ABSTRACT

Authentication is the first step of defense against any attack which compromises integrity and confidentiality of the data. The traditional authentication methods like the password based authentication and the token based authentication are commonly used but are susceptible to various attacks such as the dictionary attack, guessing attack and keylogger attack. Even the biometric authentication method is susceptible to replay attack and also the cost involved with it is not easily affordable by everyone. The alternative to the text based and biometric based authentication methods is the graphical based authentication method. This paper proposes a puzzle based authentication method with the help of server monitoring to produce a secure authentication mechanism. This proposed mechanism would overcome the loopholes present in the traditional authentication methods. With the help of the puzzle based authentication approach, the server would keep a watch on suspicious behavior and would block the request if any suspicious behavior takes place.
Table of Contents

ABSTRACT ........................................................................................................................................ ii
Table of Contents .......................................................................................................................... iii
List of figures ................................................................................................................................... vi
List of tables ................................................................................................................................... viii
1. INTRODUCTION .................................................................................................................. 1
   1.1 Authentication .................................................................................................................. 1
   1.2 Traditional authentication methods ............................................................................... 2
      1.2.1 Text based authentication ...................................................................................... 2
      1.2.2 Token based authentication ................................................................................... 2
      1.2.3 Biometric authentication ...................................................................................... 3
      1.2.4 Graphical based authentication ........................................................................... 3
   1.3 History ............................................................................................................................... 4
   1.4 Loopholes in the traditional authentication methods .................................................... 5
      1.4.1 Loopholes in the text based authentication mechanism ....................................... 5
      1.4.2 Loopholes in the token based authentication mechanism .................................... 7
      1.4.3 Loopholes in the biometric authentication mechanism ......................................... 8
      1.4.4 Loopholes in the graphical based authentication .................................................. 9
   1.5 Rationale ........................................................................................................................... 9
2. NARRATIVE ............................................................................................................................ 11
   2.1 Problem Statement ......................................................................................................... 11
   2.2 Motivation ....................................................................................................................... 12
   2.3 Scope ................................................................................................................................ 13
   2.4 Functionality of the project ......................................................................................... 13
3. PROPOSED SYSTEM DESIGN ......................................................................................... 15
   3.1 A puzzle based authentication mechanism with server monitoring ........................... 15
   3.2 Framework ..................................................................................................................... 16
      3.2.1 Steps in the project development ...................................................................... 16
      3.2.2 System requirements ......................................................................................... 16
   3.3 Proposed Mechanism .................................................................................................. 17

iii
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.1</td>
<td>Working</td>
<td>18</td>
</tr>
<tr>
<td>3.4</td>
<td>System design</td>
<td>20</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Dataflow diagram</td>
<td>20</td>
</tr>
<tr>
<td>3.4.2</td>
<td>Use case diagram</td>
<td>21</td>
</tr>
<tr>
<td>3.4.3</td>
<td>Sequence diagram</td>
<td>22</td>
</tr>
<tr>
<td>3.4.4</td>
<td>Collaboration diagram</td>
<td>23</td>
</tr>
<tr>
<td>4.1</td>
<td>4. FUNCTIONALITIES OF THE APPLICATION</td>
<td>25</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Modules Description</td>
<td>25</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Client module</td>
<td>25</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Server module</td>
<td>30</td>
</tr>
<tr>
<td>5.1</td>
<td>5. TESTING AND IMPLEMENTATION</td>
<td>34</td>
</tr>
<tr>
<td>5.2</td>
<td>Types of Testing</td>
<td>34</td>
</tr>
<tr>
<td>5.2.1</td>
<td>White box testing</td>
<td>35</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Black box testing</td>
<td>35</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Unit testing</td>
<td>35</td>
</tr>
<tr>
<td>5.2.4</td>
<td>Integration testing</td>
<td>36</td>
</tr>
<tr>
<td>5.2.5</td>
<td>Validation testing</td>
<td>36</td>
</tr>
<tr>
<td>5.2.6</td>
<td>Output testing</td>
<td>36</td>
</tr>
<tr>
<td>5.2.7</td>
<td>User acceptance testing</td>
<td>37</td>
</tr>
<tr>
<td>5.3</td>
<td>Test cases</td>
<td>37</td>
</tr>
<tr>
<td>6.1</td>
<td>6. COMPARISON WITH OTHER AUTHENTICATION METHODS</td>
<td>51</td>
</tr>
<tr>
<td>6.2</td>
<td>Advantages</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Disadvantage</td>
<td>52</td>
</tr>
</tbody>
</table>
7. CONCLUSION AND FUTURE WORK ................................................................. 53
BIBLIOGRAPHY AND REFERENCES ............................................................... 54
List of figures

