Secured Personal Notes Application using PlayFair Cipher 8 x 8 Matrix

Gottam Ravi Teja Reddy
Department of Computer Science and Engineering,
Anurag University, Hyderabad-500085, India
Email: 18h61a0554 [AT] cvsr.ac.in

Thota Nagesh
Department of Computer Science and Engineering,
Anurag University, Hyderabad-500085, India
Email: 18h61a0520 [AT] cvsr.ac.in

Gudipati Harsha Vardhan
Department of Computer Science and Engineering,
Anurag University, Hyderabad-500085, India
Email: 18h61a0521 [AT] cvsr.ac.in

D. S. R Murthy
Department of Computer Science and Engineering,
Anurag University, Hyderabad-500085, India
Email: dsrmurthycse [AT] anurag.edu.in

Abstract--- **Secured personal notes application is a mobile application that allows a person to secure his personal and confidential information by storing it in the application after encrypting the data. This application involves complex encryption algorithms which keeps user data secured. Traditional notes applications allow users to barely have a password for the application which does not provide security at the higher level. So, in this application users are allowed to encrypt their personal information in order to provide high level security by entering a key which the user alone knows.**

Keywords- Encryption, decryption, playfair cipher, secret key, key matrix

I. INTRODUCTION

These days information security has become one of the most overseen aspects in any field. Information security is consideredimportant as misuse of data can create a lot of problems and havoc situations. It is very important to keep information secure as data costs more to many people in society. Hackers and intruders try to get data from various sources by hacking databases and servers of various social media websites or any other application servers. Hackers try to misuse that data and benefit from it. So, it is very important to keep data secure so that there won't be any misuse of data. Information security is not only about protecting data from unauthorized users but also about storing, accessing and managing data without being corrupted and modified by others. Information security also deals with the disclosure, disruption, inspection and recording ofdata.

Basically, information security builds around three main objectives; they are Confidentiality, integrity and availability. Confidentiality means data is not disclosed to any unauthorized individuals. Confidentiality ensures that data is accessible to only authorized users. Confidentiality is majorly achieved by using passwords and keys. Integrity means maintaining accuracyof information and correctness of data. That is data cannot be modified by unauthorized users. Integrity ensures that data is modified or changed only by the valid users, who are allowed to do so. Availability of data refers to the availability of data when it is needed.

Even personal information has got a lot of importance which might include family details, passwords, health details and other confidential information. Basically people keep noting many of their daily activities and personal information in the notes. All this data will be lost when we lose those notes and it is very common that others can view the notes so easily. This will not ensure confidentiality, integrity and availability of data. So, it is very important to manage our personal information keeping it very secure and confidential. All this can be done with the secured personal notes application. Secured personal notes application provides additional security to the confidential data of the user. Apart from security provided by the application using basic passwords and locks, secured personal notes application provides more security by encrypting data.

The application uses encryption techniques like the playfair cipher algorithm to encrypt the data. Playfair cipher is one of themost widely used encryption algorithms which uses substitution principles. The data which is encrypted using this algorithm is not in the human understandable form. It would be very difficultto decode and read the data after encryption; this makes the application more robust and secured.

II. LITERATURE SURVEY

[1] Modified Version of PlayFair Cipher by using 8 x 8 Matrix and Random Number Generation

This paper explains about a new approach to encryption of messages using an 8 x 8 matrix. The traditional PlayFair cipher uses a 5 x 5 matrix and can encrypt only alphabets. It cannot be used to encrypt numbers or special characters

due to its limited functionality. The approach presented in this paper tries to overcome this drawback by extending the matrix size to 8 x 8.This 8 x 8 matrix contains numbers and special characters apart from alphabets. The other functionality added in this new approach is the encryption of space character which is missing in the traditional approach. The spaces are replaced by '|' and encrypted using the matrix. The encryption and decryption is based on a key given by the user.The encryption is done by filling the matrix with a set of key (given by user) characters and the remaining characters and then encrypting the message based on encryption rules. Decryption is simply the reverse process of encryption. To summarize, the traditional playfair method is extended by increasing the matrix size and adding more functionalities to make it more scalable and secure.

[2] Playfair Cipher Encryption Program In Python

This paper discusses the execution of playfair cipher encryption program in python language. The playfair cipher encryption uses a matrix (5 x 5) to encrypt a plain text. The encryption process begins with dividing the plain text into sub parts (each part is a pair of two letters). A dummy character is added at the end if any character is leftover. The next step is to build a cipherkey matrix based on the key given by the user. The key matrix contains a total of 25 cells, each cell containing a character. Initially, each character from the key (without repetition) is written in matrix and then the remaining characters are written. This matrix is then used to encrypt the plain text. The encryption is done by taking each pair of characters and locatingtheir indices in the generated cipher matrix. After locating their indices, the pair of letters are encrypted based on the encryption rules. If they are in the same row then they are replaced by their respective adjacent characters. Same goes if they are in the samecolumn i.e., they are replaced by the characters present below them. This replacement follows a circular path. If the pair of characters are not present in the same row or column then a rectangle matrix is taken with these pairs of characters as two corners and their respective adjacent corners are used to replace them. In this way, the plain text is converted into cipher text using playfair cipher encryption method.

