Defending Shoulder Surfing Attacks in Secure Transactions Using Session Key Method

M. R.Divya, A.P.Janani,

Abstract— **To improve the security of the various devices, the graphical password is a memorable authentication method for authorization. But when a personal identification number (PIN) entered as a numeric password in mobile or stationary systems, the Shoulder Surfing Attack (SSA) becomes great unease. To avert SSA and to establish a secure transaction, The Session key mechanism is proposed. This mechanism constructed based on the basic layout of a vertical array of digits from 0 to 9 with another array of ten familiar Symbols. This method makes harder for a criminal to obtain PINs even if the iteration are fully observes the entire input of a PIN entry procedure. For Secure transaction, A One Way Hash is generated to Validated PIN and is sent to Server on public channel so that an active attacker cannot extract the PIN by monitoring the channel. Once Server Authenticated the PIN, Quick Response for the Mobile App will be redirected the user to the Services.**

***Index Terms*— Authentication, Personal Identification Number, Shoulder Surfing Attack, Validation, Hash function.**

I. INTRODUCTION

A. Authentication

Authentication is the process of confirming the identification of the person or thing. In private and public computer networks, authentication is usually done through the use of passwords. Passwords are used in, Logging into accounts, emails, Accessing applications, Networks, Web sites, workstations, etc.

The most widely used authentication techniques are, *Token based authentication (Ex.* Key cards, band cards, smart card), *Biometric based authentication* (Ex. Fingerprints, iris scan, facial recognition), and *Knowledge based authentication (Ex.* Text-based passwords, picture-based passwords).

B. Passwords

Password is a covert (word or string) of characters that is used for user authentication to prove his identity and gain access to resources. Two types of Passwords are, Alpha Numeric Password and Graphical Password.

Manuscript received
M.R.Divya *PG Scholar, Computer Science and Engineering, Sri Subramanya College of Engineering and Technology, Palani. Dindigul, India.*
A.P.Janani, *Associate Professor, Department of Computer Science and Engineering, Palani, Dindigul, India.*

Alpha Numeric Password Ideally, the user should combine upper and lower case letters and digits, which should be at least 8 characters. This password should not be a word that can be found in a dictionary or public directory. But two conflicts requirement of the Alpha numeric password is Easy to remember and Hard to guess. But most of the user tends to ignore the second requirement which leads to frail passwords. Numerous solutions have been proposed to avoid this issue. Graphical password is one of the solutions.

C. Graphical Password

Graphical password is an authentication system that works by the user select password using the images, in a specific order, presented in a graphical user interface. For this reason, the graphical-password technique is sometimes called as graphical user authentication. It is more difficult to break graphical passwords using the traditional attack methods such as, brute force attack, spyware or dictionary attack.

An Example of a system that uses an image on the screen and lets the user chooses a password by some clicks. These clicks are the "password", and the user has to click closely to these points again in order to complete the authentication. Such passwords are easier to remember & hard to guess. Two types of Graphical password is, Recall Based Techniques and Recognition Based Techniques.

In *Recall Based Technique***,** A user is asked to reproduce something that the user created or selected earlier during the registration stage. In *Recognition Based Techniques*, A user is accessible with a set of images and the user passes the authentication by recognizing and identifying the images that selected during the registration stage. One of the covert passwords is Personal Identification Number.

D. Personal Identification Number

A personal identification number(PIN) as a 4 digit numeric password in mobile or stationary systems, including smart phones, tablet computers, automated teller machines (ATM), and point of sale (PoS) terminals, a direct observation attack based on shoulder surfing becomes great concern. The PIN entry can be observed by nearby adversaries, more effectively in a crowded area. Usually the same PIN is chosen by a user for various purposes and used repeatedly; a compromise of the PIN may cause the user a great risk. To cope with this problem, which is between the user and the system, cryptographic prevention techniques are hardly applicable because human users are limited in their capacity to process information. Instead, there have been alternative approaches considering the asymmetry between the user and the system.

