ISSN: 1832-5505

Applied GIS

Vol-7 Issue-01 Jan 2019

A Secure Authentication System for Blind Users

Shailja Varshney[1], R. lavanya kumar[2]
Z.H. College of Engineering and Technology, Aligarh Muslim UniversityAligarh, India

Abstract. Some mobile device users face security risk because of their visual disability, so they can't access authentication methods that use commonly. The mostly used authentication method such as password entry, picture based pass- word, scrolling password and grid based password schemes not useful for the blind user. So we provide such technique that is useful for Authentication on mobile or other devices for blind user as well as normal user. Here we have suggested a new Authentication Scheme. There are some hardware requiring like Mike and Speaker or we can say a head phone that is easily accessible by any user. This method is also secure from shoulder surfing attack.

Keywords: Blind, mobile devices, Security, mike and speaker, head phone.

Introduction

The use of mobile devices are risky than traditional computers because of authentica- tion method and size. Because the size of handheld devices is small in comparison of traditional computers, so entering the password on small screen keyboard causes frus- tration to the users. Small size handheld devices also face the risk being lost or stolen. People commonly contain their personal information like emails, contact numbers, pictures and other private data, that can be lost or stolen if no authentication mecha- nism has not been used. The blind users mostly do not use any authentication mecha- nism. They commonly access mobile information via special features of the devices like screen readers, Apple's Voiceover for iOS devices, which read the contents of the screen and user input. Using mobile in public places is very risky for blind users be- cause of these features. User Authentication is an effective and common way to pro- tect private data. Here we have suggested a new authentication scheme that provides security from shoulder surfing attack. It contains good password space so it secure from brute force attack also. In summary, we can say that two aspects have been dis- cussed in this paper.

1. Study of security risks in terms of mobile device for blind users.
2. A new Authentication scheme has suggested for both normal and blind users.

Previously used algorithms

Most of the times authentication methods can be divided into three major areas:

2.1 Token Based Authentication

Bank cards and smart cards etc are mostly used in token based authentication method. Most of the time token-based authentication systems used knowledge based pass- words for authentication to improve security of system. For example, ATM cards are used with a PIN password for authentication purpose.

2.2 Biometric Based Authentication

Biometric Authentication is a security process that takes the measurement and calcu- lation of the human's characteristics individually. This information is used for authen-tication purpose at login time. Biometric based Authentication is also divided into twoparts:

Physiological Biometric Authentication like – Face, **Fi**

Behavioral Biometric Authentication like – Keystroke, Signature, Voice Recogni- tion.

2.3 Knowledge based authentication

Knowledge based authentication method are mostly used for authentication. In this method text-based passwords and pictures based passwords are employed for authen- tication purpose. Picture based password method is also divided into some techniques:

Recognition based method
With the help of recognition based method, a user gives set of images during registra- tion time, and the user is authenticated by recognition of these images.

Recall based method
In recall based password method, a user is authenticated by answering some questions at the time of registration.

Hybrid Scheme.
It is the technique, which uses more than one Authentication methods. So, because of the use of more than one method, hybrid authentication scheme is more secure and complicated to design.

Possible attacks on Password

Shoulder Surfing: In case of shoulder surfing, text based password have more risk because if user operates system in such place where CCTV camera is available then entered password can be captured by the CCTV camera and attacker can break the password by zooming it.

Brute Force Attack: In this type of attack, attacker tries all possible combination of letters and numbers to break the password in case of text passwords. Larger password space reduces the strength of this attack.

Spyware Attack: Spyware is software which gains some information about a person or organization without their knowledge, which send information to another person or machine that is unauthorized person without the knowledge of the user.

Dictionary Attack: In this type of attack, attacker tries all passwords by guessing those types of passwords that are mostly common such as name, Date of birth, 123…etc.

Phishing Attack: In this type of attack, the attacker makes the fake website in which user enters their password and attacker steal it.

REALATED WORK

Here the work comes under the two categories:

3. Security issues for blind peoples.
4. Mobile Authentication mechanism for general population.

Over work is the first focus on the security issues for the blind mobile device uses. Shri Azenkot et al. proposed a Pass Chords authentication technique for blind users. This method is related to tapping on the screen with fingers and create password. This technique can create some problem when users have any cut, wound and other prob- lem in their fingers. Here problem can also be arises in authentication due to the posi- tion of the handheld device. And the password space of this technique is not so good. Kuber and Sharma proposed accessible authentication method for desktop computers using a tectile mouse. Most of the papers are related to Graphical Password authenti- cation methods, i.e., not useful for the blind users of mobile device.
Shailesh and Muhammed Ilyas proposed a scheme in which user provide the sequence to some sound clips. The password space for this scheme is small so it can be easily break by brute force attack.
Biometric authentication offers another type of authentication based on physical acces- sibility that is an alternative to graphical and alphanumeric password scheme. Biometric technique always requires some special hardware which is costly and cannot applied everywhere. Here we focus on lightweight authentication scheme.

