Shoulder Surf Resistant Screen Locking for Smartphones: A Review of Fifty Non-Biometric Methods

Hazleen Aris
Institute of Informatics and Computing in Energy
Universiti Tenaga Nasional
Kajang, Malaysia
hazleen@uniten.edu.my

Wira Firdaus Yaakob
Sapura Secured Technologies
Kuala Lumpur, Malaysia

***Abstract*—With a lot of personal information being stored in the smartphones nowadays, there is an urgent need to protect them from unauthorised access. The first line of defense of a smartphone is its screen lock. Thus, many screen locking methods have been designed with the aim of minimising, if not eliminating the chances of unauthorised access through attacks such as shoulder surfing. This paper provides an overview on the state of research on non-biometric shoulder surf resistant screen locking methods with the aim to identify the techniques used by these methods in defending against shoulder surf attacks. A systematic literature review performed found a total of 84 methods designed and developed to date, which covers the time span of ten years. A notably higher number of new methods was published each year during the last five years and the number continues to grow steadily, indicating the relevance and currentness of the research area. Non-biometric screen locking methods in particular was found to constitute the majority of the methods with 50 methods. During the analysis, these methods were first vertically classified into PIN-based, pattern-based and image-based. Then they were horizontally categorised into those that use fixed password and those that use one-time password to unlock the screen. At the end of the analysis, a total of ten shoulder surf resistant techniques used in these methods was extracted. These techniques were used either in isolation or in combination with one another. Findings from this study would be useful in providing the state-of-the-art summary of the non-biometric shoulder surf resistant screen locking methods.**

***Index Terms*—smartphone security, graphical password, touch screen, authentication, systematic review**

I. Introduction

Smartphones have become a necessity to most people nowadays. Due to its sophisticated and technologically advanced features, their use has extended beyond phone calls and short messages. A survey showed that the significant majority of users store their personal data in the smartphones [1]. Thus, the need to protect the smartphones from unauthorised access has become even more important. The first line of defense in protecting the phone from unauthorised access is its screen lock. Screen lock is a security feature for computers and mobile devices that helps prevent unauthorised access to the devices. It requires a specific action to be correctly performed by the users, before they can be used [2]. By employing a screen locking mechanism, the attackers will not be able to access the applications or obtain the personal information contained in the smartphones, even if they manage to get hold of them. Amongst the widely used screen locking methods are the personal identification numbers (PINs) and pattern. PINs resembles the conventional authentication performed at the automated teller machine where a series of between four to six digits serves as the unlock code. Users tap the digits in sequence on the response keypad to unlock the phone. In an effort to improve the usability and memorability of the unlock code, pattern was introduced in Android smartphones. In pattern lock, points located on an $n \times m$ grid are used instead of the digits. To unlock, user draws a pattern that crosses some of the points, where a point can only be used once and cannot be skipped or jumped over in order to go to another point.

However, these conventional screen locking methods are said to be very vulnerable to the (soft) side channel attacks, such as shoulder surf attack. In shoulder surfing, the attacker secretly observes as the user is unlocking the phone in order to 'steal' the unlock code. This is traditionally done by observing from over the latter's shoulder, hence the name. Due to the vulnerability of the conventional methods, a number of alternative screen locking methods have been proposed by the researchers that use various techniques to prevent shoulder surf attacks. In this study, these methods are being reviewed, with the objective of identifying the techniques used. This objective is attained by answering the following research questions.

- RQ1 How many shoulder surf resistant screen locking methods are published to date?
- RQ2 How many of these methods are non-biometric methods and what are they?
- RQ3 How can the non-biometric methods be classified?
- RQ4 What are the techniques used to improve resistance against shoulder surf attack in these methods?

A systematic literature review (SLR) was performed to answer the first two questions followed by a qualitative analysis to answer the remaining questions. From the SLR, a total

978-1-5386-6925-9/18/$31.00 ©2018 IEEE

of 84 methods was identified from 90 selected publications. These methods can be broadly classified into biometric, non-biometric and hybrid. Fifty out of the 84 methods are non-biometric. Two dimensional classification was performed on the non-biometric methods. The first dimension categorises them into PIN-based, pattern-based and image-based. The second dimension categorises them into fixed password and one-time password. At the end of the analysis, a total of ten techniques used by the methods to improve their resistance against shoulder surf attacks was identified. The rest of the paper is organised as follows. Section II describes about the systematic literature review method employed. Results from the literature search are presented in section III and discussed in section IV. Section V concludes the paper.