ISSN: 2278 – 7798

E. Shoulder Surfing Attack

In computer security, shoulder surfing refers to using direct observation techniques, for example looking over someone's shoulder, to find the information. It is generally used to obtain passwords, PIN security codes, and similar data. Shoulder surfing can also be done at a distance using binoculars or other vision - enhancing devices. Inexpensive, miniature closed-circuit television cameras can be covered in ceilings or fixtures to observe the data entry. To avert shoulder surfing, it is advised to shield formalities or the keypad from view by using one's body or one's hand.

There are several technologies were introduced to avoid the shoulder surfing attack. Some of the techniques were discussed in the related work and the Session key method is proposed to avoid the shoulder surfing attack which is more secure and ease to use for the user and difficult for the attacker.

II. Related Work

Mun-Kyu Lee have proposed the Black and White(BW) Method [1] where the regular numeric keypad is colored at random, half of the keys in black and the other half in white (Fig.1), which is called as BW method. A user who knows the correct PIN digit can answer its color by pressing the separate color key. The basic BW method is aimed to resist a human shoulder surfing attack. But if the selected halves were memorized or written on a paper for m, consecutive rounds and recalled to derive their Grouping Patterns, the shoulder surfer could identify a single digit of the PIN.

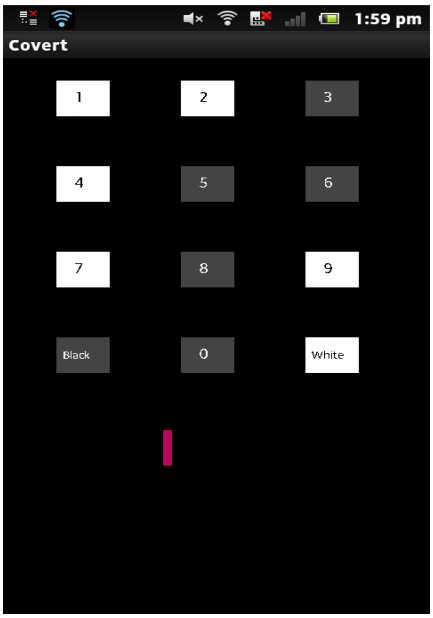

Fig1. Black and White Method

A. D. Luca, E. von Zezschwitz, L. Pichler, and H. Hussmann presented a system using fake cursors [2] to hide password entry on on-screen keyboards. The objective of the fake cursor is, adding overhead to the input to make it hard to follow. The authors propose using several concurrent cursors that move in the exact same way to quickly reach objects on big screen spaces. In this system, only one cursor performs the actual input (Fig.2) while the other cursors act as distraction for an attacker. That is, they do not move in line with the genuine cursor. Since the fake cursors move differently from the active cursor, users can identify it while attackers have difficulties to do so. An attacker may confuse while tracking the PIN entry by the user.

0	1	2	3	4	5	6	7	8	9	⇦
Q	W	E	R	T	Y	U	I	O	P	.
A	S	D	F	G	H	J	K	L	@	,
Z	X	V	B	N	M	#	$	%	&	*

Fig2. Fake Cursor

M. Kumar, T. Garfinkel, D. Boone, and T. Winograd, proposed the gaze-based, password entry [3] which deters or prevents a wide range of these attacks. It is similar to normal password entry, except the place of typing a key or touching the screen, the user looks at each desired character in the sequence (Fig 3). This approach can be used for both with character-based passwords and with graphical password schemes by using an on-screen keyboard.

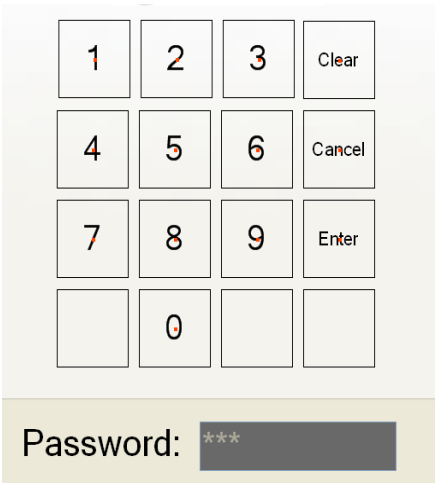

Fig3. Gaze – based, password entry

Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, Designed leakage resilient password entry[4] scheme that leveraging on the touch screen feature of mobile devices. It improves leakage resilience while preserving most benefits of legacy passwords.