III. METHODOLOGY

Secured personal notes application is divided into several modules based on their functionalities. This application performs few operations like encrypting data and storing it in a database and decrypting the data while retrieving it. The application is divided into three modules namely

1. User authentication module
2. Secured notes accessing module
3. Secured notes storage module

1. User Authentication Module

This module is the initial module which gets executed when the application is started. This module ensures that the user who is accessing the application is an authorized user. When the application is first installed this application takes the user login credentials and stores it in the database and uses it to verify the user whenever he tries to login again. This module is used to verify whether he is a valid user or not using the credentials which were stored initially. As it is said earlier that this project has two factor securities, user authentication is of it. This module does not allow invalid users to access the application or user data. Only valid users are allowed access to the notes whichare stored inside the application.

2. Secured notes storage module

This module is the important module to the secured personal notes application. This is the actual module which stores the notes of an individual in the database after encrypting it in the database. The module asks the user to enter a secret key to encrypt the user information which is used in the implementation of 8x8 playfair cipher encryption algorithm. Playfair cipher substitutes the characters in the user information with the character from the 8 x 8 matrix using the secret key entered by the user. The algorithm uses the secret key to subsequently decrypt the encrypted data while accessing the notes. It is the responsibility of the user to keep the secret key confidential from others. After encrypting the data, only the encrypted data is being stored in the database. So, if any hacker or intruder accesses the database, he cannot know the actual information as the data is encrypted which is not in understandable format.

3. Secured notes accessing module

This application module is used to access the data which is already stored in the database. Users are allowed to add notes oftheir own and store them in the database. Later when he wants to access the notes, it will be retrieved from the database. When the user clicks on the list of notes available, it will be retrieved from the database and given to the user. User is supposed to enter the key which he used while encrypting the notes or storing the notes. If the key which is entered is not correct then the user gets only encrypted data which is not understandable. So it is very important to remember the secret key used while encrypting the data.

IV. WORKING

Secured personal notes application majorly works on encryptionand decryption of data. This application takes data from the userand encrypts it and then stores it in the database.

Step 1: **User Authentication** - First factor authentication is used to authenticate the user. It takes login credentials from the user for the first time. And uses the same details every time the user tries to login. It separates each user based on their credentials, and stores the data for each user

separately. It maintains data of each user in separate documents.

Step 2: Application shows all the available notes to the user if any. It also provides a button to add notes of his own. If the userwants to access or see any of the previous notes that he has already saved, then he can click on the card named with the title of his desired notes. Application then searches for the notes in the database, if found it will retrieve it from the database and show it to the user. Here the retrieved data from the database is actually in the encrypted format, to decrypt it, the application asks the user to enter the secret key which is used by the at the time of encryption. After entering the secret key application will show the actual notes/data that the user has stored, in the way two factor securities is maintained.

Step 3: To add the new notes, a separate floating button is maintained. By clicking on this floating button the user will be redirected to the page where he can add the title of the notes andthe information in the notes. Then he can save the notes by clicking on save button, while saving user will be asked to enter a secret key, that secret key is used to encrypt the data, and then notes will be stored in the database securely.

In the background, while the user enters a key to encrypt the data, the playfair cipher algorithm using the 8 x 8 matrix is executed on the data and secret key given. Secret key entered bythe user is used to encrypt the data. Here the playfair cipher algorithm using 8 x 8 matrixes will give a lot of scope to add many characters which are not included in the traditional playfair cipher encryption using 5 x 5 matrix.

This application implements the play fair cipher using 8 x 8 matrix in dart language. Dart language is a separate kind of language which is used along with a flutter framework to write the functionalities for the mobile application. Play fair cipher using 8 x 8 matrixes is also used to encrypt and decrypt the data while storing data in the database and retrieving data from the database respectively.