II. Method

The systematic literature search performed in this study comprised the following steps.

1) Formulate the search string
2) Select the databases
3) Determine the selection criteria
4) Identify articles to be included based on the selection criteria

To begin with, two key terms were identified as central to the study; *screen lock* and *shoulder surf*. To formulate the search string, the different ways on how they are being used in the literature were identified by performing initial literature search. The result is shown in Table I.

TABLE I
Basic Search Terms and Their Variations

Base Term	Variation	Base Term	Variation
screen lock	screenlock	shoulder surf	shoulder surfing
	screen locking		shoulder surfer
	screenlocking		shoulder surfers
	screen unlock		shoulder-surf
	screen unlocking		shoulder-surfing
	screen (un)lock		shoulder-surfer
	screen (un)locking		shoulder-surfers
	screen un-lock		shouldersurf
	screen un-locking		shouldersurfing
			shouldersurfer
			shouldersurfers

Thus, the following search string was formulated to be used in the systematic search.

(“screen lock” OR screenlock OR “screen locking” OR “screen unlocking” OR “screen unlock” OR “screen (un)lock” OR “screen (un)locking” OR “screen un-lock” OR “screen un-locking”) AND (“shoulder surf” OR “shoulder surfing” OR “shoulder surfer” OR “shoulder surfers” OR shoulder-surf*)*

Six scholarly databases were included in the search; Google Scholar, IEEExplore, ACM Digital Library, Scopus, Science Direct and Springer Link. These are the well known databases for technical publications related to the topic under study. No restriction was put on the publication period since research on the screen locking method is relatively new. The first touch screen smartphone was released in 1993 [3], which is around 25 years back and it is expected that research on screen locking for smartphones should have only started after that. Table II shows the inclusion and exclusion criteria used in selecting the articles to be included in the review. Results returned from the six databases were first checked for duplications prior to undergoing the following selection process.

TABLE II
The Inclusion and Exclusion Criteria Used in the Study

Inclusion Criteria	Exclusion Criteria
The method is meant for screen locking, not for other authentication such as login	The work is not published in English
Screen locking method is proposed in the study and not just applying existing or other’s method	The article plagiarise another (earlier) publication
The objective of the method is to improve resistance against shoulder surf attack	The method is designed for specific type of users, e.g. children, visually impaired
The method is meant to be implemented on or is compatible with touch screen smartphones	

1) **Title reading.** In title reading, selection is made based on the title of the source. Three possible outcomes of the title reading are included (INC), excluded (EXC) and undecided (KIV). A source is included if the title clearly indicates that all selection criteria are met. A source is excluded if the title clearly indicates that any one of the criteria is violated. If decision cannot be made based on the title, a source is classified as undecided and proceeds to the abstract reading stage for further evaluation.
2) **Abstract reading**. In this stage, results with the KIV status from the title readings stage would undergo abstract evaluation after which their status would either be changed to INC or EXC, or remains unchanged. A source is included if the abstract clearly indicates that all selection criteria are met. A source is excluded if the abstract clearly indicates that any one of the criteria is violated. If a decision still cannot be made based on the abstract, the KIV status of the source is retained and the source proceeds to the adaptive reading stage.
3) **Adaptive reading.** In adaptive reading, full text of the sources with the KIV status are downloaded. However, only the relevant parts of the text would be read to verify if all of the selection criteria are met. This is the last stage of the selection process and is usually needed for articles that are not well structured. At the end of this stage, an article is either included (INC) or excluded (EXC).

It is expected that one shoulder surf resistance screen locking method may be presented in more than one publication and vice-versa. Therefore, a step to merge and unmerge the methods is performed. In this step, a number of documents that originate from the same authors and/or co-authors that describe about the same method but from different perspective is

merged under one method. Likewise, methods that come from the same article will be separated (unmerged). The last step prior to finalising the number of evidence to be included for analysis was quality assessment. Selected sources are checked for quality based on the recommendation in [4] to confirm that they comply to the minimum quality requirements.

