A Secure Scheme to Manage Complex Password Capable of Overcoming Human Memory Limitations

S. Maruthi Srinivas, Bharath Manchikanti, G. Chetan Babu, N. Harini

Abstract--- ***Security policies are required that protect information from illegal access, and also respect challenges users face in creating, and particularly managing, increasing numbers of passwords. With the increase in dependence of people on internet services for their day to day activities the number of passwords in use is more, the relationship between the passwords and the services is more complex. Each of the users follows their own strategy to remember and manage. Clearly, managing multiple passwords requires effort for creation, encoding, retrieval and execution. Most of us rely on the memory or reuse of passwords for easy management. The intricate characteristics of secure passwords, however, posit an unfortunate problem for password users. That is, whereas such passwords are difficult to be guessed by intruders, they are in general considerably difficult to be remembered by authorized users. This paper proposes a highly secure scheme that facilitates complex password management at ease without lack of user-friendliness.***

Keywords--- ***Encryption, Finger print, Biometric, Authentication, Single factor, Multi factor***

I. INTRODUCTION

With Internet becoming an essential tool for communication, commerce and financial services, Internet services have experienced tremendous growth. These services are made accessible to users regardless of their location. An inhibiting factor for the growth of these apps is only fear of fraud and data theft. The issues related to electronic security are of high importance to users, business and government. Most of the security policies and corporate initiatives design's by researches ignore user friendliness. This may in-turn limit user registration for new services apps and technologies. Addressing user friendliness is equally important for increasing the number of Internet app users. Today there is a high dependency of people on Internet dependent apps to carry out their day to day activities like: performing online app transactions for managing money transfers, communicating in social media to share personal interests and enrich knowledge from news services, perform online shopping etc. Undoubtedly youngsters are more attracted to gaming websites, socially connecting using media like Facebook, Snapchat etc.

Manuscript received February 01, 2012. (Fill up the Details)

S. Maruthi Srinivas, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore.Amrita Vishwa Vidyapeetham, India. (e-mail: cb.en.u4cse17456@cb.students.amrita.edu)

Bharath Manchikanti, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore. Amrita Vishwa Vidyapeetham, India. (e-mail: cb.en.u4cse17432@cb.students.amrita.edu)

G. Chetan Babu, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore. Amrita Vishwa Vidyapeetham, India. (e-mail: cb.en.u4cse17418@cb.students.amrita.edu)

N. Harini, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore. Amrita Vishwa Vidyapeetham, India. (e-mail: n_harini@cb.amrita.edu)

The rapid growth of smart phones has paved way for go anywhere, application support to avoid variety of social, financial and enterprise services, for any user with a cellular phone. Threat could be in the form of a malware, device theft, eves-dropping, etc. Statistics show that smart phones and mobile devices are exposed to higher number of threats for reasons like they contain huge amount of personal information stored in them. Android is an Operating System designed for smart phone to provide a sandbox execution environment. Mobile security is an area dealing with securing portable devices like smart phones tablets, etc.

The new venture dominating in the business world BYOD(Bring Your Own Device) is considered as one of the major challenges, as one is forced to connect to an open network which is more vulnerable to attack the users to work with different apps using the same mobile device, expected to manage multiple user accounts such as having each associated with different usernames and passwords. One has to notice that the use of same usernames and passwords is quite dangerous as the password breach can be used to attack multiple accounts of the same user. Although the literature specifies several authentication mechanisms that enable users to prove their identity to use online services like using passwords, possession of smart cards, mobiles using facial, fingerprint etc., to the best of our knowledge an app facilitating remembrance of these authentication tokens is lacking. This paper aims to provide a secure scheme that enables the users to manage multiple secrets used for accessing different applications using smart phones. The experimentation results clearly broughtout the strength of the scheme in terms of theft attack, eavesdropping attack clearly reveal the capability of the scheme to mitigate them while still providing a user-friendly way to manage secrets.

II. LITERATURE REVIEW

Most of the Internet-based services requires users to authenticate. Authentication could be done using tokens that are known to the user, possessed by the user or inherent in users. The existence of vulnerabilities in the network has increased the number of cyber criminals.Most of the apps today demand authentication based on multiple factors rather than single factors.