S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, proposed the Convex Hull Click Scheme [5] is an effort to develop security innovation. It aims to motivate the user with a fun, game-like visual environment designed to develop positive user affect and counterbalance the drawback of the longer time to input the password. The user wants to locate three or more pass-icons in the window (Fig 4) and mentally form the convex hull of those pass-icons. The user was specifically told to click within the convex hull. The experimenter also instructed the participant not to move the mouse from one pass-icon to another to "trace" the boundaries of the convex hull, since that could reveal the pass

ISSN: 2278 – 7798

icons to an attacker. The experimenter explained to the user that feedback on correctness would be given only at the end of the whole password input, not between each of the five challenges. The process took approximately ten minutes.

Fig4. convex hull with 3 pass-icons

D. Davis, F. Monrose, and M. K. Reiter, proposed the Graphical password scheme [6] which support graphics and a mouse or stylus entry. Author implemented the two schemes. One is Face scheme and another one is story scheme. In the Face scheme (Fig 5.1), the password is a collection of faces. Each faces selected from a distinct set of faces. Each of the faces randomly chosen from a set of faces that stored in the database. Faces are unique and do not repeat for the single user. These images are visible in the grid on the screen. The user wants to select the image as a password. In story scheme (Fig 5.2), the images depict everyday objects, materials, animals, sports; any pictures which will be made a story. The same set of images is shown to the user, but that images are shuffled in each round.

Fig5.1 Face Scheme

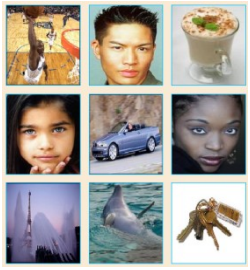

Fig5.2 Story Scheme

A. Bianchi, I. Oakley, and D. S. Kwon proposed A novel unimodal non-visual interaction technique [7] for PIN entry at public terminals, such as bank ATMs or door-locks, that is both secure (e.g. Resistant to brute force and observation attacks) and usable. The proposed technique is based on temporal numerosity, the human ability to accurately, confidently and rapidly count the number of cues presented in rapid temporal succession.

C. S. Kim and M.-K. Lee, proposed the Secure and user friendly PIN entry method[8]. Author proposed the system that assesses the recognizable facial images for automated teller machine applications. This achieves the robustness against facial postures and acceptable partial occlusions using a component based approach and inattentiveness toward the clarification environment through the grayscale image – based methods.

Q. Yan, J. Han, Y. Li, and R. H. Deng, proposed a Leakage-Resilient Password Entry [9] on Touch screen Mobile Devices. The authors implemented a concise yet effective authentication scheme, Cover, Pad which is designed for password entry on touchscreen mobile devices. Cover Pad improves the leakage re-silence of password entry while retaining most benefits of legacy passwords. Leakage resilience is achieved by utilizing the gesture detection feature of touch screen in forming a cover for user inputs. This formed cover is used to deliver hidden message safely.

A. Bianchi, I. Oakley, and D.-S. Kwon, introduced a Spinlock technique which is novel any model non – visual interaction technique [12] which is used for PIN entry in public terminals such as ATMs, door locks, etc. This is a more secure technique which is resistant to brute force and observation attacks. Spinlock is based on the rotating dial for traditional safe. This system unlocked by input a dial as a clockwise and anticlockwise rotation. The more safe PIN entry will be 2-anti clockwise, 8-clockwise, and 7–clockwise. Spinlock was introduced for the Apple iPhone and iPod touch devices. The users interact with the system by selecting the edge of the circular dial widget and drag the cursor around the rim.

A. Bianchi, I. Oakley, and D. S. Kwon also proposed A novel observation-resistant authentication system [11] uses either audio or haptic cues to confuse a PIN entry process. This study showed the feasibility of the concept in terms of task completion time, error rate and user acceptance.

Andrea Bianchi, Ian Oakley, Dong Soo Kwon proposed the Uni-model SHK [10] that perform the simple act of exploring tactons and immediately performing selection actions to enter PIN items in the same physical space appears rapid, easy to grasp and effective.