III. Results

When the systematic literature search ended on 30th July 2018, a total of 595 results was returned from the six scholarly databases searched, with the distribution as shown in Table III. Eighty seven duplicates were found and subsequently excluded after combining the results from the different databases, giving a new total of 508 unique results that went to the selection process. The majority of the results (263) was excluded during the title reading stage. A further 20 results were excluded at the abstract reading stage and the final 135 results were excluded at the end of the adaptive reading stage. This gave us a total of 90 articles selected for the analysis; 13 from the title reading stage, 12 from the abstract reading stage and 65 from the adaptive reading stage. All of the 90 articles have passed the quality assessment performed. Fig. 1 summarises the selection process together with the number of results included and excluded at each stage.

TABLE III
Raw Results Returned from the Systematic Search

Database	Result[a]	Duplicate[b]	Non-English	Subtotal
Google Scholar	254	10	10	234
IEEExplore	178	0	1	177
ACM Digital Library	122	0	0	122
Scopus	31	0	0	31
Science Direct	10	0	0	10
Springer Link	21	0	0	21

[a]Excluding patents.
[b]Duplication within the same database.

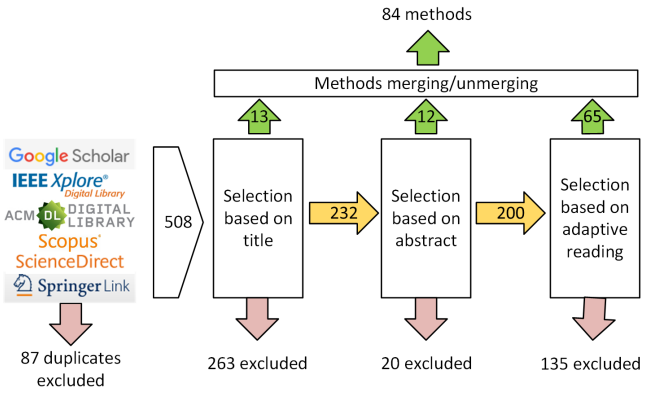

Fig. 1. Summary of the selection and methods extraction processes.

Although no time range was specified when performing the literature search, the earliest work on shoulder surf resistant screen locking method was found published in 2009 and the latest in 2018, thus covering a span of ten years. The most number of articles were published between 2014 and 2018 as shown in Fig. 2. Articles published in 2018 are steadily catching up with six already published as at July 2018. After the merging and unmerging process, a total of 84 unique shoulder surf resistant screen locking methods was compiled and this answers the first research question (RQ1).

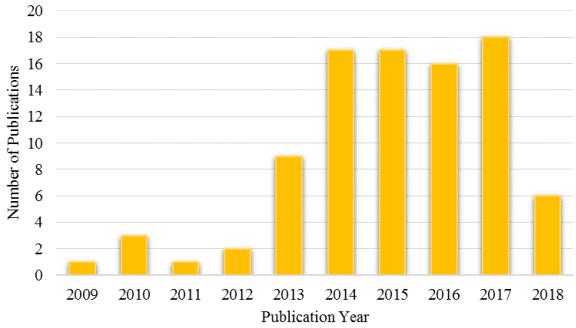

Fig. 2. Distribution of selected articles across the ten years.

IV. Analysis and Discussion

The preliminary analysis performed on the 84 methods found that at the highest level of abstraction, they can be categorised into biometric, non-biometric and hybrid. Biometrics screen locking methods use users' characteristics as the unlock codes, which can be further divided into physiological and behavioural. Physiological biometric method unlocks the phone based on who you are, using the techniques such as face and thumb print recognition. Behavioural biometric method on the other hand unlocks the phone based on how you behave, using the techniques such as gestures recognition. Non-biometric screen locking methods, which is the focus of this paper, do not use unique users' characteristics to unlock. As can be seen in Fig. 3, they constitute the majority of the methods where 50 out of the 84 methods (59%) belong to this category. Table IV lists the fifty non-biometric screen locking methods together with the sources, the publication types and years of publication. This answers the second research question (RQ2). As can be seen from the table, the majority of the methods were published as conference papers (31), followed by journals (12) and work in progress or posters (7).

