International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 423 – 428

Secure E-mailing System Using Pair Based Scheme and AES with Session Password

Mandar A. Joshi, Vikrant S. Shendarkar, Khushbu Solanke, Monika Chandelle, Nidhi Iche
Department of Computer Science and Engineering, Sant Gadge Baba Amravati University,
P.R. Pote College of Engineering and Management Amravati, Amravati, Maharashtra, India

***Abstract*—** In early days Textual passwords are used for security of session but these passwords are vulnerable to the various attacks like Dictionary attack, Shoulder surfing, eves dropping, etc. Further graphical passwords and bio-metric passwords are invented. These two techniques are good performer but they have their own disadvantages. Such as requires extra time for login and more cost respectively. Thus we proposed a session password scheme in which the passwords are used only once for each and when session is terminated the password is no longer in use. The proposed of session password scheme uses Pair Based Authentication scheme for generating session password. In every Data communication system security to data is primary aim. Data security can be provided by many ways. This Paper gives a design of effective security for data communication in network by AES algorithm for encryption and decryption.

Keywords- *AES, Brute Force Attack, Dictionary attacks, Pair Based scheme, Secret Pass Key*

*****

I. INTRODUCTION

In the lifestyle of humans, Social networking has acquired one of the most important places. As it allow us to connect with long distance persons. There are many social networking services are available. E-mailing service is one of the most important services from them. Due to good service and strong security mailing service has got peoples attraction. So In this paper we have focused on security of mailing systems.

The Security is mainly given by two mechanisms which are **Authentication** and **authorisation**. what is authentication and authorisation.

Authentication verifies **"who you are?**" It is a process in which the input provided by user are compared and matched with the file stored in a database of authenticated users.

For example the simple authentication is done every time when you log in to your mail account from the different computer or other device.

Authorisation gives information about what you are authorised to do. Authorisation is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular.[1]

Another question arises "**What is session?"** In computer science or in particular networking, the session is a semi-permanent interactive information interchange. That is nothing but the interaction of informative communication within the limited time period.

What is **session password?** Now the password that is being used for the authentication for that session which means that the password is being used for the limited period of time is session password. For every session there will be a new session password.

Encryption is a technique in which data is represented in unreadable form. It is process of hiding and representing data into secured manner and that can only be accessed by authorized users. Encryption is done by using cipher. This cipher contains encrypted data block.

Decryption is the opposite process of encryption. In decryption process encrypted data is converted back into its original form, so it can be understood.

The scheme **Pair Based Authentication** helps user to keep the login process secured. It also removes the disadvantages faced by various schemes invented before. Also **AES** provides advanced security to the data. [1]

II. BACKGROUND

Various authentication schemes were proposed for more secured authentication. Every scheme consists of new inventions and updates. Some of the related terminologies are:

1. Token Based Authentication

Token based authentication is one of the earliest security techniques which provide easy authentication to user. This method of authentication provide authentication to user who want to login to server, network or a system. For authentication purpose "Token" is provided by server and security token is provided by user.

An authentication is successful if a user can prove to a server that he or she is a valid user by passing a security token. These tokens have validity. Token based technique has examples such as key card, bank card. It is good technique of authentication but it has some drawbacks. Such as:

- Less security and due to that it can be stolen.
- More chances of misuse of hacked token.
- It involves additional cost for token and token replacement process. [1], [2].

2. Biometric Based Authentication

Biometrics is a technology which uses physiological or behavioral characteristics to identify or verify a person. In this system human body parts are used for authentication. Typical characteristics used for authentication include fingerprint, face, and iris. Fingerprints are widely used biometric type.

Biometric scheme works according to modules. First user have to register input data to biometric sensors. These sensors

proceed that input to biometric databases. Here feature of input is identified and stored into databases. At the time of authentication matching of input feature is done. If it matched with stored input then authentication is successfully done. Due to some drawbacks this scheme is not widely used for authentication. Some drawbacks are listed as follows :

- The performance of biometric systems is not ideal.
- Biometric systems still need to be improved in the terms of accuracy and speed.
- Biometric systems are more expensive.

Some of the known types of Biometric system are Fingerprint scan, Iris scan, Retina scan.[3], [4].