THREATS AND DEFENSES

5.1 Aural eavesdropping:

A fraud bystander can hear the private information that is spoken by screenreaders.

5.2 Visual eavesdropping:

A fraud bystander can see the private data display on the screen. If a person has lowsight, is using large font or magnifies feature of the mobile device.

5.3 Unauthorized user access:

Both blind and sighted user faces this problem due to stolen and loss the device.

5.4 Password Protection:

Password is required for authentication before using the device. Password providesthe security for private Information within the device.

ISSN: 1832-5505

Applied GIS

Vol-7 Issue-01 Jan 2019

PROPOSED METHOD

For this method we require Mike, Speaker or Headphone. These devices provide the security from aural eavesdropping and visual eavesdropping. In this scheme user pro-vides all the detail with the help of headphone and mike at both time.

6.1 At Registration Time –

- Users are register with details in system.
- Asking randomly any five questions to the user at registration time.
- Answer length should be between 3 to 20
- After that system provide a simple formula that is used at login time.

6.2 At Login Time –

- User enters their user name.
- System randomly asks any one question from the set of questions that are enter atregistration time by the user.
- System also provides a random number with question.
- User knows the answer but not given to exact.
- User takes the letter from answer that is positioned according to random number i.e. generated by system.
- User calculates new position for that letter by the formula.
- Place that letter in new location and remaining letters can be dummy letters, andrecognize the user.

Here password length restricted from 5 to 12.

Example:-.

At registration time:
Machine gets some details about user like username, name, sex, phone number, emailid, and randomly any five questions. Like-

Q- What is your childhood name?Ans- jenny

Q- What is your hobby?Ans- listening music

Q- What is your pet name?Ans- jacky

Q- Who is your idle?
Ans- APJ abdul kalam

Q- What is your favorite festival?Ans- Diwali

And suppose formula-

(Random No.*3) % Answer lengthAt login time:
System asks username, like-“Rahul121”

System asks a question randomly, like-

Q- What is your pet name? And give a random no. 3

Here user knows answer, but he/she gets “c “at third place, and calculates new loca-tion for “c”.
(3*3) % 5 = 4.

Now, in new password c shift at fourth position and remaining letters will be dummyletters. Like "fdgcdff ".

Note – if we get new position "0" then all letters should be dummy letters, except thatletter whose positioned want to be changed. Now, user will recognize by the system.

Question	*Question*
Q1	What is your pet name?
Q2	What is your childhood name?
Q3	Who is your favorite Singer?
Q4	Who is your Idle?
Q5	What is your favorite festival?
Q6	What you like to do in your free time?
Q7	What is your lucky color?
Q8	What is your best friend name?
Q9	What is your hobby?
Q10	What type of music you like?

Table1: Question table

			U3	**U4**	**U5**
	Jac		Mo		Till
	Jen	I		Son	
		L	Raf		
	Al ab		Su		Sach
	Div i			Eic	Hol
		Hc		Cric	
			Rec	Gre	Blac
		Ka			
	Lis Mu		Ch	Read g	
		Rc			Class al

Table 2: User Answer Table

U	**Qu**	**Formul**	**Rand No.**	**New Pass**
U	Q	(r.n.*3) %	3	sdfcg
1	Q	(2+r.n.)%	4	hjugt
U	Q	(r.n.*2)+	2	ghtyg
1	Q	(r.n.%3)-	2	hjuik
U5	Q4	(r.n.*2)%3	5	ipkluy