V. SAMPLE CODE

```
String encryption(String plainText, String
key) {

  key = key.toLowerCase();

 plainText = plainText.replaceAll(" ",
  "|").toLowerCase();plainText =
  convertPlainTextToDiagraphs(plainText);
    int i1, j1, i2, j2;

    List cipherText = [];

    List keyMatrix =
    generateKeyMatrix(key);int i = 0;
    while (i < plainText.length) {

    List n1 = indexLocator(plainText[i],
    keyMatrix); List n2 =
    indexLocator(plainText[i + 1], keyMatrix);if
    (n1[1] == n2[1]) {
      i1 = (n1[0] + 1) % 8;j1 = n1[1];
      i2 = (n2[0] + 1) % 8;j2 = n2[1];
      cipherText.add(keyMatrix[i1][j1]);
      cipherText.add(keyMatrix[i2][j2]);
    } else if (n1[0] == n2[0]) {i1 = n1[0];
      j1 = (n1[1] + 1) % 8;i2 = n2[0];
      j2 = (n2[1] + 1) % 8;

      cipherText.add(keyMatrix[i1][j1]);
      cipherText.add(keyMatrix[i2][j2]);
    } else {

      i1 = n1[0];

      j1 = n1[1];

      i2 = n2[0];

      j2 = n2[1];

      cipherText.add(keyMatrix[i1][j2]);
      cipherText.add(keyMatrix[i2][j1]);
    }

    i = i + 2;}

   String finalCipherText = "";

   for (int i = 0; i < cipherText.length; i++) {
     finalCipherText = finalCipherText + cipherText[i];
   }

   return finalCipherText;

}

String decryption(String cipherText, String key) {String
   finalText = "";
   int i1, j1, i2,
   j2; List
   plainText =
   [];
   List keyMatrix =
   generateKeyMatrix(key);int i = 0;
   while (i < cipherText.length) {

    List n1 = indexLocator(cipherText[i],
    keyMatrix); List n2 =
    indexLocator(cipherText[i + 1], keyMatrix);if
    (n1[1] == n2[1]) {
      i1 = (n1[0] - 1) % 8;
```

```
    j1 = n1[1];

    i2 = (n2[0] - 1) % 8;j2 = n2[1];
    plainText.add(keyMatrix[i1][j1]);
    plainText.add(keyMatrix[i2][j2]);
  } else if (n1[0] == n2[0]) {i1 = n1[0];
    j1 = (n1[1] - 1) % 8;i2 = n2[0];
    j2 = (n2[1] - 1) % 8;

    plainText.add(keyMatrix[i1][j1]);
    plainText.add(keyMatrix[i2][j2]);
  } else {

    i1 = n1[0];

    j1 = n1[1];

    i2 = n2[0];

    j2 = n2[1];

    plainText.add(keyMatrix[i1][j2]);
    plainText.add(keyMatrix[i2][j1]);
  }i = i + 2;}

for (int i = 0; i < plainText.length; i++) {finalText =
finalText + plainText[i];
}

finalText = finalText.replaceAll("|", " ");String finalt
= "";
finalt = finalt + finalText[0];

for (int i = 1; i < finalText.length - 1; i++) {if
  (finalText[i] == '^' &&
      finalText[i - 1] == finalText[i + 1] &&finalText[i - 1]
      != " ") {
    continue;
      } else { finalt += finalText[i];}}

    finalt = finalt +
    finalText[finalText.length - 1];if
    ((finalt.length) % 2 == 0) {
      return finalt.substring(0,
finalt.length - 1);}return finalt;
      }

}
```

VI. FUTURE ENHANCEMENTS

It is possible to add many other modules like allowing the user to delete his notes from the database if he thinks it is useless is one of the future enhancements that we can add to this application. Even though playfair cipher with 8x8 matrix has given a lot of scope for security of data. One can encrypt the data even more securely by using many other algorithms which are even better and robust than playfair cipher. In this project or application the user is allowed to store or record only his personal information which is a text format. But in the future it would be great if the application could store his personal images, videos or any other media files by encrypting them.

VII. CONCLUSIONS

Secured personal notes application is one of the finest applications which have all the features to store the data of the user in a secured way possible. The application using playfair cipher algorithm is making it even more secure and robust. Implementing playfair cipher algorithms using the 8x8 matrix have extended the boundaries of the application to next level, where the application was able to handle large no.of characters instead of only handling with alphabets which was a drawback with 5 x 5 matrices. The process of working of the playfair cipher algorithm remained the same even for an 8 x 8 matrix, so is the time complexity of the algorithm. As data security has gained a lot of importance, secured personal notes applications can serve the needs of people to store their personal informationsafely and securely. This application has got its importance by encrypting and decrypting data before storing it in the database.

REFERENCES

[1] Shiv Shakti Srivastava, Nitin Gupta, Rajaram Jaiswal, "*Modified version of Playfair cipher by 8 x 8 matrix*", Third International Conference on Computer Modeling and Simulation (ICCMS), 2011.

[2] Karan Munjani, "*Playfair Cipher encryption program in Python*", Article in www.dev.to, Oct 2021.