3. Knowledge Based Authentication

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords. Knowledge based authentication scheme is consist of two types: Static Authentication and Dynamic Authentication. Knowledge based Authentication is also called as KBA. KBA involves both Graphical authentication and Text based Authentication. It is divided into three categories:

1 Recognition-Based Graphical Technique
2 Recall-Based Graphical Technique
3 Hybrid Authentication Technique

Above mentioned techniques are used in knowledge based authentication scheme. By using this strong security can be provided to session. But they also have their own drawbacks.

3.1 Recognition-Based Graphical Technique

Recognition based technique require the user to identify and recognize the secret, or part of it, that the user selected before. Generally during password creation the users are required to memorize a series of images, and then must recognize their images from among decoys to log in. This technique is widely used in all over the world as it serve best security against the phishing hacking attack. But it has some dislikes which applied some break on success of this technique.

- In Recognition based graphical technique user must have to remember all the password pictures.
- This Technique is highly suffered by shoulder surfing attack.

3.2 Recall-Based Graphical Technique

Using recall-based techniques, a user is asked to reproduce something that user has created or selected earlier during the registration stage. The problem with the Grid based methods is that during authentication the user must draw his/her password in the same grids and in the same sequence. This technique is categories into two types: Pure Recall-Based Technique and Cued Recall-Based Technique.

Some drawbacks of this technique are:

- It is really hard to remember the exact coordinates of the grid.
- Small and less password size.[4].

3.3 Hybrid Authentication Technique

In this Technique, the authentication will be typically the combination of two or more schemes. i.e. Graphical and textual. Different colors are also used in this technique. These schemes are used to overcome the drawbacks of a single scheme, such as spyware, shoulder surfing and so on.

During registration, user rates the colors in the first method or enters his password in the second method. During login phase, the user has to put the password based on the interface displayed on the screen. The entered password verifies by the system by comparing with content of the password stored and session password. During recovery phase, if user forgets his password, he may recover the password by answering security questions which user had selected during registration phase. Dislike of this technique is that it is too long process and has to do more unnecessary task.

Above explained techniques provides different level of security to session or an authentication process. Some of them are out dated techniques and some are latest. The out dated techniques had provided us an very good security service but as time runs up and new inventions done in network security domain which lags them behind. Other Newly invented services such as Text based and Graphical based authentication techniques are presently in use. Now a days Hackers and network thief are smart enough to break the security of graphical password and text password. So due to that network needs next generation security services. I this paper we have used An best authentication scheme for authentication and session security and best encryption for data security.

Pair authentication scheme is one of the most efficient method of authentication and it provides highest security to network. In this paper this scheme is applied on session. This increases the level of security. Encryption to data avoids all the thief operations. AES provides best encryption security and it is proved by NIST (National institute of standard and technology).

III. AIM, OBJECTIVES AND SCOPE

The most important Aim of this system is that to provide an efficient option to all the orthodox login systems and authenticate the system at highest level.

To design a secure authentication system for online authentication platform which will robust, user friendly and resistance to all the hacking attacks.

Another important aim is, To design a virtual session password keypad which will be anti-screenshot able. Also secured from Shoulder surfing and logger attacks. Efficient, highly secured and user friendly system is the preference.

The Objectives of this system are:

- To develop a secured e-mailing system in which emails will be stored in encrypted format.
- To develop Pair based authentication system as the preventive measure for shoulder surfing attack and other too.

 ISSN: 2321-8169
423 – 428

- To improve security of current mailing system and develop user friendly but strongly secured mailing system.

The Scopes of the System are:

In the Pair based authentication the display changes after every session. Due to this it is difficult to hack the password. Thus, the scheme help user to keep login process secured. This system can be used as security measure for Net backing, online payment application, online documentation process, cloud storages.

IV. SYSTEM DESIGN

Pair based authentication system and AES algorithm is the two techniques used in this paper foe authentication security and data security respectively. Pair based authentication technique is used to create session time password. This makes system more efficient. On other hand AES algorithm is used to apply encryption and decryption to the data. AES is strongest algorithm technique for data security. Following we have the complete system flow of Pair based Authentication scheme and AES execution. This flow chart shows the complete flow of system, i.e. from User Registration to the Logging Out of system.[1], [2].