Figure 1: Proposed mechanism’s architecture .............................................................. 18
Figure 2: Proposed system's dataflow diagram .............................................................. 21
Figure 3: Proposed system’s use-case diagram ............................................................. 22
Figure 4: Proposed system’s sequence diagram ............................................................ 23
Figure 5: Proposed system’s collaboration diagram ...................................................... 24
Figure 6: Hostname of the user .................................................................................... 26
Figure 7: New user registration ................................................................................... 26
Figure 8: Registration process ..................................................................................... 27
Figure 9: Registration process ..................................................................................... 28
Figure 10: Login stage .................................................................................................. 29
Figure 11: Accessing the server .................................................................................. 30
Figure 12: Server keeping track of client details ......................................................... 31
Figure 13: Server keeping track of registration details .................................................. 31
Figure 14: Server keeping record of the puzzles allocated to the users ....................... 32
Figure 15: Server keeping track of the users’ movements .......................................... 33
Figure 16: Hostname of the computer ....................................................................... 39
Figure 17: User entering the correct hostname of the computer .................................. 39
Figure 18: User providing incorrect hostname ............................................................. 40
Figure 19: Successful registration by the user .............................................................. 41
Figure 20: Unsuccessful registration .......................................................................... 42
Figure 21: User logging in ............................................................................................ 43
Figure 22: User solving the puzzle successfully ............................................................ 43
Figure 23: Fraudulent login ......................................................................................... 44
Figure 24: User’s IP address ............................................................................................. 45
Figure 25: Server monitoring the user’s IP address .......................................................... 46
Figure 26: Server maintaining a list of registered users ................................................... 46
Figure 27: Server monitoring the moves of a genuine user .............................................. 47
Figure 28: Server monitoring the moves of an attacker .................................................... 47
Figure 29: Server sending email to the user when the user logsins .................................. 48
Figure 30: Server sending an email to the user when more moves than usual take place 48
Figure 31: Server sending an email when puzzle is not solved ....................................... 49
Figure 32: File access with server ..................................................................................... 50
List of tables

Table 1: Comparison of the authentic methods ................................................................. 51
1. INTRODUCTION

1.1 Authentication

Security is an important concern for any individual, firm or an organization. Authentication is the process which provides the first line of security or the basic security to an individual or a firm. Authentication is a process which determines whether a particular entity should be allowed to access the resources or not. It makes sure that only the genuine entity is getting access to the resources. Authentication is performed with the help of three factors- 1) Something the user has, 2) Something the user knows and 3) Something the user is. In the first factor, authentication is performed with the help of a physical device that an individual possesses. The device may be a token or any other smart card. The individual should present this device to the authorizing center to get access to the resources. In the second factor, authentication is performed with the help of something that the individual knows like a password or a pass phrase. The individual should provide the correct password or pass phrase to get access to the resources. In the third factor, authentication is performed with the help of the physical features of an individual like the fingerprint or the face.

Conventionally, the text based passwords are used for user authentication. But it is a challenging task for the users to memorize huge passwords. The text based passwords are also vulnerable to many attacks. Thus as an alternative to the textual based authentication method, the graphical based authentication method was proposed. [Newman 2005] The image based passwords generally are more memorable than text based passwords. This proved to be a significant advantage for the graphical based
authentication scheme. [Masrom 2009] The graphical based password schemes which currently exist are mainly divided into three categories: 1) Recognition of pass-images, 2) Repeating actions in a sequential order and 3) Reproduce a particular drawing. Draw-A-Secret (DAS) is a method which comes under the “Reproduce a particular drawing” category. In the DAS method, the user would be needed to create a drawing on an N x N grid which would be used as the graphical password.

The graphical authentication mechanism proposed in this paper would be like a puzzle based authentication method. This method would also have a server monitoring continuously. The server would detect any fraudulent attempt by the attacker to gain access to the system.

1.2 Traditional authentication methods

1.2.1 Text based authentication

The password based authentication is the method which comes under the text based authentication. [Ziran 2009] In the password based authentication method, the user has to create an alphanumerical key initially during the time of registration. The user should type this same key each time he wants to access the system or the resources. The text based authentication can also have some security questions which need to be answered with the help of the keyboard. This is the most common type of authentication practiced around the globe.

1.2.2 Token based authentication

In the token based authentication system, the user would be provided with a device like a token or an electronic smart card. The user would have to present the token
to the authorizing center to get access into the system or the resources. Normally in corporate offices, every employee would have his identification card. The employee would need to swipe his identification card in order to enter the office or in order to gain access to the system. This is how the token based authentication mechanism works. The token based authentication mechanism is not as common as the text based authentication mechanism.

1.2.3 Biometric authentication

The biometric authentication method makes use of the basic fact that all humans have unique physical features. [Maytas 2010] The biometric authentication process would depend on the physical features of the humans which would remain the same throughout their life span such as the finger prints. The most common type of this method is the fingerprint scanner method. Initially the user would register himself with his fingerprint in the fingerprint scanner. In future, the user would have to give his fingerprint impression on the scanner. If it matches with the initial fingerprint during the registration, then the user would be given access.

1.2.4 Graphical based authentication

The [Sabzevar 2008] graphical based authentication method replaces the text based passwords with the image based passwords. A user would generally remember a graphical image better than plain text. Because of this reason, the usability of the graphical based authentication method is higher than other authentication methods. The graphical based password method completely eliminates the susceptibility to dictionary attack and key-logger attack. Thus graphical based authentication method would provide much higher security than other authentication methods. Generally the graphical
authentication methods would be classified into two categories: Recognition based and Recall based graphical methods. In the recognition based method, a group of images would be displayed to the user and the user would have to select the correct image to get access into the system. Awase-E system is an example of this method. In the recall based method, the user would be asked to recall something which he created during the registration phase. The pass-point method which is the previously proposed graphical method comes under the recall based graphical methods.