III. Objectives & Overview Of The Proposed Mechanism

A. Objectives

The main aim of this project is to prevent human shoulder surfing attack and to establish a secure transaction between the mobile App and Server by implementing the Session Key Method.

B. Overview of the proposed Mechanism

Session Key Method is a new Graphical PIN-entry method. The basic layout of this method comprises a vertical array of digits from 0 to 9, with another array of ten familiar objects such as +, *, /, @, $, etc. The total of four rounds used to select the PIN. By using this method, the Shoulder surfing attack will defend because, this method is complex to the attackers to guess the PIN. In fact, if the attacker recorded the

ISSN: 2278 – 7798

PIN entry of the user, Then also attacked could not find the PIN.

IV. SESSION KEY METHOD

The session key method has the 4 rounds. The first round is the session key decision round, and the remaining three rounds are PIN-entry rounds.

In the *session key decision round*, ten randomly arranged objects (Fig 6) are displayed to the user. The user can decide any of the symbols and assign it to the 1st digit of the PIN using the "Up" or "Down" buttons. If the user presses the "Up" button, then the symbols move immediately upper wards. If the user presses the "Down" button, then the symbols move immediately downwards.

Using this Up and Down buttons, user moves the decided key to the PIN and then presses "OK.". While the user moves the symbols, then all the symbols will move Up and Down in which direction the user moving the symbols. So, if the shoulder surfer watches the user enters or even though if attacker records the process, can't find the PIN. In next round, the symbols were shuffled with new symbols too. So this is too tuff to guess or find the PIN by this Session key logon procedure. Now the Session key was decided by the user as well as the 1st digit of a PIN is validated. This same Session key (Symbol) must use for remaining 3 rounds which is the PIN entry method.

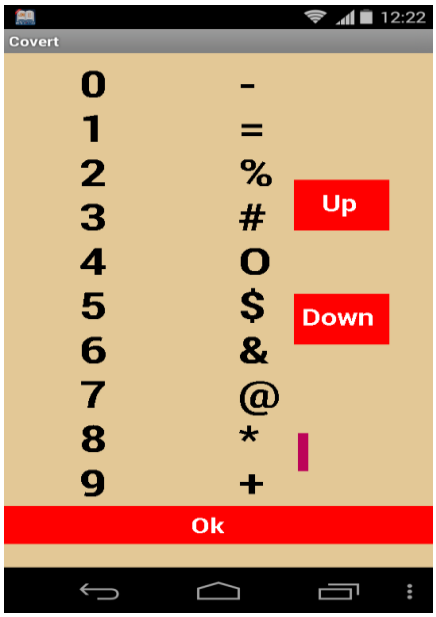

Fig 6. Session Key Method

The remaining 3 rounds are *PIN-entry rounds*, in which the *i* th digit of the PIN is entered in the *i* th round (Here *i* = 2, 3, 4). In each of these each rounds, the 10 symbols were shuffle. The user wants to assign the session key for each round using the "Up" and "Down" button. In each round user presses the 'OK" button. When the user presses the OK button, then the PIN considered.

V. AUTHENTICATION AND SERVICES

Once the User Entered Pattern is manipulated and a PIN is Identified, It will be checked with the Local Database provided by Android OS using SQL Lite. This Process is to prevent unwanted Server end process handling playful requests. A One Way Hash is generated for the Validated PIN and is sent to Server in public channel so that an active attacker cannot extract the PIN by monitoring the channel. Once got authenticated by Server a Quick Response to the Mobile App will redirect the user to the Services. In ATM Services Cash Withdrawal, Deposit and Fund Transfer can be done securely using the concept of Virtual Money which is already employed by many other applications successfully in the Web. This reduces the overhead complexities in the server and will provide the User an ease of access to the Banking Services.

A. One-way Hash Function (HMAC)

HMAC represents the Hash Message Authentication Code. HMAC is a many to one function that it condenses a variable-length message M to a fixed sized message by using the secret key K, through some compression function. Hash functions are generally faster. Hash includes a key along with a message. Original proposal of a hash function is,
Keyed Hash = Hash (Key | Message).