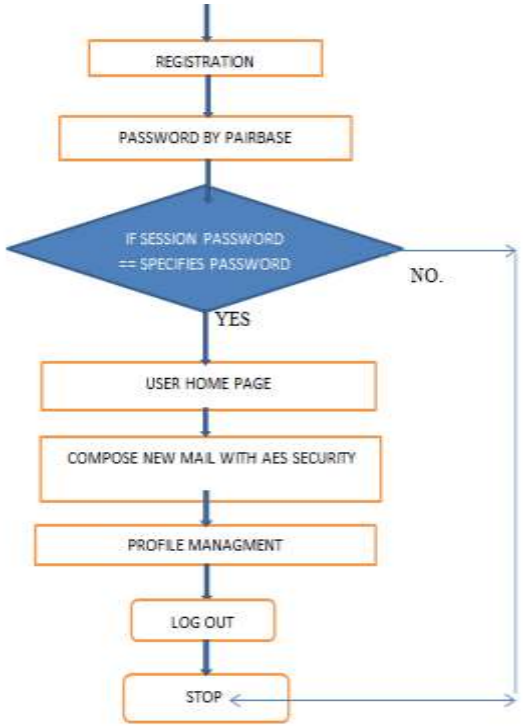

Figure 1: Complete Execution flow of Authentication system.

V. PROPOSE SYSTEM

Our system is proposed as an alternative to other password based techniques. The current system present for authentication has several loop holes. We are trying to eliminate password guessing through dictionary attacks, brute force attack and guessing attacks. Our objective is to overcome the known weakness of traditional passwords. It is also designed to make the passwords more memorable, easier for people to use and also more secure.

This system gives output in the form of secured authentication and user data. It uses AES encryption technique. AES algorithm works on data encryption in which it has multiple rounds of encryption. AES uses keys to provide security to data. Multiple encryption rounds and secrete key encrypt the data in unreadable form. For decryption purpose same method is used.

As this is E-mailing system, therefore this system will give all the basic services related to mailing work. Such as Login/Logout, Communication and History.

VI. IMPLEMENTATION

A. Pair Based Authentication Scheme:

In the course of registration, the user submits the secret pass. The minimum length of the secret pass is 8 and it should contain even number of characters. During the primary level authentication, when the user chooses the pair-based authentication scheme, an interface consisting of row X Colom grid is displayed. The grid contains both alphabets and numbers which are placed at random and the interface changes every time. The mechanism involved in the pair-based authentication scheme is as follows: Firstly, the user has to consider the secret pass in terms of pairs. The first letter in the pair is used to select the row and the second letter is used to select the column in the row X Colom grid. The intersection letter of the selected row and column generates the character which is a part of the session password. In this way, the logic is reiterated for all other pairs in the secret pass. Thereafter, the password inputted by the user i.e. the session password is now verified by the server to authenticate the user. The scheme Pair Based Authentication helps user to keep the login process secured. It also removes the dis-advantages faced by various schemes invented before.[5],[8].

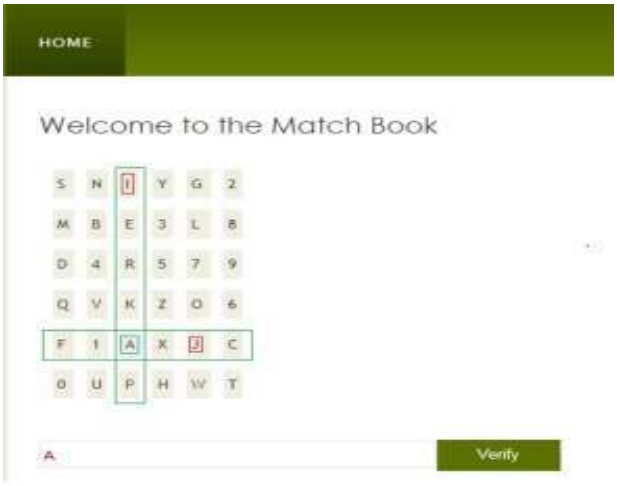

Figure 2: Pair Based Grid Authentication

The scheme Pair Based Grid Authentication consists of three phases: Registration, Login and Verification Phase. In the Registration phase User registers the password. When login is to be performed users have to enter the credential from the

 ISSN: 2321-8169
423 – 428

shown grids. The system then verifies the password with the stored database password. As the system is designed to work with pair of characters only even length passwords are allowed.