Passwords have been or still being accepted as a factor in multifactor authentication schemes the security offered by passwords mainly rely on strength of the passwords.

Weak passwords are generally prone to attacks whereas

strong passwords are less prone to attacks

[1]. It is equally important for one to understand that any password weak or strong could be breached with brute force attack. Today we have systems capable of generating strong passwords but the randomness introduce in the string makes it highly difficult for user to remember the password [2].The stringent rules insisted like include more digits, symbols, upper case letters also make password management difficult even for the legitimate user. Reports reveal that even these less memorable passwords were cracked at a lower rate [3]. This demands for a factor that is inherent and need not be remembered to be included as a part of the secret. Fingerprint based authentication has gained popularity because of their simplicity in usage when integrated with password based on authentication mechanisms.

A. Fingerprint based authentication

Authentication is a fundamental building block for security over the Internet. A user who successfully authenticates himself/herself gains access to remote services. The service provider makes the services available only if the authentication is success. There are many authentication schemes in literature like certificate, onetime password, personal password (main password), card-based authentication schemes, etc. The problem with these schemes is that something needs to be remembered or carried, to overcome this problem authentication using inherent characteristics in users were introduced (examples include facial, iris, finger print detection, etc.).With the mobile devices, laptops, tablets, being built with finger print scanners, authentication using finger prints is accepted now as simpler and strong scheme for enhancing the security [4].

B. Multi-factor security

Generally multifactor security scheme [5][6] is expected in scenario where safety requirements are higher than usual. The scheme generally involves with users first registering their authentication tokens (registration phase). At times when access is required the account user has to provide his / her security token values and the same is sent to service provider (Login phase). The service provider then verifies the tokens and if found OK, enables the customer to avail the service. Unsuccessful verification leads on rejection of uses. Multiple unsuccessful attempts may lead to locking of account. The common security tokens that are used to include:

Password protection

Password protection is a security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.

Voice Protection

To preserve privacy, authentication systems that can identify one without actually hearing one's voice or even keeping an encrypted record of one's voice[7].

Facial recognition

A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source [8]. It is typically used as access control in security systems and can be compared to other biometrics such as fingerprint or eye irisrecognition systems.

Iris recognition

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance.

Hand geometry

Hand geometry is a biometric that identifies users by the shape of their hands. *Hand geometry* is very reliable when combined with other forms of *identification*, such as *identification* cards or personal *identification* numbers.

Finger Vein recognition

Finger vein recognition is a method of biometric authentication that uses pattern-recognition techniques based on images of human finger vein patterns beneath the skin's surface. Finger vein recognition is one of many forms of biometrics used to identify individuals and verify their identity. Any of the above schemes can be combined to create multifactor authentication themes. The need of the hour is a scheme that is more secure but at the same time imposes a very little strain on legitimate users. This is particular important with a single individual being forced to work with multiple applications for their day to day activities.

III. PROPOSED SYSTEM

The Fig. 1(a),1(b) show the authentication scheme based on single factor. More over the scheme also suffers vulnerability as users tend to choose the weak password that could be easily remembered. The proposed scheme allows the user to choose a password containing a random string of any length including numbers, alphabets and special characters. The system provides a secure storage database that facilitates remembrance of passwords. Care is taken to ensure that passwords are stored only as encrypted values in the database. Furthermore the encryption is based on the finger print that is registered in the user mobile (meaning that the user need not perform additional steps to remember this encryption key). Assuming a case that an attacker has ceased the mobile to hack all credential in the database, a thorough experimentation was done. In all the cases the attempt of the attacker was failed proving the capability of the system to with-stand brute force attack, insider attack, man in the middle attack [9] and replay attack [10].

The working of scheme is illustrated in Fig. 2(a),2(b). In the initializing phase the system records the fingerprint of the owner of the mobile. In addition to which he/she uses the signup page associated with apps to create his/her login information. The password that is entered in the signup page is concatenated with the registered fingerprint and communicated to the application server as the final credential of user. During login and authentication phase when the user requires access to the service from the app they need to perform an interactive authentication procedure which

enables then to obtain the password of the app from the database at ease.