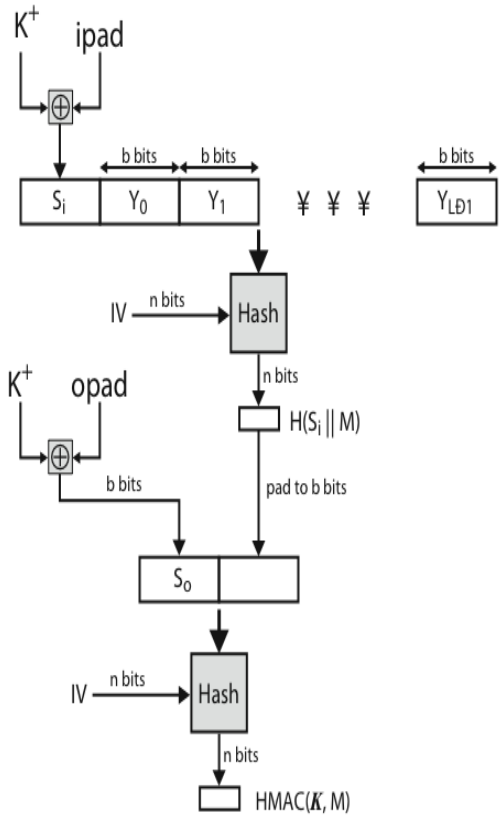

Fig7. HMAC overview

$HMAC_K = Hash[(K^+ XOR opad) || Hash[(K^+ XOR ipad)||M)]]$

where K^+ is the key padded out to size and ipad, opad (Fig 7) are the specified padding constants overhead is just 3 more hash calculations than the message needs alone any hash function can be used. Eg. MD5, SHA-1, RIPEMD-160 and Whirlpool.

The security of HMAC relates to that of the primary hash algorithm attacking HMAC requires either the brute force attack on key used and birthday attack (but since keyed would need to observe a very large number of messages)

ISSN: 2278 – 7798

choose hash function used based on speed verses security constraints.

VI. ARCHITECTURE OF THE PROPOSED SYSTEM

System architecture is the conceptual sculpt that defines the structure, activities, and views of a system. An structural design description is a formal description and representation of a system, organized in some manner that supports analysis about the structures and activities of the system. System architecture can cover the system components, the superficially visible properties of those components, the associations between them. It can bid a plan from which the products can be procured, and the system developed, that will work together to implement the overall coordination. The Architecture of this project is shown in the fig 8.

The architecture gives the detail description about the process. First the user wants to register their details.

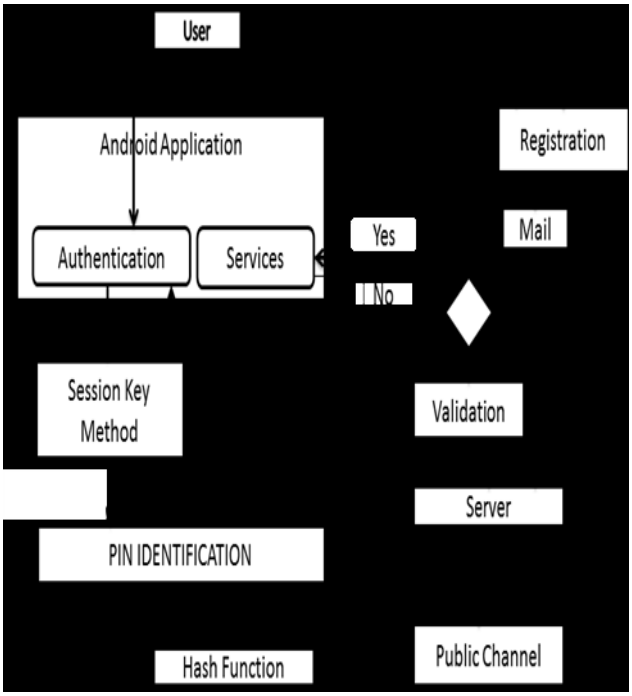

Fig8. Architecture Diagram

The details are register in the server through the public channel. Once the registration, User will be provided with a Unique PIN Sent to Their Respective Mail ID. Once it got validated a User will be able to access our Application by entering the Username and Password Chosen at the time of Registration. Then our application will provide users its services. Then if the user will go with ATM services, user is asked to provide the PIN digit. So anytime the user can logon and access their account. First the user wants to enter the Password for the authentication. Once the user entered the password, then the local database checks that the PIN is valid or not. If PIN is not valid, then it gives another chance to enter the PIN. If again PIN is invalid, then gives the 3rd chance. If the third chance also invalid, then the alert message will automatically send to the user and the details were stored in the database.