Following is the execution Flow of AES algorithm. Which is shown in three parts as fig(a), fig(b) and fig(c) respectively.

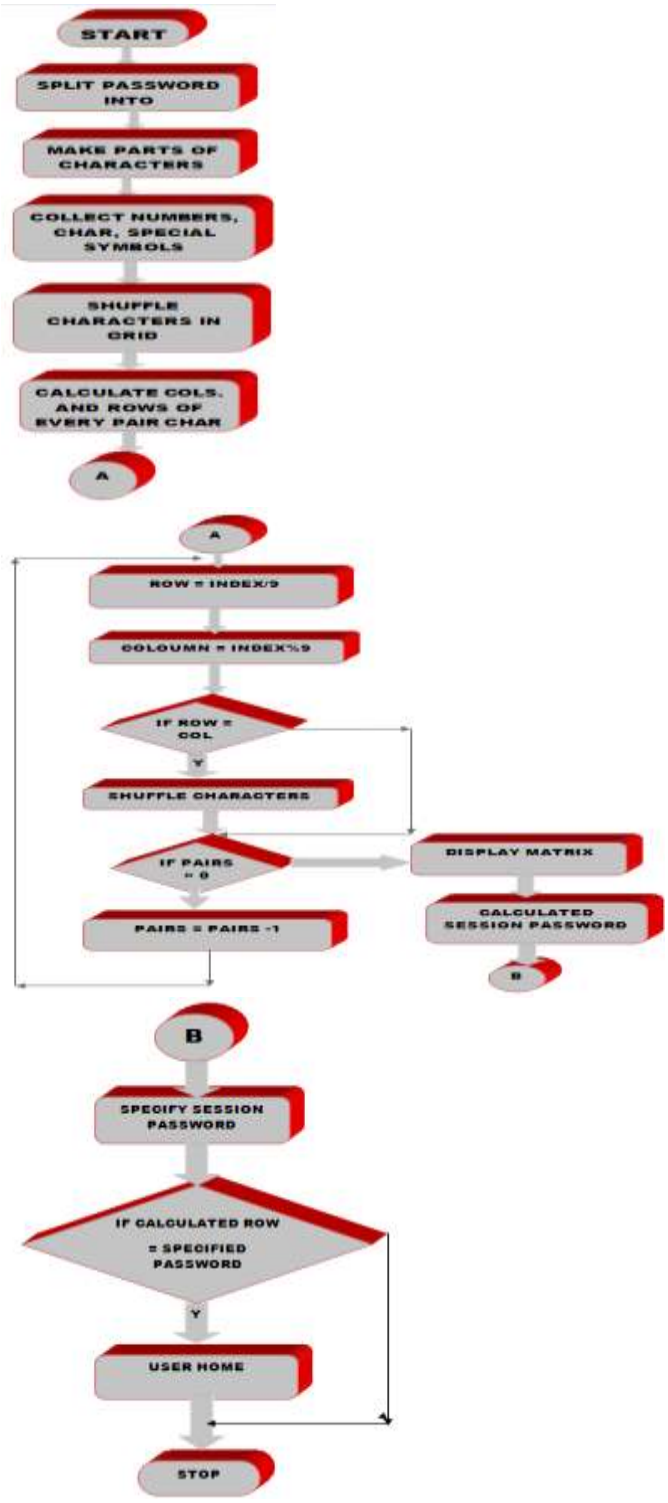

Figure 3: Data Flow Diagram of Paired Based System

B. AES Algorithm

The algorithm is based on AES Key Expansion technique. AES algorithm works on data encryption in which it has multiple rounds of encryption. AES uses keys to provide security to data. Multiple encryption rounds and secrete key encrypt the data in unreadable form. For decryption purpose same method is used.