Initially the system displays only the encrypted version of the password to prevent the exposure of password from the eyes of the hacker. The user is then prompted to provide the second factor of authentication that is the fingerprint. On provision of the correct registered fingerprint the system displays the password in plain text which could be copied and pasted in login page of application. As the password is claimed to have longer strings ranging a length of 128 to 256 characters. Any eavesdropper who performs shoulder surfing attack [11] will be unable to memorize the string. The database also includes search facility that helps locating password at ease.

The advantage of the scheme is that the scheme has been tried and found to be working fine on a mobile environment that is associated with resource constraints.

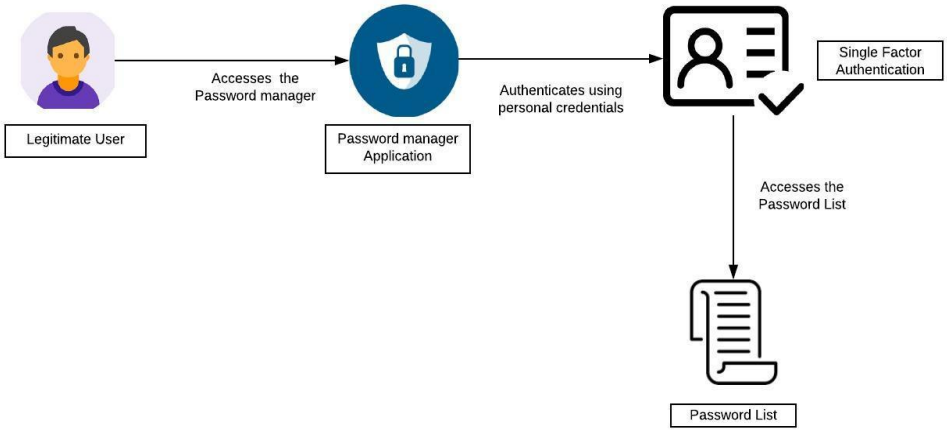

Fig. 1(a): Accessing the account via single factor authentication by a legitimate user

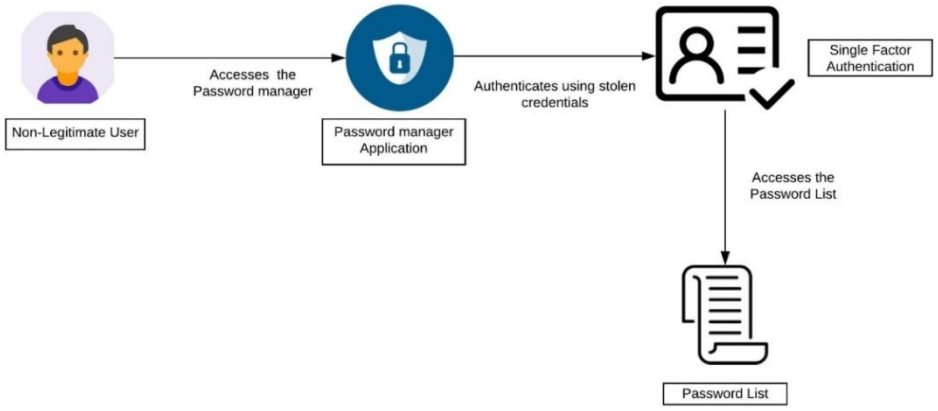

Fig. 1(b): Accessing the account via single factor authentication by a non-legitimate user