Fig 9. ATM Services

If the entered PIN is valid, then the one way hash function is generated for the validated PIN. Then the validated PIN converted as a digital – signature, which is in an unreadable format. This digital signature is sent to the server by the public channel. Now the server reads the PIN and authenticates it. Once the server confirms that the user is authorized user, then the server allow the user to use the services. Here the service represents the ATM services (Fig 9), as Cash Withdrawal, Deposit, Fund Transfer and Balance information can be done securely. The authorized user can do their transactions easily and much efficiently with highly secured password entry.

VI. CONCLUSION

The main focus of this proposed system is to give a more secure PIN entry method for common user authentication with high usability and give compatibility and cost effectiveness (means no additional expensive hardware) by the session key method. Session key method is a graphical password method which is easier to the user as well as hard to the shoulder surfer. The one way HMAC algorithm is used to secure the PIN after the logon procedure. In this system, the human shoulder surfing attack is prevented and a secure transaction between the mobile App and Server is established by using The Session Key Method.

REFERENCES

[1]. Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry," In Ieee Transactions On Information Forensics And Security,VOL. 9, NO. 4, APRIL 2014, pp. 1556-6013.

[2]. A. D. Luca, E. von Zezschwitz, L. Pichler, and H. Hussmann, "Using fake cursors to secure on-screen password entry," in *Proc. CHI*, 2013, pp. 2399–2402.

[3]. A. D. Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN: Securing PIN entry through indirect input," in *Proc. CHI*, 2010, pp. 1103–1106.

[4]. M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in *Proc. SOUPS*, 2007, pp. 13–19.

ISSN: 2278 – 7798

[5]. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proc. AVI*, 2006, pp. 177–184.

[6]. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. 13th Conf. USENIX Security Symp.*, 2004, pp. 151–164.

[7] D. S. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: More secure password entry on public touch screen displays," in *Proc. 17th Austral. Conf. Comput. Human Interaction OZCHI*, 2005, pp. 1–10.

[8] C. S. Kim and M.-K. Lee, "Secure and user friendly PIN entry method," in *Proc. 28th Int. Conf. Consum. Electron.*, 2010, p. 5.1–1.

[9]. Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Designing leakage resilient password entry on touchscreen mobile devices," in *Proc.ASIACCS*, 2013, pp. 37–48.

[10]. A. Bianchi, I. Oakley, and D. S. Kwon, "Counting clicks and beeps:Exploring numerosity based haptic and audio PIN entry," *Interact.Comput.*, vol. 24, no. 5, pp. 409–422, 2012.

[11].A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," in Proc. TEI, 2011, pp. 197-200

[12].Andrea Bianchi, Ian Oakley, Dong Soo Kwon, "The Secure Haptic Keypad: A Tactile Password System," in CHI 2010 Input, Security, and Privacy Policies April 10–15, 2010, Atlanta, GA, USA

[13].W. Moncur and G. Leplâtre, "Pictures at the ATM: Exploring the usability of multiple graphical passwords," in *Proc. CHI*, 2007, pp. 887–894.

[14].R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44, no. 4, article 19, pp. 1–41, 2012.

[15].H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *Proc. AINA Workshops*, 2007, pp. 467–472.

[16].A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 4th USENIX Conf. Offensive Technol. WOOT*, 2010, article 1–7, pp. 1–10.

[17].E. von Zezschwitz, A. Koslow, A. D. Luca, and H. Hussmann, "Making graphic-based authentication secure against smudge attacks," in *Proc. IUI*, 2013, pp. 277–286.

ISSN: 2278 – 7798