- *Sub Bytes Step*

This step is same as Sub Bytes step of AES algorithm. In this step, each byte in the matrix is shuffled using an 8-bit substitution box. This substitution box is called the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF (28), known to have good nonlinearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points (and so is a derangement), and also any opposite fixed points. This step causes confusion of data in the matrix. S-Box Substitution is carried out separately for LPT and RPT. This is the first step of iterative round transformation. The output of this round is given to the next round.

```
public byte[ ][ ] subBytes(byte[][] state)
{
for (int i=0;i<4;i++)
{
for (int j=0;j<4;j++)
{
int row = getFirstFourBits(state[i][j]);
int column =
getSecondFourBit(state[i][j]);
state[i][j] =
sBoxSubstitution(row,column);
}
}
return state;
}
```

- *Shift Rows Step*

The Shift Rows step is performed on the rows of the state matrix. It cyclically shifts the bytes in each row by a certain offset. The first row remains unchanged. Each byte of the second row is shifted one position to the left. Similarly, the third and fourth rows are shifted by two positions and three positions respectively. The shifting pattern for block of size 128 bits and 192 bits is the same.

```
  shiftRows(byte state[][])
  {
  for(int i=0;i<4;i++)
  {
//cyclic left shifts ,i"th row, i"times
  cyclicLeftShift(i);
  }
}
```

- *Mix Columns Step*

In the Mix Columns step, the four bytes of each column of the

state matrix are combined using an invertible linear transformation A randomly generated polynomial is arranged in a 4*4 matrix. The same polynomial is used during decryption. Each column of the state matrix is XOR-ed with the corresponding column of the polynomial matrix. The result is updated in the same column. The output matrix is the input to Add Round Key.

```
public byte[ ][ ] mixColumns(byte[ ][ ] state)
{
for (int c=0;c<4;c++)
{
state [c]=matrixMultiplication(state[c], polynomial);
}
Return state;
}
```

- *Add Round Key*

A round key is generated by performing various operations on the cipher key. This round key is XOR-ed with each byte of the state matrix. For every round a new round key is generated using Rijndaell's key scheduling algorithm.

```
public byte[ ][ ] addRoundKey(byte[ ][ ] state,byte[ ][ ]
roundkey)
{
for (int i=0;i<4;i++)
{
for (int j=0;j<4;j++)
{
state [i][j]=doExclusiveOR(state[i][j],
roundkey[i][j]);
}
}
return state; [6], [7].
```

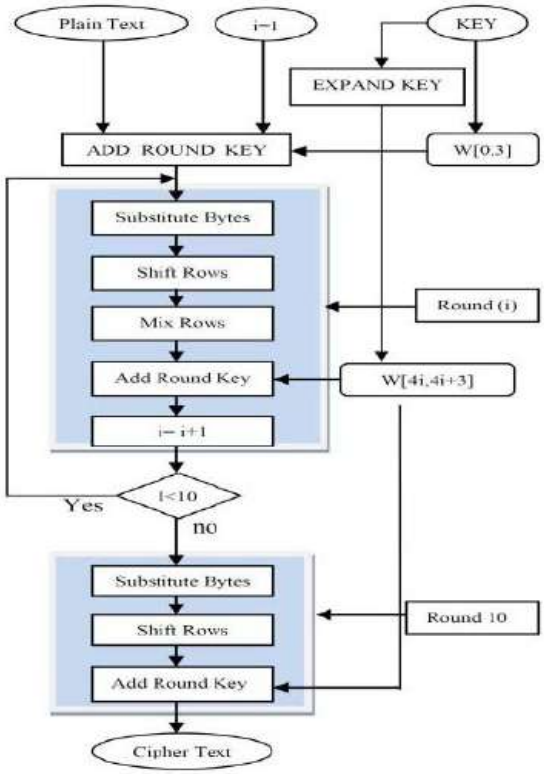

Figure 4: Flowchart of AES Algorithm.

VII. APPLICATION AND ADAVANTAGES

A. APPLICATION

- In mobile pattern lock, we use this system is more secure.
- In Military we use to secure confidential data.
- In Companies store secret data and all important information with maximum security.
- Also, we can use this system in Net banking, Online Payment Application, Online document storage, Online Photo storage and other such places.

B. ADVANTAGES

- ***Easy to register***

In this system new user can register. Then new user can register such as fill the data such as Username , E-mail address, birth date, gender, local address, city, mobile number, password, first name, last name etc.

- ***More secure***

Textual password scheme are when any user is enter the password then this password seen by other persons. In textual password scheme passwords should be easy to remember and the easy to cracked. But in graphical and pair-based scheme password guessing is not easily done. So it is more secure.