In the pass-point method, the user would have many regions in an image to choose as the password. In other words, there would be many clickable regions in an image for the user to choose from. To set a password, the user has to choose some regions in the image as a design and should produce the same design to get access into the system. Since the pass-point method has many clickable regions in an image, it would mean that the password space would increase. Increase in the password space would in turn increase the security level. Thus pass-point method has high security compared to all the graphical based authentication methods and was the previously proposed method.

1.3 History

Authentication is normally the first line of defense in any system. Thus authentication is really given high importance to provide integrity and confidentiality of data. The authentication based methods traditionally started with the text based authentication methods. The text based authentication method is still the most commonly used authentication method till date. The text based authentication methods started with password based methods and eventually evolved. The text based authentication methods also have included security questions wherein the user would be needed to answer the
security questions and remember it. The authentication mechanisms later evolved and came up with the biometric authentication methods. These methods required the users to produce some impression of their physical features. It made use of the fact that every human in this world would have unique physical features. The fingerprint method is the commonly used biometric authentication method which is used on a large basis.

The token based authentication later came into existence and this required the usage of token. The user had to present a token to get access to the resources. This token had to be kept very secure. Then the graphical based authentication came into existence which did not require the use of the keyboard. [Haichang 2009] In this type of authentication, the user had to use some sort of design or remember some image. This type of authentication is still not commonly used. There are many issues concerning the graphical based authentication method. Some of the issues that this authentication method has are that it might consume more time or it might not be practical enough.

1.4 Loopholes in the traditional authentication methods

Now the loopholes in each of the authentication methods would be discussed.

1.4.1 Loopholes in the text based authentication mechanism

The text based authentication mechanism is susceptible to 1) Guessing attack, 2) Dictionary attack, 3) Key-logger attack

1) Guessing attack

This type of attack would generally take place in the text based authentication mechanism. In this type of attack, the attacker would try to guess the password of the user based upon the details of the user. The attacker would make intelligent guesses and if any
of the attacker’s guess would turn right, then the attacker would get access into the system. Normally the attacker would get all the personal details of the user and would try to use them as passwords. An attacker can try the user’s nick name or the user’s place of birth or any other random thing associated with the user. This type of attack is a very common attack and any normal person can try to do this kind of an attack. Normally attackers make very intelligent guesses which a normal person cannot make.

2) Dictionary attack

This type of attack would also take place in the text based authentication mechanism. In the dictionary attack, the attacker would try to use all the words of the dictionary to crack the user’s password. If any of the dictionary’s words match the password of the user, then the attacker would gain access to the user’s resources. Thus it is generally required that the user should not keep a dictionary’s word as his or her password. The dictionary attack can take huge amount of time to implement because there are many words in the dictionary. The dictionary attack is not as common as the guessing attack.

3) Key-logger attack

This attack also takes place in the text based authentication mechanism. This is the most effective and most dangerous attack. In this attack, the attacker would install the key-logger software on the user’s machine. Once this software is installed, it would record all the keystrokes typed by the user. It would record all the passwords, security questions and even private chat material which the user would type on the keyboard. The attacker would then open the software and simply look into the keystrokes typed. By looking, the attacker can easily know the user’s password and the attacker would crack
the user’s password. The user would have no idea that the software is installed on the machine. This is a very dangerous attack because all the user’s activities will be monitored easily by the attacker. This type of an attack does not require a person to have high professional skills. Any normal person with simple knowledge and understanding of computers can perform this attack. The key-logger software is easily available on the internet for free of cost and hence it is cost effective also.

1.4.2 Loopholes in the token based authentication mechanism

The token based authentication mechanism is susceptible to 1) Man in the middle attack and 2) Loss of token

1) Man in the middle attack

This type of attack happens in the token based authentication method. This type of attack takes place when an attacker would try to act as a proxy between the user and the authorizing center. The user would think that the attacker is a genuine authority and would present his details to the attacker. The attacker would thus gain all the resources of the user.

2) Loss of the token

Sometimes the user might misplace his token or forget his token somewhere or the user might drop it somewhere accidentally. The attacker might get hold of the user’s token and use the token to gain access to the system. Thus it is extremely important to not lose the token. If the token is lost, the user might have his confidential data to be accessed by the attacker.
1.4.3 Loopholes in the biometric authentication mechanism

The biometric authentication mechanism is susceptible to 1) False-positive matches and false-negative matches, 2) Replay attack, 3) Altering the biometric representation of features, 4) Overriding of the features

1) False-positive and false-negative matches

The false-positive matches may occur sometimes in the biometric device when a false fingerprint would be accepted as a genuine fingerprint. If this occurs, an unauthorized user would gain access to the user’s system. The false-negative matches may occur when a genuine fingerprint would not be accepted by the biometric device. If this happens, the genuine user would not be able to access his or her system.

2) Replay attack

In this type of attack, the attacker would resubmit a recorded signal to the biometric device. By doing this, the attacker would just replay the genuine user’s fingerprint and would gain access to the user’s resources.

3) Altering the biometric features

In this type of attack, the features which are extracted from the data would be replaced with another fake feature set.