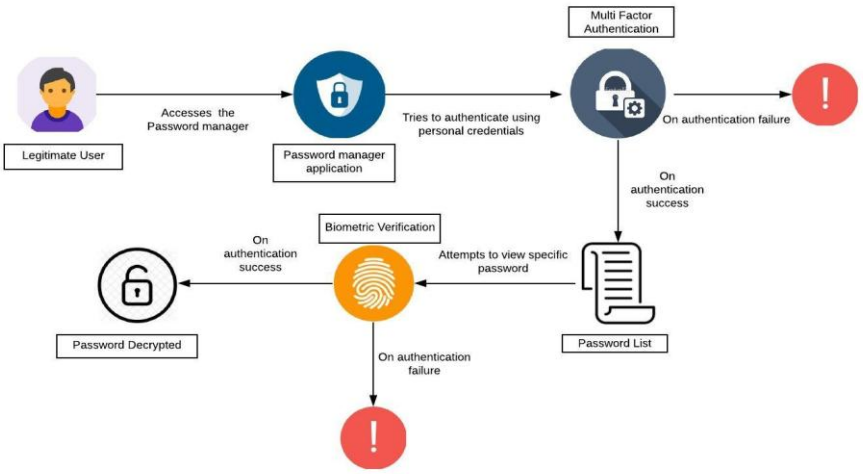

Fig. 2(a): Accessing the account via multi factor authentication by legitimate user. (Proposed Scheme)

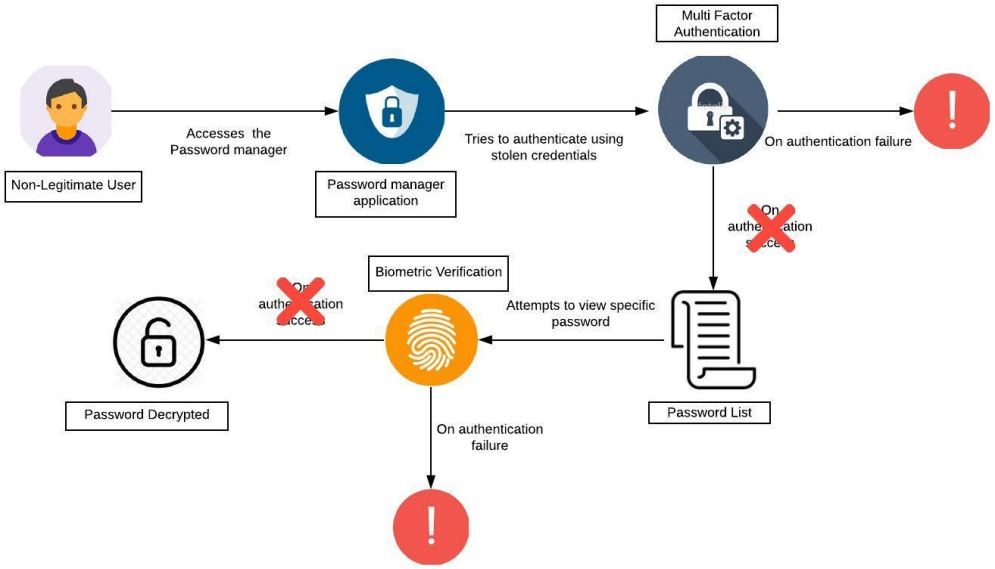

Fig. 2(b): Accessing the account via multi factor authentication by non-legitimate user (Proposed Scheme)

IV. RESULTS AND DISCUSSIONS

In this section we discuss the performance of proposed scheme in terms of security property and computation efficiency. The screen shots of the implementation and results contained are included in Fig (3-10).The security analysis indicates that proposed scheme can be free from well-known attacks on password based authentication. To improve the usability of password and facilitate user to work with strong passwords the paper proposes a design of an authentication scheme that is user friendly based on multiple factors and allows access to any service at ease for legitimate users and also ensures that the credentials are not exposed to the evil eyes of the attackers. The scheme is not based on computation intensive schemes like RSA [12], ECC [13][14], etc. It is more suitable for accessing apps using smart devices.