Answering the third research question (RQ3) on the means to classify the non-biometric shoulder surf resistant screen locking methods is quite challenging and far from straightforward. This is due to the numerous techniques used in making the methods resistant against the shoulder surf attack. A number of different classifications were attempted at in order to identify the one that would be able to provide the most meaningful overview of the methods. After much deliberation, two dimensional classification consisting of the vertical and horizontal components was used. The vertical classification is based on the nature of the *password* and the horizontal classification is based on how the password

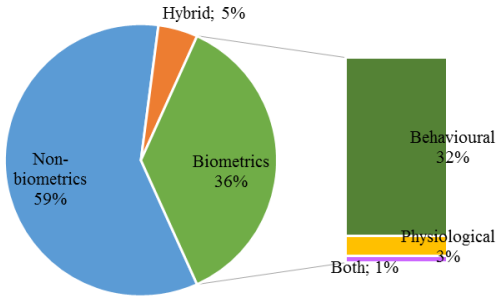

Fig. 3. Distribution of biometric, non-biometric and hybrid methods.

is used to unlock the phone. The password (PWD), in the context of the discussion in this paper refers to the piece of information that the user has to remember to be able to unlock the phone. For the vertical classification, three main groups of the passwords are PIN-based, pattern-based and image-based. In the PIN-based methods, the passwords are either numeric or alphanumeric. In the pattern-based methods, the passwords are made up of patterns to be matched and in the image-based methods, the passwords comprise images, either 2D or 3D.

With regard to how the passwords are used to unlock the phones (horizontal classification), our analysis found that they are either used *directly* or *indirectly*. Direct use means that the remembered passwords are entered as-is to unlock the phones, i.e. the password is the unlock code (Eq. 1). In indirect use, a password is not entered directly, but rather used as the cue to obtain the one-time password (OTP) to unlock the phone. The cue can either be used on its own (Eq. 2) or in conjunction with a *token* that is communicated to the user at the beginning of the unlock session (Eq. 3). The former is termed implicit token and the latter as explicit token in the content of this study. An OTP is valid only for one unlock session. The attacker is therefore prevented from unlocking the phone because each unlock session requires a different OTP.

$$UC = PWD \tag{1}$$

$$UC = f(PWD) \tag{2}$$

$$UC = f(PWD + Rand(TKN)) \tag{3}$$

Where:
UC is the unlock code
PWD is the remembered password and
TKN is the token

Based on the above classifications, the following set of questions were composed to help us in classifying the 50 non-biometric shoulder surf resistant screen locking methods.

1) Is there a password to be remembered?
2) Does the user enter the remembered password to unlock the screen?
3) Is the password used as cue to obtain the unlock key?
4) Is the unlock key explicit?
   a) Is the token transmitted using secondary channel?
5) Is the unlock key implicit?
6) Is the password based on PIN?
7) Is the password based on pattern?

