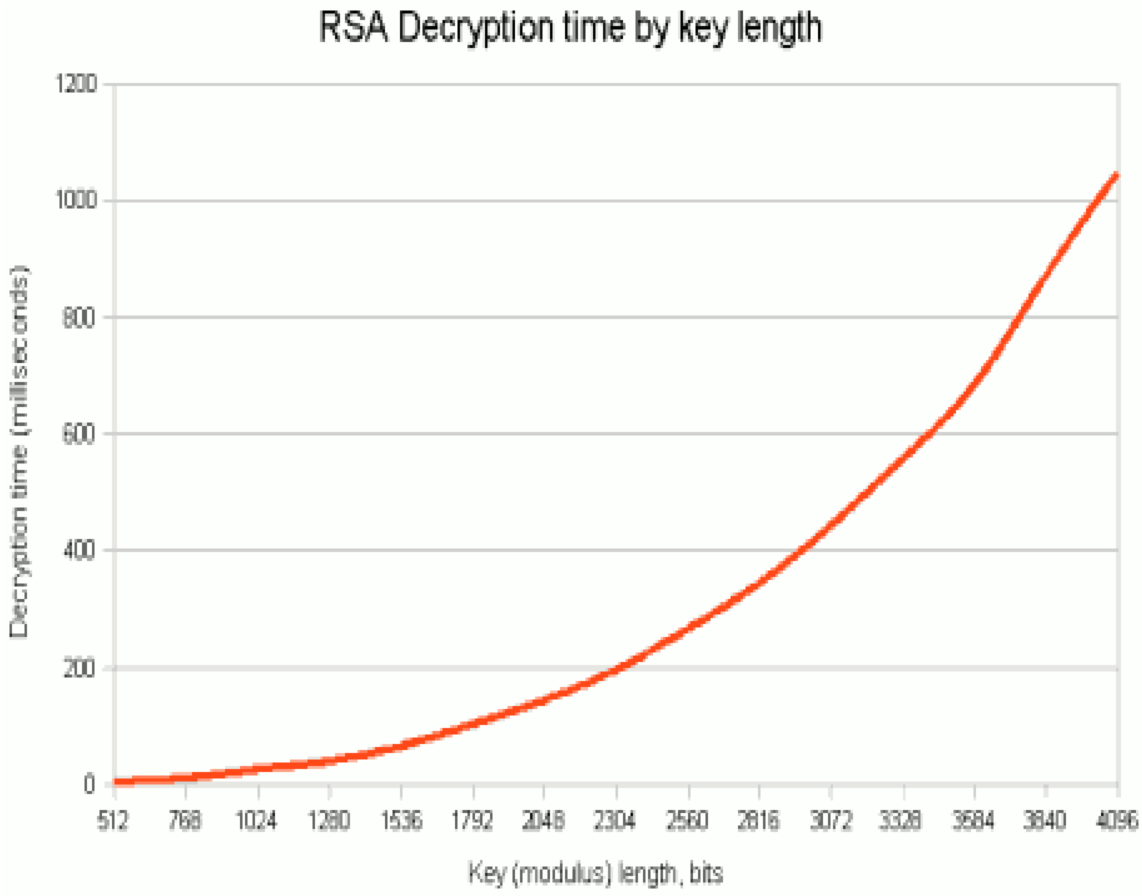


Fig 5.9 Mutual authentication using RSA [14]

Using RSA method for encryption and decryption in mutual authentication the time is infinite to bits length. If the length of bits is larger time is increased for decrypting. This is showed in this graph. Mutual authentication is used where high level security is needed. This process is costly because it refers to only two parties authenticating each other at the same time.

6. CONCLUSION

Through this thesis, security in a distributed system has been described. The advantages and drawbacks of each process have been pointed. Comparative analysis has been done within described methods. Implemented methods of mutual authentication and password based authentication has been showed; found that time varies with each method. Authentication using password is right for ordinary users where mutual authentication is used when extra protection is needed and authentication using biometrics is used in super high level area. Access control security can be done by protection domain in a small area but for large and high protected organizations, firewall can be the best. The main motive of this thesis is to have a secure environment for a distributed system as well as reduce cost, save time and find simple methods for secure authentication and authorization.

ACKNOWLEDGEMENTS

Special thanks go to my teacher under whom I have done my thesis for his kindly guidelines; and especially for providing very useful and timely suggestions. Without his insight, resources and information, it would have been very difficult to write this thesis.

Finally, I also want to thanks to my family and my friends for their inspiration to move forward.

REFERENCES

[1]. Andrew S. Tanenbaum, Maarten Van Steen,*Distributed Systems principle and paradigms* , New jersey , Pearson Prentice Hall,2006, pp. 396-442.
[2]. Andrew S. Tanenbaum, *Modern Operating System*, Pearson Prentice Hall,Amsterdam, 2009,pp. 651-655.
[3]. Andrew S. Tanenbaum, Whterall,*Computer Networks*, New York, Pearson Prentice Hall , 2011, pp. 794-796.
[4]. A.Kshemkalyani , M.Singhal, *Distributed Computing : Principles, Algorithms and Systems* , New York ,Cambridge University press ,2008, pp. 623-625.
[5]. Andrew S. Tanenbaum, Whterall, *Computer Networks*, New York, Pearson Prentice Hall , 2011, pp.763-871.
[6]. Andrew S. Tanenbaum, Maarten Van Steen,*Distributed Systems principle and paradigms* , New jersey , Pearson Prentice Hall,2006,pp. 378-439[7]

Biometrics, “Advantages of Biometrics : Why opt for biometric technology?” , Internet: http://www.questbiometrics.com/advantages-of-biometrics.html , August 8,2014.
[8]. Encyclopedia of Business, “Firewalls”, Internet: www.referenceforbusiness.com/small/Eq-Inc/Firewalls.html , August 3,2014.
[9]. Edmund Spinella , *Biometric Scanning Technologies: Finger, Facial and Retinal Scanning* , SANS Institute InfoSec Reading Room,28 May 2003,pp 8-10.
[10]. Gollmann, D. (2001). Computer security. West Sussex, England: John Wiley & Sons Ltd.
[11]. L. Moreno , *Distributed Systems Security: Java, CORBA, and COM+*, SANS Institute InfoSec Reading Room, pp. 5-7.
[12]. Mohammadian M., “Advatages and disadvantages of using mobile agent approach”, Internet: http://flylib.com/books/en/4.4.1.138/1/ , August 3 , 2014.
[13] S. M. Bellovin and M. Merritt, Encrypted key exchange: password-based protocol secure against dictionary attacks, *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, 1992, 72–84.
[14] RSA key length,“RSA key length”, http://www.javamex.com/tutorials/cryptography/rsa_key_length.shtml ,November19,2014.

BIOGRAPHIES

Halima Akhter has done her B.Sc in CSE at Stamford University Bangladesh. She is much more curious, intend to learn something new and hardworking She is very much interested for research in the field of authentication and authorization of distributed system as well as network security.

Md. Ansarul Haque is the faculty member at CSE department, Stamford University Bangladesh. He had done his M.Sc at Halmstad University, Sweden with the collaboration with Aalborg University, Denmark. He had his B.Sc in CSE at Shahjalal University of Science and Technology, Sylhet. He is continuing his research in the field of Information Technology.