4) Overriding of the features

In this type of attack, the attacker would force the device to produce fraudulent features given by the attacker instead of genuine values produced from the sensor device.
1.4.4 Loopholes in the graphical based authentication

In the graphical based authentication, [Xiaoyuan 2005] the main loophole or the disadvantage is that it is not as user friendly as text based authentication. Also it is not easy for the aged people or handicapped people to implement it. Also it is a bit difficult to produce the same design or same pattern at the time of login.

1.5 Rationale

In terms of security, authentication has always been the first line of defense. [Almuairfi 2011] Authentication mechanisms have been evolving since many years. Since the traditional authentication mechanism which is the text based authentication came into existence, researchers have been trying to propose various authentication mechanisms which provide complete security. Researchers have tried extensively to propose an authentication mechanism which is not complex and at the same time provide complete security. But nevertheless, there has not been a single authentication mechanism till date which has provided complete security. The attackers have also been evolving at the same time and have been creating new mechanisms or ways to crack the user’s authentication. Thus it has always been a challenge to produce a complete secure authentication mechanism.

The puzzle based authentication method proposed in this paper is a type of graphical based authentication. There have been some graphical based authentication mechanisms in the past but they were not completely secure and user friendly. The puzzle based authentication proposed in this paper takes a hint from the earlier versions. In this approach, care is taken that the puzzle provided to the user is not very difficult or complex. Also there has not been an authentication scheme which has server monitoring
continuously over it. There have some authentication methods which had some kind of additional security but no authentication method had a server completely monitoring it. Thus a graphical authentication scheme with server monitoring would provide great amount of security. This idea has been put into the puzzle based authentication method. A decent intelligent server is merged along with the puzzle strategy.
2. NARRATIVE

2.1 Problem Statement

As the discussion has been made in the introduction, there has been no authentication method which had server surveillance. [Wiedenbeck 2005] There have been some graphical based authentication methods or some puzzle based mechanisms but none of them had a server which continuously monitors the users’ activities. If the server would continuously monitor what the user or the client is doing, it would help a great deal in increasing the security of the user.

The traditional authentication methods are all susceptible to some kinds of attacks like the guessing attack, dictionary attack, key-logger attack, man in the middle attack, replay attack and many other attacks. In order to overcome this, the graphical based authentication was developed. The graphical authentication would provide more security as it is less vulnerable to the attacks. Even then, there has not been a graphical authentication mechanism which has been user friendly. There has not been a graphical authentication method which is not only easy to solve but also provides maximum security.

Even in the graphical based authentication, there has not been a puzzle type mechanism wherein the user would find it interesting and easy to solve. In another words, there has not been a puzzle based mechanism which is merged with the server surveillance to provide in depth security to the user. This has been the problem which is addressed in this proposed project.
2.2 Motivation

In today’s scenario, each user is having important information or confidential data in his email account or any other account. There have been reports generating daily that many users’ data is getting leaked or their resources are getting accessed by the attacker. This is causing a huge problem to the users. Sometimes in the online bank accounts, there have been innumerable cases wherein the users’ security is compromised and the attacker got access to the resources. This would cause a drastic problem to the users because they might lose huge amounts of money or they might also lose confidential data which is very important.

It might also happen that an attacker would want to access the personal or private information of the users. There have been attackers trying to know the personal details or there have been some cases where the attackers would just spy the users’ activities. This has been causing many problems to the users personally as well as professionally. There are also some attackers or hackers who would try to crack the user’s authentication mechanism for the fun of it. They find it extremely fun to work with or they find it something to boast about.

All these mentioned cases have been happening because of one reason which is authentication. Since the existing authentication mechanisms are not secure, the users have been easily getting access to the users’ activities. This has been the main motivation in pursuing with this project.
2.3 Scope

The purpose of developing this paper is to produce a puzzle based authentication mechanism with server surveillance. A graphical interface would be created and both the server and the client applications would be developed. The user would have his security upheld with the help of the puzzle as well as the server application. Then two cases would be presented. In the first case, a genuine user would try to log in and in the second case, an attacker would try to log in. The events and actions which would happen when these two cases happen would be discussed. The project developed will block the attacker and would provide the user about the details of the attacker.

2.4 Functionality of the project

This proposed project can have various functionalities. The project can be used in various places. This project can very well work on the LAN (Local Area Network) or the WAN (Wide Area Network) provided the required software is installed. Normally, in schools, colleges, banks, offices and other places where a LAN is used, this project would be very helpful. When the server application and the client application of this project would be installed in the computers connected to LAN, the genuine users’ security would be protected. An attacker or a fraudulent person would not be able to access the clients’ resources. If any signs of an attack take place, the server which would monitor continuously would immediately notify the genuine user that something wrong is going on.

Also, the proposed project can be used as an alternative to text based authentication in many real time applications. It would provide more security and the server would notify the genuine user if anything wrong is going on. In this way, the user
would have his security held and even if some kind of an attempt to attack takes place, the user would immediately know about it
3. PROPOSED SYSTEM DESIGN

3.1 A puzzle based authentication mechanism with server monitoring

This project is developed as a graphical based authentication mechanism by using the puzzle strategy as well as a decent intelligent server. The main aspects that the proposed project stresses on are as follows:

- **User friendliness:** By noticing the earlier methods, enough care has been taken to see that the puzzle based authentication method proposed in this paper is easy to understand and implement. Any user with limited knowledge of computers can easily use this authentication mechanism.