TABLE IV
DEMOGRAPHICS INFORMATION OF THE EVIDENCE INCLUDED IN THE STUDY

ID	Method Name	Source	Publication Type	Year
M1	Image-Recall[c]	[5]	Conference	2010
M2	PassMatrix	[6]	Journal	2018
M3	Stroke-based[c]	[7]	Conference	2009
M4	TictocPIN	[8]	Journal	2015
M5	Index-Key[c]	[9]	Conference	2015
M6	Chameleon Dial	[10]	Work in progress	2015
M7	Glass Unlock	[11]	Conference	2015
M8	IllusionPIN	[12]	Journal	2017
M9	ColorPIN	[13]	Conference	2014
M10	ShaPIN	[13]	Conference	2014
M11	Operation Code	[14]	Conference	2010
M12	Turn-and-Tap[c]	[15]	Conference	2017
M13	Puzzle Auth.[c]	[16]	Conference	2014
M14	RSVP	[17]	Journal	2017
M15	GesturePuzzle	[18]	Conference	2012
M16	Pattern-Based[c]	[19]	Conference	2015
M17	LIN_4 and LIN_5	[20]	Journal	2014
M18	SteganoPIN	[21]	Journal	2017
M19	SWIPASS	[22]	Journal	2016
M20	SysPal	[23]	Conference	2017
M21	EvoPass	[24]	Journal	2017
M22	3DPIN	[25]	Conference	2014
M23	GP-DIP	[26]	Conference	2014
M24	Stamp-Grid[c]	[27]	Conference	2011
M25	Tiles	[28]	Conference	2012
M26	LSES/LSSI	[29]	Journal	2016
M27	XSide	[30] [31]	Conference	2013, 2014
M28	Pattern-Ext[c]	[32]	Journal	2016
M29	TMD	[33]	Conference	2013
M30	mtaPIN	[34]	Journal	2014
M31	EmojiAuth	[35]	Conference	2017
M32	PassApp	[36]	Conference	2015
M33	Picassopass	[37]	Work in progress	2013
M34	V8D	[38]	Conference	2015
M35	VDA	[38]	Conference	2015
M36	TiltPass	[39]	Work in progress	2018
M37	TinPal	[40]	Work in progress	2018
M38	VAP Code	[41]	Journal	2016
M39	YCS-MyPIN[c]	[42]	Conference	2016
M40	ColorSnakes	[43]	Conference	2015
M41	Random-Pad[c]	[44]	Conference	2017
M42	ChordPass	[45]	Work in progress	2013
M43	VibraInput	[46]	Work in progress	2014
M44	Spiral Lock	[47]	Conference	2014
M45	SwiPIN	[48]	Conference	2015
M46	SwitchPIN	[49]	Conference	2014
M47	Phone Lock	[50]	Conference	2010
M48	WearLock	[51]	Conference	2017
M49	Pass-O	[21]	Work in progress	2017
M50	NumberPIN	[13]	Conference	2014

[c]Name given by the authors for the purpose of this study.

8) Is the password based on image?

Table V shows the result of the horizontal and vertical classifications. As can be seen from the table, the majority of the non-biometric screen locking methods proposed is largely PIN-based (27 methods) followed by the image-based (12 methods) and the pattern-based (10 methods). One method in particular (M48) could not be classified under any of the groups. In this method, there is no password that the users have to remember. They just need to remember to wear their smart watch with them all the time.

TABLE V
SUMMARY OF METHODS CLASSIFICATION

Method	PIN-based	Pattern-based	Image-based
Fixed password	M5, M6, M8, M12, M13, M16, M17, M24, M30, M34, M39, M40, M41, M42, M44, M45, M49, M50	M20, M26, M27, M28, M29, M36, M37, M38	M1, M10, M14, M15, M21, M25, M31, M33
OTP with explicit token	**Primary:** M11, M18, M22 **Secondary:**M4, M7, M9, M35, M43, M46	**Secondary:** M47	**Primary:** M2
OTP without token	-	M3	M19, M23, M32

With regard to the last research question (RQ4) on the techniques used to improve resistance against shoulder surf attack, the discussion is presented according to the classification made in Table V, which is presented next.

A. PIN-Based

From the 27 PIN-based methods, 18 of them belong to the direct/fixed category, nine belong to the OTP with token and none belong to the last category (OTP without token).

1) Fixed Password: Since the user enters the remembered PINs directly in this approach, the PINs are fixed and are the same for all unlock sessions. Therefore, there is a need to 'cover' the PINs from the attacker's view during entry. A straightforward approach is to increase the complexity and/or password space by randomising the (response) keypad so that different points are seen tapped on or swiped from during each unlock session, despite the same PINs. This is the approach used in M13, M40, M41, M45 and M50. Another approach is by rearranging the keypad, e.g. by using circular grid (M44, M49). However, keypad randomisation and rearrangement is vulnerable to repeated shoulder surf attacks such as camera attack. After a number of observations, the attackers would be able to identify the numbers that are always used in all unlock sessions. Therefore, to further increase the resistance against shoulder surf attack, keypad randomisation is usually combined with one or more other techniques. For example, in M41, 'decoy' PINs are included in between the correct PINs. This technique is also used in M16, were the decoy PINs are included either before or after the correct PINs. The decoy PINs will be different each time since the keypad is randomised, which makes it more difficult for the attacker to guess the correct PINs combination.