Table 3: Example Table

ISSN: 1832-5505

Applied GIS

Vol-7 Issue-01 Jan 2019

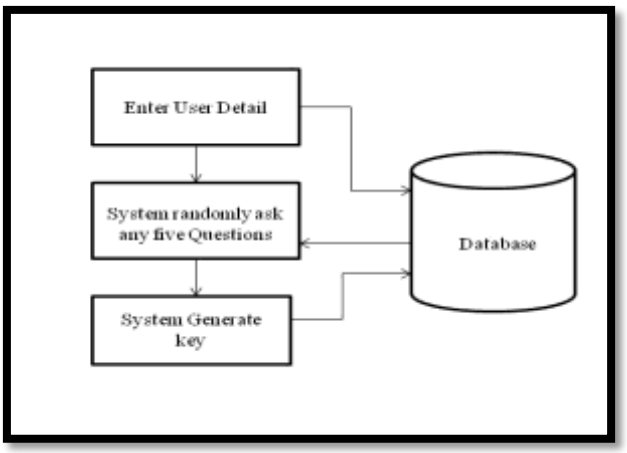

Figure: At Registration time

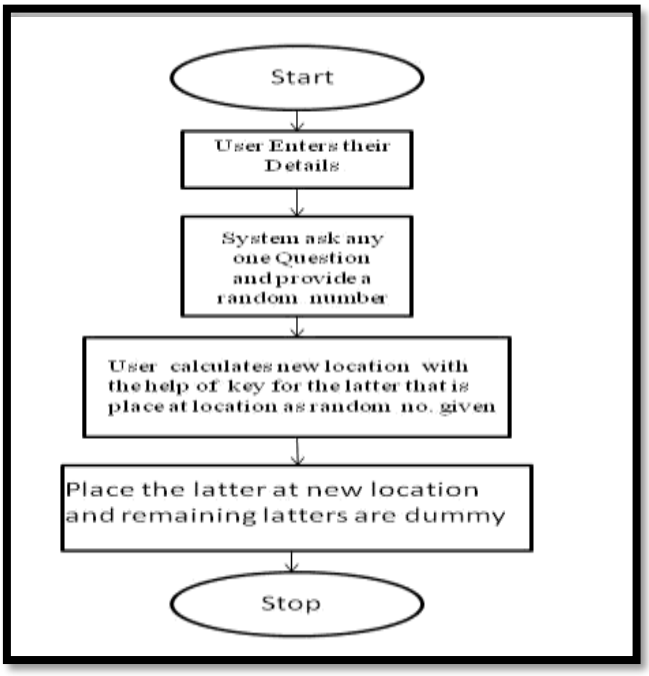

Figure: At Login Time

Password Space

Password space is calculated to check the strength of password. The original pass- word is never used again once the registration is complete. It is only used for calcula- tion of a new position for a character from original password. Therefore, this schemeis save from shoulder surfing attack.
Password space of this scheme is very large so this authentication scheme is more powerful and saves from brute force attack and dictionary attack.
Sample Space for the original password is given as:

$S = A^N$

S= 64^(5) = 1,073,741,824.
Where, N= Length of the password (5-10) A=Total keyboard characters (i.e. 64)

Conclusion

Authentication of the user is an important component in computer security systems. In this paper, we have proposed a simple Text password authentication system, com- bined with some method for text passwords. And try to achieve the best solution for security. This security system is completely resistive of shoulder surfing because formula will be different for the users and if user in some case

does not use the de- vice, then also no one can steal the password i.e. given by user. This scheme saves from aural eavesdropping and visual eavesdropping. No need to access any special features of the device like screen occlusion, brightness low etc. This system provides the security for the Blind as well as normal user of the mobile device.

References

1. Ziran Zheng,Xiyu Liu,Lizi Yin and Zhaocheng Liu," **A Hybrid Password Authentica- tion Scheme Based on Shape and Text**", JOURNAL OF COMPUTERS, VOL. 5, NO. 5, MAY 2010.
2. ShiriAzenkot, Kyle Rector, Richard E. Ladner and Jacob O. Wobbrock, "**PassChords: Se- cure Multi-Touch Authentication for Blind People**", Assets'12, October 22-24, 2012, Boulder,Colorado, USA.
3. Mr. Shailesh.S, Mr. Muhammed ILyas.H, "**Incorporating Homomorphic Encryption with Hybrid Numerical Authentication for Blind Computer Users**", International Con- frence on Intelligent Computing ,Instrumentation and Control Technologies(ICICICT), 2017.
4. Brajesh Kumar Kushwaha, "**An Approach for User Authentication One Time Pass- word (Numeric and Graphical) Scheme**", Journal of Computer Research In Computer Science, Volume 3, No.11, November 2012.
5. Salim Ishtyaq and Lovish Agrawal, "**A New Technique For User Authentication Using Numeric One Time Password Scheme**", International Journal of Computer Sciences and Engineering Vol.-4(5), May 2016.
6. Arash Habibi Lashkari, Azizah Abdul Manaf, Maslin Masrom, and Salwani Mohd Daud," **Security Evaluation for Graphical Password",** DICTAP 2011, Part I, CCIS 166, pp. 431–444, 2011.
7. Swaleha Saeed, M. Sarosh Umar," **A Hybrid Graphical User Authentication Scheme**", International Conference on Communication, Control and Intelligent Systems (CCIS),2015.
8. Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng," **A Shoulder Surfing Resistant Graphical Authentication System**", DOI 10.1109/TDSC.2016.2539942, IEEE, 2015.
9. A.R.Johnson Durai and V .Vinayan, "**A Novel Crave-Char Based Password Entry Sys- tem Resistant to Shoulder-Surfing**", International Journal of Computing Algo- rithm,Volume: 03, May 2014.
10. Akanksha Goakhale and Vijaya Waghmare, "**A Study of Various Password Authentica- ton Technique**", International Conference on Advances in Science and Technology (ICAST), 2014.