Fig. 3: Finger-print registration

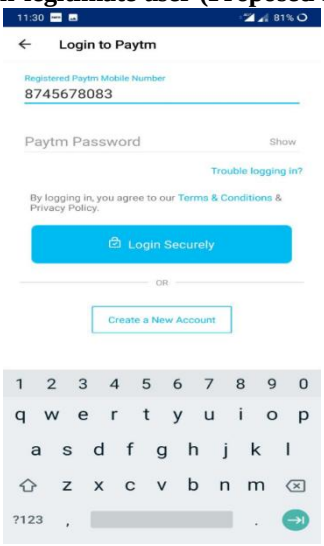

Fig. 4: User accessing his/her account

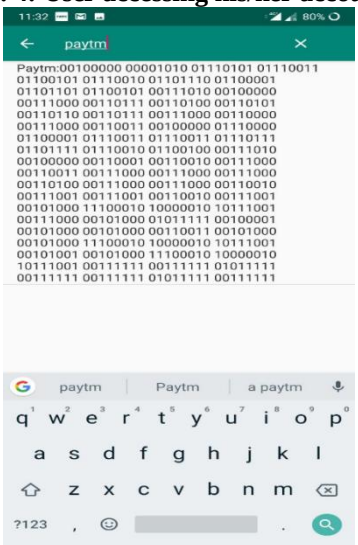

Fig.5: User searching for credentials

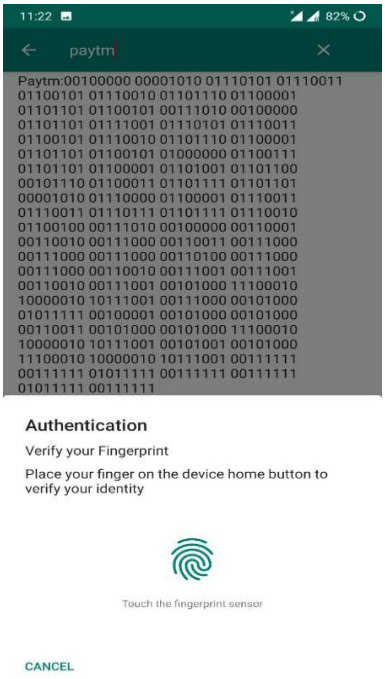

Fig. 6: Verification to decode the password

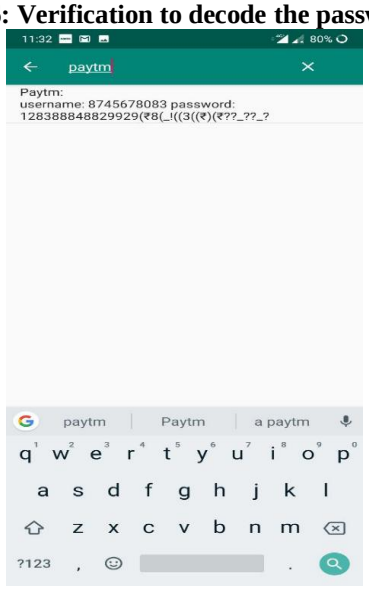

Fig. 7: Decoded version of the credentials

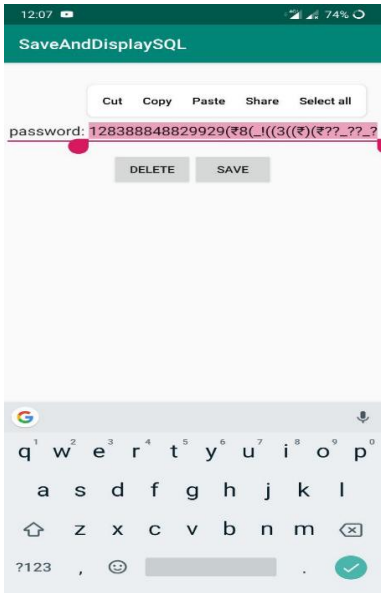

Fig.8: Copying the credentials

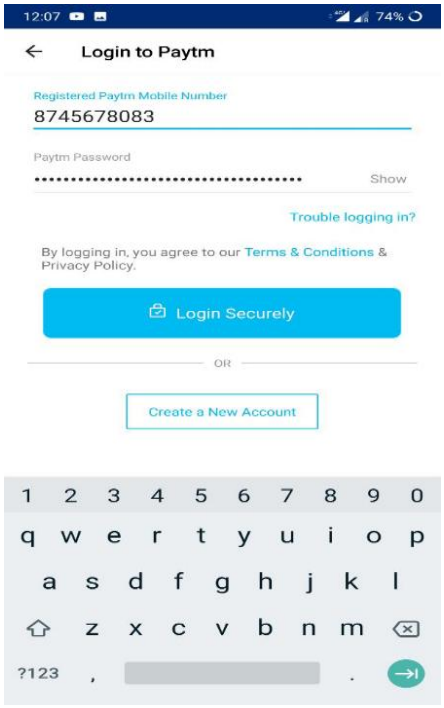

Fig. 9: Copied credentials used to login

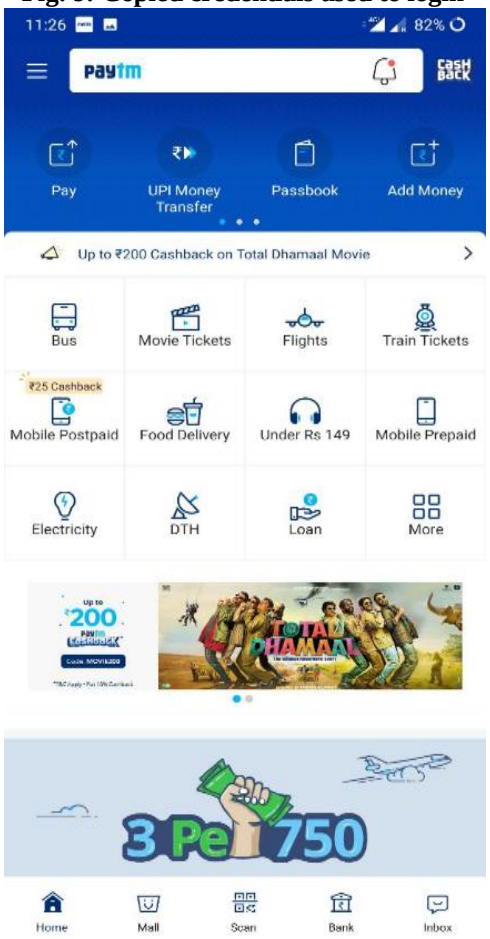

Fig. 10: Successful login

The screenshots of the code snippet for the checking the finger print of the user which on succesfull verification lead to accessing and manupulating the data is given in Fig. 11(a) and 11(b)

```
private String encrypt(String string) {
    String s1 =string;
    int space=0,size=s1.length();
    String seperate="";
    for(int counter =0;counter<size;counter++)
    {
        if(s1.charAt(counter)==' '){
            space=counter;
            break;
        }
        else
        {
            seperate=seperate+s1.charAt(counter);
        }
    }
    s1=s1.substring(space);
    byte[] bytes = s1.getBytes();
    StringBuilder binary = new StringBuilder();
    for (byte b1 : bytes)
    {
        int val = b1;
        for (int j = 0; j < 8; j++)
        {
            binary.append((val & 128) == 0 ? 0 : 1);
            val <<= 1;
        }
        binary.append(' ');
    }
    String finalstring=seperate+binary.toString();
return finalstring;
```

Fig. 11(a)

```
MainActivity.java
    private Button btnAdd, btnViewData;
    private EditText editText;
    public String newEntry;
    public int c;
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        editText = (EditText) findViewById(R.id.editText);
        btnAdd = (Button) findViewById(R.id.btnAdd);
        btnViewData = (Button) findViewById(R.id.btnView);
        mDatabaseHelper = new com.tabian.saveanddisplaysql.DataBaseHelper( context: this);

        btnAdd.setOnClickListener((v) -> {