In M45, each PIN on the randomised keypad has to be swiped in a certain direction that is randomly determined during each unlock, a technique that is also used in M34. This means that each PIN is associated with a *property*, e.g. direction, and its value, e.g. down, and both the PINs and their property values have to be correct before the phone can be successfully unlocked. The property can be different for each PIN, or the same for all PINs. For example, in M13, all PINs have to be arranged in the same direction. Other forms of the property include the index key or symbol or location to align each PIN with (M5, M6, M12, M17), pattern of entering the PINs (M30) and the tap duration for each PIN (M 39). Some of the properties are assigned randomly during each each unlock session that makes it difficult for the attacker to guess. The M45 method is also further protected from the shoulder surf attack by means of the indirect touch input where the user can swipe from any location on the screen relative to the PINs. This will further obfuscate the PINs from the attacker. Indirect touch input is also used in M40, together with the fake input technique. In this technique, which is also applied in M24, other 'potentially correct' PINs are also shown the moment each corrent PIN is entered to camouflage the correct PINs. Finally, an approach is also seen that leverages the fact that the attacker usually stands at a different location from the user and hence, will be viewing the phone screen from a different angle. This approach uses software manipulate the keypad view in such a way that the attacker views the keypad differently from the user (M8). Multi-touch screen is also seen explored (M42).

2) One-Time Password (OTP): In the PIN-based methods, only OTP with explicit token technique is seen used. Primary (M11, M18) and secondary channels are used to communicate the token. When primary channel is used, additional measure is seen taken because the primary channel is exposed to the attacker's view. For example, M22 uses special 3D screen property to ensure that the token is only visible to the user. An attacker viewing from a different angle will not be able to see it, an approach that is similar to M8 but with different implementation. In M18, user needs to scoop their hand above a specific point in the screen to reveal the token in the form of challenge keypad. To overcome the risk of exposing the tokens to the attacker, secondary channels are used to communicate it to the users. These include using specialised hardware such as Google glass and hololens (M7, M46), and vibration (M4, M9, M35, M43).

B. Pattern-Based

In pattern-based methods, the passwords that the users have to remember are stroke patterns or points to swipe through to complete a pattern. Because each point in a pattern-based methods looks the same, keypad randomisation is not a relevant technique to be used. One prevalent technique used in pattern-based is by increasing the complexity of the pattern and/or the password size, such as by increasing the number of

pattern strokes (M26), by allowing pass points to be repeated, temporally and spatially (M28), by allowing the pattern grid to extend beyond a page (M29) to complicate attacker's view, and by influencing the users to choose more complicated patterns during setup (M20, M37). Another approach that requires the use of specialised hardware is to hide part of the unlock code from the attacker's view by stroking some of the input patterns on the back side of the phone (M27). A similar approach in M36 is making use of the gyroscope found in the later versions of the smartphones. The remaining pattern based methods are using the techniques that are similar to the PIN-based methods, i.e. redundancy (M20), behavioural property (tap duration) (M38), OTP with explicit token (vibration) (M47) and OTP without token (M3).

C. Image-Based

In the image-based methods, the passwords that the users have to remember are made up of images. These images can be the photos taken using the phone's camera or saved from the internet, 2D images, drawings or icons. All image-based methods are seen using the $m \times n$ grid where the pass images together with the decoy images are presented in random order. In the simplest implementation, the locations of the pass images, or a selection of them, will be randomised during each unlock session (M25, M31). While able to increase complexity, grid randomisation per se is prone to repeated attack as explained earlier. Therefore, grid randomisation is also found combined with one or more other techniques, i.e. redundancy (M1, M10, M15, M33) and image degradation (M14, M21). In M14, the randomisation of grid is temporal, rather than spatial. One image based method that falls under the OTP with explicit token category is M2. Since primary channel is used to communicate the token to the user, an additional measure is added where user has to scoop their hand above a specific point on the screen to reveal it, a technique that is similar to M18. The remaining three image-based methods fall under the OTP without token category where the remembered images serve as hints to determine the swipe direction (M19), the portion used for the image challenge (M23) and the app icons installed in the phone (M32).

In summary, a total of ten techniques was found used in the existing non-biometric shoulder surf resistant screen locking methods as shown in Table VI. Some of these techniques are used in isolation while some are used in combination by the methods in our study. With regard to the threat to validity, while utmost care has been taken in performing all steps in the review, it cannot be guaranteed to be totally error free and complete. The systematic search was performed only on the six selected databases. Thus, there is a risk that a number of related publications from other databases are left out. However, our choice of databases includes Google Scholar that should have the widest coverage of related publications. Thus, the risk of missing out these publications is perceived to be low.