- **Log details:** The proposed project would have a log of all the details of users’ activities. The details like the IP address, host name, the movement of the users in the puzzle strategy would be recorded by the server.

- **Attack detection:** The proposed application will have the capability to detect if any attack takes place and would block the access if it finds any. Thus the security would be upheld.

- **Reporting:** In this proposed project, the server would monitor all the details and would report everything to the user. It would report the hostname, any fraudulent activities to the genuine user.
3.2 Framework

Normally, puzzle based strategies have been very interesting and every person might have solved or come across a puzzle in his or her lifetime. Normally, puzzles have been used in a gaming zone or for entertainment purpose. The usage of puzzles in authentication would also bring in interest among the users. This idea was the main reason to implement this project. In order to make a puzzle based authentication mechanism, a puzzle had to be implemented. Also, each user should have an unique puzzle. Thus building some puzzles and merging it with the authentication became a challenge. Thus the puzzles have been developed and merged with the authentication scheme in this proposed project.

3.2.1 Steps in the project development

The steps involved in building this project from the inception are given below in brief:

1. Building a graphical user interface
2. Building a database
3. Creation of the client and server applications
4. Linking the applications with the database
5. Creating modules
6. Setting up the server and the client

3.2.2 System requirements

Normally any computer installed with SQL 2005 and visual studio 2008 will be able to run this project. Sometimes the windows 7 64 bit version and also the 32 bit
version are having some compatibility issues. This application runs best on windows XP operating system. The basic system requirements that are required in order to run this project’s application will be given below:

**Software requirements: (Minimal requirements)**

Front End/GUI Tool : Microsoft Visual studio 2005  
Operating System : Windows Family  
Language : C#.NET  
Back End : SQL SERVER 2005

**Hardware requirements: (Minimal requirements)**

Processor : Pentium dual core  
RAM : 1 GB  
Hard Disk Drive : 80 GB

**3.3 Proposed Mechanism**

The puzzle based authentication method is the proposed mechanism in this project. The architecture of the proposed mechanism can be seen in figure 1.
3.3.1 Working

As it can be seen in figure 1, there will be two main applications. One is the client application and another is the server application. The server application’s main role is to monitor the client application. Initially the client will have to register with the server. The client is the user who wants to get access with the server.
Registration phase

While registering, the server would present the user with registration details along with the puzzle. The user can solve the puzzle by himself or by taking the help of the server. The server would provide a hint to the user about how to solve the puzzle. After solving the puzzle, the user gets registered. Now the server would monitor the time taken by the user to solve the puzzle and store it in the database.

Login phase

At the time of login, the user would first be asked to enter the hostname of the computer. Each computer would have a unique hostname. After entering the hostname, the server would record the hostname. Then the user would be presented with the same puzzle which he solved during the registration phase. The user would get the same time in which he solved the puzzle during the registration phase. If the user solves the puzzle in the given time, the user would gain access to the server. If the user does not solve the puzzle in the given time, the server would block the access. Thus the user would not have the confidentiality or the integrity of the data compromised.

Monitoring and Reporting

When the user or the attacker does not solve the puzzle within the given time, the server would notify the user immediately through email that an attacker attempted to access the user’s account. The server would also monitor continuously and keep track of the IP address of the user, the movements of the user, the host name and the time. If the user accesses the server from any other hostname, the server would email the user saying that an access has been made from the particular hostname.
Thus in this proposed project, a simple and user friendly puzzle is given to the user who solves it and uses it as his password. The server continuously keeps track of all the activities and lets the user know if any fraudulent attempt to gain access to server takes place. The server would record complete details and store them in the log. Thus a very secure puzzle based authentication method with server surveillance is developed in this project.

3.4 System design

The proposed application design process will be discussed in this section. Various UML diagrams explaining the design of the proposed application will be presented and explained.

3.4.1 Dataflow diagram

The dataflow diagram explains how data moves or flows in a system. The dataflow diagram concerning the proposed project can be seen in figure 2.
As it can be seen in figure 2, the details of the data flow in this proposed application is shown graphically. The client would register with the server and server would analyze the clients’ steps and the server would decide to give access or to not give access.

3.4.2 Use case diagram

The purpose of the use case diagram is to graphically represent the functionality of the system with regard to actors, their aims (shown as use cases) and any kind of dependencies arising between the particular use cases. The proposed system’s use case diagram can be seen in figure 3.
3.4.3 Sequence diagram

The sequence diagram is a type of interaction figure which shows how various processes operate with each other and in what order they operate. The proposed system’s sequence diagram can be seen in figure 4.
3.4.4 Collaboration diagram

Collaboration diagrams are similar to sequence diagrams which show how object would interact over some period of time. But instead of presenting the sequential events on the layout, collaboration diagrams would represent the sequence by giving a number.
to each message in the diagram. This would make it simpler to show which objects are grouped together.

Figure 5: Proposed system’s collaboration diagram
4. FUNCTIONALITIES OF THE APPLICATION

The proposed application’s modules would be discussed in this section. The modules would be explained with the respective screenshots.