                newEntry = editText.getText().toString();
                c=0;
                if (editText.length() != 0) {
                    new BiometricManager.BiometricBuilder( context: MainActivity.this)
                            .setTitle("Authentication")
                            .setSubtitle("Verify your Fingerprint")
                            .setDescription("Place your finger on the device home button to verify y...")
                            .setNegativeButtonText("CANCEL")
                            .build()
                            .authenticate( biometricCallback: MainActivity.this);

                } else {
                    toastMessage("You must put something in the text field!");
                }

            });

MainActivity › onCreate() › new OnClickListener › onClick()
```

Fig. 11(b)

V. CONCLUSION

The rapid development in information and network technology has driven exponential growth in the number of services offered through mobile and Internet platforms. To ensure that these services can be accessed conveniently by authorized users, many single factor and multi factor schemes have been proposed. But one has to understand however complex the scheme may be the choice of the secret is more important for assuring security.In this paper a user-friendly authentication scheme that facilitates user to choose complex passwords while still assisting them in accessing a wide variety of Internet services using the passwords that are normally unrememberable has been proposed.The performance clearly reveals the fact that the proposed scheme is advantageous in terms of security and efficiency and is more desirable for practical applications. The authentication procedure doesn't need any additional hardware to enhance security. Also the computation cost and authentication procedure is kept as simple as possible. In short, the proposed scheme surpasses other schemes in literature in terms of providing stronger security guarantee and password management without compromise in user friendliness.