TABLE VI
SUMMARY OF THE SHOULDER SURF RESISTANT TECHNIQUES USED BY THE METHODS UNDER STUDY

No.	Technique	Description
1.	Increase of password items	The number of pattern points or strokes is increased to be higher than the conventional to increase complexity
2.	Keypad reordering	Items on the keypad is simply rearranged to be different from the conventional $n \times m$ grid
3.	Keypad randomisation	Items on the keypad are arranged in random order at each unlock session
4.	Behavioural property	Each password item is associated with an attribute or state that describes how it should be entered
5.	Offset touch	Users do not touch on the input item when unlocking, but at a different location on the screen
6.	View manipulation	Software or hardware properties are used to cause the attacker to view the keypad differently
7.	OTP with explicit token	A token is used in conjunction with the password to produce OTP to unlock the phone. The token is communicated using either primary or secondary channel
8.	OTP without token	The password is used independently to produce the OTP
9.	Specialised hardware	The use of built-in or external hardware features/devices hide the password or token from the attacker
10.	Image degradation	Applicable only to image-based methods, this technique reduces the quality of images used in such a way that makes them difficult to be recognised by the attackers

V. CONCLUSION

Protecting the smartphones from unauthorised access is important because a lot of personal information is stored in them. The first line of defense in doing so is by activating the screen locking function. Conventional screen locking methods such as PIN-based and pattern-based are found to be prone to shoulder surf attack. As a result, many alternative screen locking methods were proposed to overcome the vulnerability of conventional methods. This paper presents and discusses the results of a systematic literature review performed to understand the current state of the proposed screen locking methods with regard to the techniques used in resisting the shoulder surf attacks. A total of 84 methods were gathered, 50 of which are non-biometric. From the 50 non-biometric methods, a total of ten techniques to resist shoulder surf attacks was found, which are either used on their own or in combination with other techniques. To the best of our knowledge, this is the first work that performs such a comprehensive review on the non-biometric shoulder surf resistant screen locking methods. Future work includes extending the analysis to also include the biometric screen locking methods.

REFERENCES

[1] S. M. Muzammal, M. A. Shah, S.-J. Zhang, and H.-J. Yang, "Conceivable security risks and authentication techniques for smart devices: A comparative evaluation of security practices," *International Journal of Automation and Computing*, vol. 13, no. 4, pp. 350–363, Aug 2016. [Online]. Available: https://doi.org/10.1007/s11633-016-1011-5

[2] F. Stroud. screen lock. Accessed on September 2nd, 2018),. [Online]. Available: https://www.webopedia.com/TERM/S/screen_lock.html

[3] F. Ion. From touch displays to the surface: A brief history of touchscreen technology the beginnings of capacitive, resisitive, and multitouch screens. Accessed on September 2nd, 2018),. [Online]. Available: https://arstechnica.com/gadgets/2013/04/from-touch-displays-to-the-surface-a-brief-history-of-touchscreen-technology/

[4] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571–583, 2007, software Performance. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016412120600197X

[5] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in *2010 International Conference on Cyberworlds*, Oct 2010, pp. 194–199.

[6] H. M. Sun, S. T. Chen, J. H. Yeh, and C. Y. Cheng, "A shoulder surfing resistant graphical authentication system," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 180–193, March 2018.

[7] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," in *2009 First International Workshop on Education Technology and Computer Science*, vol. 3, March 2009, pp. 90–95.

[8] T. Kwon and J. Hong, "Analysis and improvement of a pin-entry method resilient to shoulder-surfing and recording attacks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 278–292, Feb 2015.

[9] A. Aratani and A. Kanai, "Authentication method against shoulder-surfing attacks using secondary channel," in *2015 IEEE International Conference on Consumer Electronics (ICCE)*, Jan 2015, pp. 430–431.