4.1 Modules Description

The proposed project consists of two modules. They are the client module and the server module. Both the modules would have different functionalities.

4.1.1 Client module

The client can be any user who wants to get access to the server. All the actions of the user would be performed in the client module. The client module will have various functionalities. The functionalities of the client module are given below in a sequential order.

- Getting the hostname of the user
- Registration stage
- Getting the credentials of the users
- Puzzle solving
- Login stage
- Access with the server

The mentioned functionalities would be provided with the screenshots and would be explained in detail in accordance with the respective screenshot.

- Getting the hostname of the user

The client module would initially ask the user to provide his or her hostname.
As it can be seen in figure 6, the user would be required to provide the hostname of the computer initially to proceed further. Every computer would have a unique hostname and the user should provide the exact hostname of the computer to proceed further.

- New user registration

In figure 7, the new user registration can be seen. If the user is not registered and has to register, the user needs to click on new user to register.
Figure 8: Registration process

In figure 8, the registration process can be seen. Once the user clicks the ‘new user’ button, the user would be directed to this page. The user needs to provide his credentials and then register.
• **Puzzle solving**

After entering the credentials, the user would be presented with a puzzle. The puzzle needs to be solved in order to finish the registration.

![Figure 9: Registration process](image)

As it can be seen in figure 9, the user would be provided a puzzle. The user can solve the puzzle in his own steps or use the hint provided by the server. The user would finish solving the puzzle in a given time and this time would be recorded by the server.
• **Login stage**

At the time of login, user would have to give his username initially. This can be seen in figure 10.

![Figure 10: Login stage](image)

As seen in figure 10, the user would have to provide with the username with which he registered during the registration phase. The user will then proceed to the puzzle authentication when the user submits his username.

• **Access with the server**

After logging in and solving the puzzle, the user can access the server in order to send or receive files.
As seen in figure 11, the user would get access to the server after a successful authentication. Here the user can download or view files from the server.

4.1.2 Server module

The server is the computer or the system which gives access to the clients. The server can be connected to many clients. The server module will also have important functionalities. The functionalities of the server module are as follows:

- Keeping track of client details
- Keeping track of registration details
- Keeping track of the puzzles allocated to the users
- Keeping track of users’ movement
- Sending email in case of an attempted attack
• **Keeping track of client details**

The server would initially keep track of the client from the registration stage. The screenshot given in figure 12 will give a detailed understanding.

![Client Details](image)

**Figure 12: Server keeping track of client details**

As it is seen in figure 12, the server would record the IP address of the user, the protocol used and also the time at which the action was made. This helps in getting more information about the attacker when an attack takes place.

• **Keeping track of registration details**

The server would keep track of all the registered usernames and their credentials.

![Register Details](image)

**Figure 13: Server keeping track of registration details**
As it is seen in figure 13, the server would have the registration details of the users who have registered. All the usernames and the users’ credentials will be recorded.

- **Keeping track of the puzzles allocated to the users**

  The server would maintain a history of the puzzles provided to the users. The way to solve the puzzle and the puzzle assigned to the user would be maintained in the records. The screenshot in figure 14 will give a better understanding.

![Figure 14: Server keeping a record of the puzzles allocated to the users](image)

As seen in the figure 14, the server would maintain the image puzzle allocated to the particular user. Also under the instructions tab, the solution to solve the puzzle will be given. Thus, the server will have a unique puzzle for each user and the details would be recorded.

- **Keeping track of the users’ movement**

  The server would keep track about the users’ steps when they solve the puzzle. The screenshot in figure 15 will give a better understanding about this.
As it is seen in figure 15, the server would record the IP address and the moves of the user while solving the puzzle. The moves can be seen under the movement tab. Normally, a genuine user would know the solution to solve the puzzle and would come with the correct steps but an attacker would try different moves to solve the puzzle. The server would record all the moves of the users. Thus if any attacker makes suspicious moves, it can easily be recognized.

- **Sending email in case of an attempted attack**

  The server would keep track of the time when the user is solving the puzzle. However, when the user will not be able to solve the puzzle in the given time, it could mean that an attacker is trying to login. If this happens, the server would immediately notify the user by sending an email immediately. By doing this, the user would be kept updated about his security and would take necessary steps when he gets notified.
5. TESTING AND IMPLEMENTATION

5.1 Testing

- Testing is the procedure to find out whether any errors arise while testing the application.
- Testing is really important in terms of software engineering.
- The main aim of software testing is to prove the developers and customers that the particular software is good to use. In another words, testing is done in order to build confidence.
- Testing consists of a number of activities which can be planned initially and conducted in a systematic manner.

5.2 Types of Testing

The following are the types of the testing:

- White box testing
- Black box testing
- Unit testing
- Integration Testing
- Validation Testing
- Output Testing
- User acceptance testing
5.2.1 White box testing

- The white box testing can also be referred to as glass box testing. The white box testing makes use of control structure in the procedural design to get the test cases.

- With the help of white box testing, a tester can make test cases that does the following things:
  - It makes sure that all the parts present in the module have been used at least once.
  - The logical decisions will be analyzed with the true criteria and false criteria.

5.2.2 Black box testing

- The black box testing can also be referred to as the behavioral testing. The black box testing stresses mostly on the software’s functional requirements.

