Journal of Engineering Sciences
Vol 11, Issue 5,May/2020
ISSN NO:0377-9254

Enhance Security for Mobile by Using Image Processing

Mininath R. Bendre[1], Poonam J. More[2],Kanchan R. Shendkar[3], Aishwarya B. Athare[4], Dhanuja M. Gite[5]
[1]*PREC, Loni Computer, SPPU, India*
[2]*PREC, Loni Computer, SPPU, India*
[3] *PREC, Loni Computer, SPPU, India*
[4]*PREC, Loni Computer, SPPU, India*
[5] *PREC, Loni Computer, SPPU, India*

***Abstract*— Today as we see all people over the world are using a smartphone, which is become an important part of life. All the data we store in the smartphone including banking data like using online banking. So secure and store that data is an important aspect form a password authentication system. But the authentication systems that we are using like textual and pattern-based are crack by hackers very easily. So we thought to design an authentication system for a smartphone that is more secure than the current authentication system. In this paper, we propose a password authentication framework that is designed for secure data and password storage of a smart-phone to make it more secure and safe to use. In this framework, we are going to use three layers of algorithm/technique to make it more secure. First, the user will authenticate using the visibility blur technique. The second authentication phase will be the chameleon algorithm and the third is encrypted negative password algorithm. So by combining three different techniques/ algorithms a secured system will be designed. This authentication system will be applied to any App on the smart-phone for security.**

Keywords-Password, Authentication, Visibility Blur, Chameleon, Hashing, Encrypted Negative Password.

1. INTRODUCTION

The Safe password authentication system is the need of the day. In that data related to banking is very important. As a new online banking app is developed then it requires more safety for the smartphone. Due to the loss of data, there is a risk of loss and theft of money. But hackers crack passwords very easily it is difficult to maintain a secured data system. that Attack includes the shoulder-surfing attack, the hidden-camera attack, the spyware attack, and the wiretapping attack, etc. to avoid such attack we are using three authentication techniques like Visibility Blur, Chameleon and Encrypted Negative Password used will create a very high end secured system. So we thought of using this technology in our project to make any Smart-phone application more secure by providing the authentication scheme using the above three layers. In these, we will propose to enhance security by using a text-based graphical password scheme to provide resistance to attacks. In that blur, the technique resists the shoulder-surfing attacks. Chameleon provides shuffling keypad which confuses the hackers and resistance accidental login. And the encrypted negative password is used for the security of the database and resist to dictionary attack and lookup table attack. In these, all aspect of security is covered in it.

2. LITERATURE SURVEY

Many mobile security techniques are searched by many researchers in the world. Like:

1. The Authentication by Encrypted Negative Password [1]:- In 2018 Wenjian Luo, Yamin Hu, Hao Jiang, and Junteng Wang authored this paper which explains a password authentication algorithm that is designed for secure password storage.
2. An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme[2]:- In 2014 Wei-Chi Ku, Dum-Min Liao, Chia-Ju Chang, And Pei-Jia Qiu authored this paper which explains enhanced capture attacks resistant text-based graphical password scheme, Chameleon, which provide resistance to accidental logins because of the shuffling keypad and high usability.
3. IllusionPIN: Shoulder-Surfing Resistant Authentication using Hybrid image[3]:- In 2017 Athanasios Papadopoulos, Toan Nguyen, Emre Durmus, Nasir Memon Authored this paper which explains The

system will use blur images that cannot be seen from long distances.

3. METHODOLOGYAND WORKING

3.1. Visibility Blur technique

At the start, we are using the Blur algorithm by decreasing the image clarity so the person seeing that image from a short distance can see it. But a person seeing an image from a large distance didn't see it properly. During putting the password on the chameleon keypad the keypad is a blur which seen clearly to the user and didn't see the attacker properly so he cannot hack our password. As shown in fig.1. By attackers view the keypad looks as shown in fig. so the attacker cannot identify the password put by the user. If the attacker remembers the position of keys then also the keypad is shuffling so the attacker can't crack the password. So for avoiding shoulder-surfing attacks, the blur algorithm is an efficient technique.

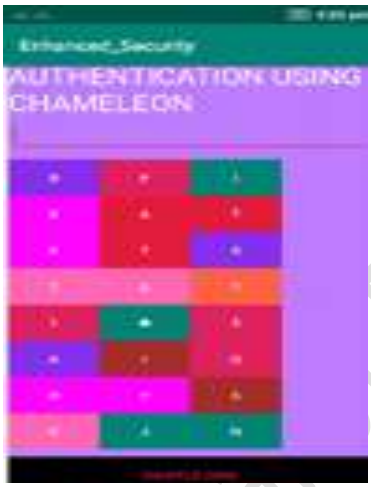


Fig.1.Blur keypad by attackers view

3.2. Chameleon Algorithm

In the chameleon algorithm as a user puts his password by the encrypted keyboard which prepares using the chameleon algorithm. That password stored in the database.