- ***Easy To Use***

This system is very easy to use because new user can register and use this method.

- ***Very Difficult To Hack***

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Passwords should be secure, i.e., they should look random and should be hard to guess, they should be changed frequently the password, also we avoid many dictionary attack and this methods are difficult to hack.

C. LIMITATIONS

- It takes more time for finding the intersection in grid.
- It might be difficult to remember all passwords, as we provide more security in this application.
- Condition of every password is that it must require 1 symbol, 1 special character.
- Encryption is applied to keys and attachment only.
- For accessing any mail user must have to know all the passwords and keys used in this application.

VIII. SUMMARY AND DISCUSSION

The below Table shows that all existing password authentication techniques. It consists of authentication techniques and its merits and de-merits. [1],[2],[5].

Table: Merits and De-merits of Authentication Techniques

Sr. No	Authentication Techniques	Advantages	Disadvantages
1	Pass faces	User can easily remember the password as it given in images.	Image based password is very long process user have to pass through selection of number of images.
2	DAS (draw-a-secret) scheme	There no need to store graphical database at server side.	During authentication the sequence can be changed or grids may be different as it is a drawing.
3	Triangle scheme	In this scheme the display is very crowd so not able to guess the password.	. As it has convex surface assigning process takes longer time and number of attempts.
4	Hybrid authentication	In this method colours are already given user only have to remember the rating.	It is somewhat difficult to remember colours with Sequence.
5	Signature based scheme	Signature of anyone cannot be copied as it is.	Remembering the grid of signature is not a simple task.
6	Biometrics	It is easy to use along with the high verification process speed and accuracy.	Fingerprints of people working in chemical sectors often affected.

IX. CONCLUSION

Conventional authentication schemes used to provide normal level of protection to user account. Which includes mainly Bio-metric based lock and Graphical password lock. This techniques and also some other techniques are in use, but they have their drawbacks such as less security and more cost. As this system is working on Pair based authentication scheme with parallel working of AES encryption technique, it becomes highly secured. The results of Pair Based Dynamic Grid Authentication show that it is efficient in reducing processing time by taking texts as the input. Also, shows the cost for designing the system is very less as no external hardware is required for the authentication process. It is resistant to many attacks and provides high protection level. The implemented authentication scheme is faster and more secured compared to the other schemes in the market. AES provide real protection to data. Therefore this system is secured by all the angles. Securing e-mailing system using pair based authentication with session password provide security from shoulder surfing, brute force and other data thieving attacks. All comparisons and summaries and implementation proves that this system is best efficient and should be adopted by internet websites.

REFERENCES

[1] Jay Patel, Prof. Ashil Patel, "A Research on Authentication Scheme for Session Password with colour Pairs and Grid compared with OTP," IJSRSET , Volume 2 , Issue 3 ISSN : 2395-1990

[2] Mr. Sagar A. Dhanake, "Authentication Scheme for Session Password using matrix Colour and Text", IOSR-JCE, Volume 16, Issue 1

[3] Reshma kadam, Swapnil kashit, "Authentication Scheme for Session password Using Hybrid and Paired Based Techniques", KJCOEMR, volume 1,issue 2,pp.175-182

[4] M.L. Gavrilova, "Biometric Based Authentication for Cyberworld Security", CDFAI, vol 2
Vaclav Matyas and Zdenek Rıha, "Biometric Authentication Security and usability", NIST ,FIPS PUB 140-1/2

[5] Janhavi Thakur, Sheetal Rathi, " Pair Based Authentication using Dynamic Grid", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 ,Issue: 8

[6] Roshni Padate Aamna Patel, "Image Encryption and Decryption Using AES Algorithm", IJECET, volume 6, Issue 1, pp. 23-29.

[7] Ashwini R. Tonde, "Implementation of Advanced Encryption Standard (AES) Algorithm Based on FPGA", International Journal of Current Engineering and Technology, EISSN 2277 4106, PISSN 2347 -5161

[8] Shashank Sawant ,Aishwarya Shetty,Payal Pawat, "Multilevel System Security Using Graphical Password and Pair Based Authentication Scheme" , The International Journal Of Science & Tech, ISSN 2321 – 919X