- The black box testing is an approach of complementary type to present different type of errors from the white box testing errors.

- Black box testing makes use of some input criteria to fully exercise the program’s functional requirements.

5.2.3 Unit testing

In unit testing, every module would be tested and then would be grouped with the system. Unit testing stresses to test on the tiniest unit of the software to make sure its working. It can also be referred to as the module testing.
Each module presented in the system would be tested separately. This testing would be done at the programming time itself. In this testing process, it is made sure that every module would work as per the requirements. The errors are easy to find in the initial stage itself rather than the final stage.

5.2.4 Integration testing

Integration testing stresses on the fact that data may be lost over an interface. A particular module can have a drastic effect on remaining sub functions and when combined will not give the required functionality. The integration type is like the systematic testing to find out the uncover errors inside the interface. The testing will be done with a small sample of data. The system which is developed will be tested with this sample data whether it will run successfully or not. With the help of integration testing, the system’s overall performance can be evaluated.

5.2.5 Validation testing

When the black box testing is at its peak, software is grouped as one package, interface related errors are corrected, the validation testing begins. There can be many definitions for validation testing. In simple words, validation will be successful only when the software produced will be as per the satisfaction of the customer. So the validation tests will be confirming whether the final user will be satisfied with the product or not.

5.2.6 Output testing

After the completion of the validation testing, output testing would be performed. The output testing would be performed because every system would want the output to be
as per the specified requirements. The output testing will prove whether the output is satisfactory or not.

5.2.7 User acceptance testing

This testing is used to find out whether the application developed is user friendly or not. The user acceptance testing will be successful if the users can access the application easily.

Types of testing performed in this project

The following testing methods have been performed in the proposed project and were successful:

- Unit testing
- Integration testing
- Validation testing
- Output testing
- User acceptance testing

5.3 Test cases

The proposed project was tested for all the test cases sequentially. The following test cases were tested:

- Verifying the hostname
  - For correct hostname
  - For incorrect hostname
• Verifying the registration phase
  ▪ For successful registration
  ▪ For unsuccessful registration

• Verifying the login phase
  • For a genuine user
  • For a fraudulent user

• Verifying the server monitoring
  • IP address
  • Registered users
  • Users moves

• Verifying server reporting
  • Sending email when user logs in
  • Sending email if user makes more moves than usual
  • Sending email if the puzzle is not solved

• Verifying file access with server

Test cases

5.3.1 Verifying the hostname

Now the hostname would be tested. If the user provides correct hostname, the user can proceed but if the user gives incorrect hostname, the user will not be able to proceed.
Correct hostname

![Figure 16: Hostname of the computer](image)

![Figure 17: User entering the correct hostname of the computer](image)

As it is seen in figure 16 and figure 17, the user types in the correct hostname of the computer. By typing the correct hostname, the user proceeds to the next step of the process.
Incorrect hostname

As it can be seen in figure 18, the user would not be able to proceed further if incorrect hostname would be provided.

5.3.2 Verifying the registration phase

In the registration phase, the user would be needed to provide his credentials and then solve the puzzle. The user would be given a puzzle and also a solution to it in the form of a hint. The user can use this hint and solve the puzzle. The time will also be recorded when the puzzle is getting solved. The user would be able to finish the registration successfully only if the puzzle is solved. The two scenarios for a successful registration and unsuccessful registration are presented in the following screenshots.
Successful registration

Figure 19: Successful registration by the user

As it can be seen in figure 19, the user filled the credentials and solved the puzzle correctly and thus getting success. Thus a successful registration is done in figure 19.
Unsuccessful registration

Figure 20: Unsuccessful registration

As it is seen in figure 20, if the user does not solve the puzzle, the registration would not be finished. The user would have to solve the puzzle to finish the registration successfully. But in figure 20, the user did not solve the puzzle; hence it is an unsuccessful registration.
5.3.3 Verifying the login phase

This is the most important aspect of the proposed project. In this section, the verification of the login phase will be done. The registered user would be verified by presenting him with the puzzle which he solved in the registration phase. The user should be able to solve the puzzle in the given time. Now two scenarios would be presented; one for a genuine user and the second one for a fraudulent user.

For a genuine user

![Figure 21: User logging in](image1)

![Figure 22: User solving the puzzle successfully](image2)
As it is seen in figure 21 and figure 22, the registered user would login and then the user would be presented with the respected puzzle. The time would be running on top of the window. The time which would be running on top of the window is the time taken by the respective user in solving the puzzle during the registration stage. The user should be able to solve the puzzle within that given time. In this case, the user solves the puzzle and hence logs in successfully.

For a fraudulent user

Figure 23: Fraudulent login
As it is seen in figure 23, the user would not solve the puzzle within the given time and thus the access would be blocked and the server would respond saying that the user maybe an attacker. Thus this is an example for a fraudulent user who tries to login.

5.3.4 Verifying the server monitoring

In this section, the testing was done to verify whether the server monitoring was correct. The server plays a very vital role in the proposed project. The server would be continuously monitoring the activities of the users. The server will record the IP address, time, and users’ moves while solving the puzzle.