When the next time user wants to open the password user should put the same password with the same letter color after putting that password the authentication is done if password matches with database then the app will open. Otherwise, the system shows a message of an invalid password.

The system will use a mesh of words with specific background colors. The user has to select the same word with the same color during verification. It will be used as the next layer of security. The weakness of most existing capture attacks resistant text-based graphical password system is an attacker can know the user's password length by just capturing one login session. Thus, the attacker can crack the user's password easier. In this, we will describe a more secure capture attacks resistant password technique, Chameleon, which is a hybrid password scheme based on texts and a pass-color-shape. The color of the pass-color-shape is used in the password length hiding. Additionally, the shape of the pass-color-shape is used to increase the resistance to accidental login attacks. In Chameleon, which involves the registration phase and the login phase, the user can efficiently and securely complete the login process.

The user's password includes two parts, the pass-string, and the pass-color-shape. The system will advise the user to register in an environment free of spyware, hidden cameras, and shoulder surfing attacks. The user has to set his pass-string of length L characters from the character set, including 26 lower case letters, 26 upper case letters, 10 decimal digits, and 28 qwerty-like keyboard symbols. Next, the user has to choose one color-shape from the 30 fixed color-shapes displayed on the screen as his pass-color-shape. And that password stored in the database using an encrypted negative password.

During login user firstly open the login screen of the chameleon and puts his password like the user put at the time of registration. The user has put the same pass-string and pass-color putting at the time of login.

In this way chameleon algorithm works which resist the accidental attacks.

Fig.2.Chameleon keypad for login and registration

3.2. Encrypted Negative password

Secure password storage is an aspect of any password authentication system. To provide secure password storage we are using encrypted negative password algorithms.

It includes a two-phase registration phase and authentication phase.

3.3.1. Registration Phase

As shown in fig.2 ENP registration phase work. In that user register his/her password from the chameleon screen. And it generates password in pass-color-shape which sends to hash. Hash function creates a hashed password and generates a negative password. Encrypt function encrypts that password and stored it in the authentication data table.

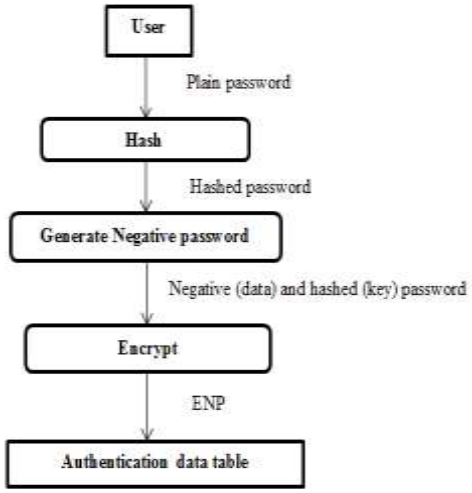


Fig.3. Generation of Encrypted Negative Password

3.3.2. Authentication phase

In the authentication phase, the password is given by a chameleon screen where the user has to put the same password with the same background colour. So the same pass-colour-shape password is taken.

In this user put his plain password on chameleon screens that password hashed using a hash password.

That password in an authentication data table is encrypted and both hashed password and negative passwords are matches. If both the password matches then it shows acceptance of password and system login.

Otherwise, the system shows the message of the invalid password.

In this way, the encrypted negative password algorithm works

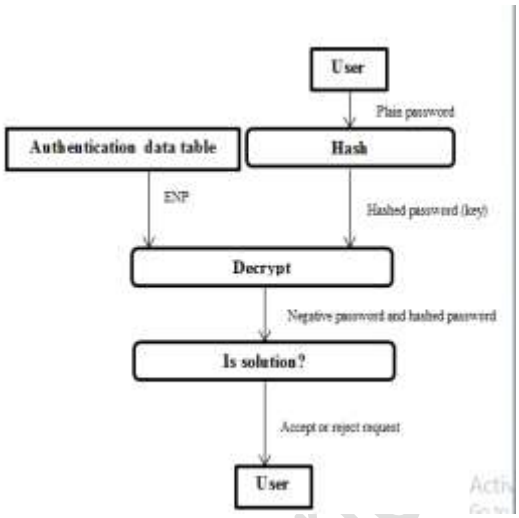


Fig.4. Authentication of encrypted negative password

4. MATHEMATICAL MODULES

4.1. Set theory applied to the project

4.1.1 .PATTERN REGISTRATION:

Set(R) = {R0, R1, R2, R3, R4, R5}

R0∈R = Select images from a visibility blur pattern using for first layer

R1∈R = Select words with a specific background colour for Second layer.