REFERENCES

1. Katha Chanda. Password Security: An Analysis of Password Strengths and Vulnerabilities, I. J. Computer Network and Information Security, 2016, 7, 23-30. DOI: 10.5815/ijcnis.2016.07.04
2. J Alex Halderman, Brent Waters, Edward W. Felten. A Convenient Method for Securely Managing Passwordshttps://jhalderm.com/pub/papers/password-www05.pdf
3. Anatomy of a hack: even your 'complicated' password is easy to crack.
4. .Mouad M H Ali, Vivek H Mahale, Pravin Yannawar, A. T. Gaikwad. Overview of Fingerprint Recognition System, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)-2016,DOI:10.1109/ICEEOT.2016.7754902.
5. Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo 3, Sergey Andreev, TommiMikkonen and Yevgeni Koucheryavy , Multi-Factor Authentication: A Survey, doi:10.3390/cryptography2010001
6. Harini, N.; Padmanabhan, T.R. 2CAuth: A new two factor authentication scheme using QR-code. Int. J. Eng. Technol. 2013, 5, 1087–1094

8. Sattar B Sadkhan, Baheeja K Al Shukur, Ali K Mattar, Biometric voice authentication auto-evaluation system, 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)DOI: 10.1109/NTICT.2017.7976100
9. Kavita, Ms. Manjeet Kaur, A Survey paper for Face Recognition Technologies, International Journal of Scientific and Research Publications, July 2016 441 ISSN 2250-3153http://www.ijsrp.org/research-paper-0716/ijsrp-p5564.pdf
10. Mauro Conti, Nicola Dragoni, and Viktor Lesyk,A Survey of Man In The Middle Attacks, IEEE Communications Surveys and Tutorials, 2016 DOI: 10.1109/COMST.2016.2548426
11. Zhizheng Wu, Sheng Gao, EngSiongChng and Haizhou Li, A study on replay attack and anti-spoofing for text-dependent speaker verification, Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2014, DOI: 10.1109/APSIPA.2014.7041636
12. Peng Foong Ho, Yvonne Hwei-Syn Kam, Chin Wee Yu Nam Chong and Lip Yee Por, Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information, Hindawi Publishing Corporation, Scientific World Journal. DOI: 10.1155/2014/838623
13. M Preetha1, M Nithya,A study and performance analysis of RSA algorithm. 2013, IJCSMC, ISSN 2320–088X
14. Himja Agrawal, ProfPRBadadapure, Survey Paper On Elliptic Curve Cryptography. International Research Journal of Engineering and Technology (IRJET) (2016). e-ISSN: 2395 -0056
15. Dr.N.Harini, Dr T.R Padmanabhan and Dr.C.K.Shyamala , ―Cryptography and security‖, Wiley India, First Edition, 2011

AUTHOR PROFILE

S Maruthi Srinivas is a student currently pursuing Computer Science and Engineering degree at Amrita School of Engineering, Coimbatore. His research interests include data encryption Mobile Application Development.

Bharath Manchikanti is a student currently pursuing Computer Science and Engineering degree at Amrita School of Engineering, Coimbatore. His research interests include Mobile Application Development and Machine Learning.

G Chetan Babuis a student currently pursuing Computer Science and Engineering degree at Amrita School of Engineering, Coimbatore. His research work includes developing the encoding algorithm.

Dr. Harini N. currently serves as Assistant Professor in the Department of Computer Science and Engineering at Amrita School of Engineering, Coimbatore Campus. Her Qualifications are Ph.D, MCA, MPhil and her primary area of research is Security.