Recording the IP address

![Image of IP configuration output]

Figure 24: User’s IP address
Figure 25: Server monitoring the user’s IP address

As it is seen in figure 24, the user’s system has the IP address 10.0.2.15. As shown in the figure 25, the server records the correct IP address of the user. The server also records the protocol and the time of access. In the figure 25, the protocol is of TCP type. Thus the verification of server monitoring is done.

Registered users

Figure 26: Server maintaining a list of registered users
As it can be seen in figure 26, the server has the registered user’s name recorded and also the puzzle allocated to the particular user is recorded. If more number of users register, the server would maintain a record of more users.

Users’ moves

<table>
<thead>
<tr>
<th>IP Address</th>
<th>UserName</th>
<th>Movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.2.15</td>
<td>anuragbm</td>
<td>2,3,7,11</td>
</tr>
</tbody>
</table>

**Figure 27:** Server monitoring the moves of a genuine user

<table>
<thead>
<tr>
<th>IP Address</th>
<th>UserName</th>
<th>Movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.2.15</td>
<td>anuragbm</td>
<td>2,3,11,15,2,7,15,15</td>
</tr>
</tbody>
</table>

**Figure 28:** Server monitoring the moves of an attacker

In figure 27, the server records the moves of the genuine user and in figure 28; the server records the attacker’s moves. It can be recognized from figure 28 that the user’s moves are more than usual and hence the moves are of an attacker. Thus the server successfully records the moves of the users.
5.3.5 Verifying server reporting

In this section, the server was tested whether it sent reports in all the required scenarios. The server sends a report to the user whenever he logs in, whenever the user exceeds the number of moves and also if the user does not solve the puzzle within the given time. Now these scenarios would be verified.

Sending email when user logins

Figure 29: Server sending email to the user when the user logins

As it can be seen in figure 29, the server would send an email to the user as soon as the user logins. The server would also notify the user of the hostname of the computer from where the user logins.

Sending email when user makes more moves than usual

Figure 30: Server sending an email to the user when more moves than usual take place
As shown in figure 30, the server would send an email to the user saying that the user exceeded the number of steps. The server would send this email if the user makes more moves than the usual number of moves.

Sending email if the puzzle is not solved

As shown in figure 31, the server sends an email to the user when it notices that the user failed to solve the puzzle within the given time. The server would assume that it is an attacker and would notify the user by sending him an email right away along with the hostname of the computer.

**Figure 31: Server sending an email when puzzle is not solved**

As shown in figure 31, the server sends an email to the user when it notices that the user failed to solve the puzzle within the given time. The server would assume that it is an attacker and would notify the user by sending him an email right away along with the hostname of the computer.

5.3.6 Verifying file access with server

After a successful login, the user can connect with the login and download the required files. This can be very useful in computers connected in a local area network.
Figure 32: File access with server

As shown in figure 32, the file access with the server would take place after a successful login. The user can download the required file from the server or the user can view the required files in the server. This can be implemented in a local area network or a wide area network.
6. COMPARISON WITH OTHER AUTHENTICATION METHODS

Table 1: Comparison of the authentic methods

<table>
<thead>
<tr>
<th></th>
<th>Dictionary attack</th>
<th>Key-logger attack</th>
<th>Man in the middle attack</th>
<th>Replay attack</th>
<th>Video recording</th>
<th>Continuous monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text based authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Not present</td>
</tr>
<tr>
<td>Biometric authentication</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Not present</td>
</tr>
<tr>
<td>Token based authentication</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Not present</td>
</tr>
<tr>
<td>Graphical authentication</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Not present</td>
</tr>
<tr>
<td>Proposed authentication</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Present</td>
</tr>
</tbody>
</table>

Note

Yes - It means that the respective authentication method is susceptible to the given attack.

No – It means that the respective authentication method is not susceptible to the given attack.
As seen in table 1, the proposed method is susceptible to video recording attack but it has continuous monitoring present in it which makes it unique and more secure. Even if an attack takes place, the user would get information and the user would do something to prevent the attack.

6.1 Advantages

The proposed authentication method overcomes most of the attacks like the dictionary attack, key-logger attack, man in the middle attack, replay attack and some other minor attacks. The biggest advantage of the proposed method is that it has a continuous monitoring device which informs the user about the activities taking place from the user’s account. In this way, the user can know the source of the attack in case an attack takes place.

6.2 Disadvantage

The proposed authentication method is susceptible to video recording attack. This can be taken as a base for future work where this disadvantage can be improved upon.
7. CONCLUSION AND FUTURE WORK

The puzzle based authentication method proposed in this paper has overcome many attacks which exist in the traditional authentication methods. The proposed method is also user friendly and can be used by any person with limited knowledge. Also the unique aspect of this project is that a continuous monitoring server is present which tracks all the activities of the user and would also inform the user about the activities. Thus the user can have complete information if an attack takes place.

The proposed method is susceptible to video recording attack. This can be something which can be worked upon in the future. Thus the future work can be aimed mostly to overcome the susceptibility to the video recording attack.

The future work can be concentrated on the time aspect. Rather than giving a time limit, the system should be able to judge whether the moves of the user are genuine and if genuine; the system should provide more time. Also in the future work, the system should provide user the option to select an image that the user wants and create a puzzle with that particular image.
BIBLIOGRAPHY AND REFERENCES