R2∈R = Save the pattern using Negative password as third layer.

R3∈R = Receive acknowledgement.

R4∈R = Apply pattern to an App.

R5∈R = View results on phone.

4.1.2. Pattern Verification:

Set (V) = {V0, V1, V2, V3, R5, V4}

V0∈V = Click the App to start.

V1∈V =Select images from a visibility blur pattern registered for first layer.

V2∈V =Select words with a specific background colour registered for Second layer.

V3∈V = Verify the pattern using Negative password as third layer.

R5∈V = View Results on Phone.

V4∈V = Open the App if the above patterns are successful.

Venn diagram of intersection of two sets

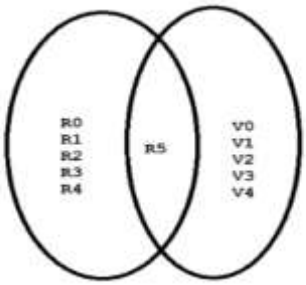


Fig.5.Venn diagram

4.2. Probability of our Project Modules

4.2.1. In Pattern Registration Module: We have two possibilities for saving correct pattern results in the database i.e. whether proper negative password is applied or not.

P (present) =1/2

P (not) =1/2

Hence, P (Save) = P (present) + P (not)

=1/2 + ½

= 1

4.2.2.In Pattern Verification Module: We have two possibilities for verification of correct pattern results in the database i.e. whether proper negative password is applied or not.

P (present) =1/2

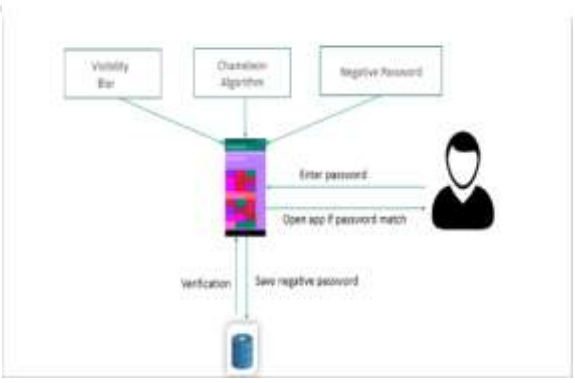
P (not) =1/2

Hence, P (Verify) = P (present) + P (not)

=1/2 + ½

= 1

5. DESIGN



6. RESULTS

The enhance security application was checked over the many banking applications of smartphone. The performance is efficient over all the applications. It resists shoulder-surfing attack, accidental login attack, lookup table attack, dictionary attack, etc.

7. CONCLUSION

In this paper, we proposed the enhance security for mobile by using image processing by integrating three algorithm visibility blur, chameleon algorithm, and encrypted negative password. Visibility blurs offers resistance to shoulder-surfing attacks. Chameleon provided high resistance to accidental login. ENP resists lookup table attack and provides stronger password protection under a dictionary attack.

We will be assembling the three algorithms together to build a whole new system which is secure and reliable for a mobile application. The proposed method is found to be better on many criteria as compared to existing studies.

ACKNOWLEDGMENTS

We would like to express our special thanks of gratitude to Dr. M. R. Bendre sir as well as our college PREC Loni who gave us the golden opportunity to do this wonderful project on the enhance security for mobile by using image processing which also helps us to do a lot of research and we came to know many new things we really thankful to them.

And, we would also like to thank our parents and friends who helped us a lot in finalizing this project.

REFERENCES

[1] Wenjian Luo, Yamin Hu, Hao Jiang, and Junteng Wang" Authentication by Encrypted Negative Password" in IEEE Journal 2018.

[2] An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme"in IEEE Journal 2014.

[3] Resistant Authentication Using Hybrid Images"in IEEE Journal 2017.

[4] Rutgers Scholar, Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[5] J. Ma, W. Yang, M. Luo, and N. Li, "A study of probabilistic password models," in Proceedings of 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 689–704.

[6] Mathur, " Combination of textual and graphical based authentication scheme through virtual environment" in IEEE 2017.

[7] C.Ganga, K.Manoj Kumar "Implementation of Graphical Passwords in Internet Banking for Enhanced Security" in IEEE 2017.

[8] Sachin Kaja, Divya Gupta "Graphical Password Scheme using Persuasive Cued Click Points" in IEEE 2017.

Authors profile

Mininath R Bendre, PhD, CSE

Poonam J. More
BE Computer(Student)

Kanchan R. Shendkar
BE Computer(Student)

Aishwarya B. Athare
BE Computer(Student)

Dhanuja M. Gite
BE Computer(Student)