[10] T. Takada and M. Ishizuka, "Chameleon dial: Repeated camera-recording attack resilient pin input scheme," in *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers*, ser. UbiComp/ISWC'15 Adjunct. New York, NY, USA: ACM, 2015, pp. 365–368. [Online]. Available: http://doi.acm.org/10.1145/2800835.2800905

[11] C. Winkler, J. Gugenheimer, A. De Luca, G. Haas, P. Speidel, D. Dobbelstein, and E. Rukzio, "Glass unlock: Enhancing security of smartphone unlocking through leveraging a private near-eye display," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 1407–1410. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702316

[12] A. Papadopoulos, T. Nguyen, E. Durmus, and N. Memon, "Illusionpin: Shoulder-surfing resistant authentication using hybrid images," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2875–2889, Dec 2017.

[13] A. Bianchi and I. Oakley, "Multiplexed input to protect against casual observers," in *Proceedings of HCI Korea*, ser. HCIK '15. South Korea: Hanbit Media, Inc., 2014, pp. 7–11. [Online]. Available: http://dl.acm.org/citation.cfm?id=2729485.2729487

[14] S. S. ul Hasan Naqvi and S. Afzal, "Operation code authentication preventing shoulder surfing attacks," in *2010 3rd International Conference on Computer Science and Information Technology*, vol. 4, July 2010, pp. 32–35.

[15] N. Wakabayashi, M. Kuriyama, and A. Kanai, "Personal authentication method against shoulder-surfing attacks for smartphone," in *2017 IEEE International Conference on Consumer Electronics (ICCE)*, Jan 2017, pp. 153–155.

[16] M. Park, Y. Kita, K. Aburada, and N. Okazaki, "Proposal of a puzzle authentication method with shoulder-surfing attack resistance," in *2014 17th International Conference on Network-Based Information Systems*, Sept 2014, pp. 495–500.

[17] A. A. Cain and J. D. Still, "Rsvp a temporal method for graphical authentication," *Journal of Information Privacy and Security*, vol. 13, no. 4, pp. 226–237, 2017. [Online]. Available: https://doi.org/10.1080/15536548.2017.1397263

[18] R. Schlöglhofer and J. Sametinger, "Secure and usable authentication on mobile devices," in *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*, ser. MoMM '12. New York, NY, USA: ACM, 2012, pp. 257–262. [Online]. Available: http://doi.acm.org/10.1145/2428955.2429004

[19] H. Shin, D. Kim, and J. Hur, "Secure pattern-based authentication against shoulder surfing attack in smart devices," in *2015 Seventh International Conference on Ubiquitous and Future Networks*, July 2015, pp. 13–18.

[20] M. K. Lee, "Security notions and advanced method for human shoulder-surfing resistant pin-entry," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 695–708, April 2014.

[21] H. Tupsamudre, V. Banahatti, S. Lodha, and K. Vyas, "Pass-o: A proposal to improve the security of pattern unlock scheme," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ser. ASIA CCS '17. New York, NY, USA: ACM, 2017, pp. 400–407. [Online]. Available: http://doi.acm.org/10.1145/3052973.3053041

[22] M. Kosugi, T. Suzuki, O. Uchida, and H. Kikuchi, "Swipass: Image-based user authentication for touch screen devices," *Journal of Information Processing*, vol. 24, no. 2, pp. 227–236, 2016.

[23] G. Cho, J. H. Huh, J. Cho, S. Oh, Y. Song, and H. Kim, "Syspal: System-guided pattern locks for android," in *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 338–356.

[24] X. Yu, Z. Wang, Y. Li, L. Li, W. T. Zhu, and L. Song, "Evopass: Evolvable graphical password against shoulder-surfing attacks," *Computers Security*, vol. 70, pp. 179 – 198, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740481730113X

[25] M.-K. Lee, J. B. Kim, and M. K. Franklin, "3dpin: Enhancing security with 3d display," in *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)*, Oct 2014, pp. 129–130.

[26] M. R. Albayati and A. H. Lashkari, "A new graphical password based on decoy image portions (gp-dip)," in *2014 International Conference on Mathematics and Computers in Sciences and in Industry*, Sept 2014, pp. 295–298.

[27] S.-H. Kim, J.-W. Kim, S.-Y. Kim, and H.-G. Cho, "A new shoulder-surfing resistant password for mobile environments," in *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication*, ser. ICUIMC '11. New York, NY, USA: ACM, 2011, pp. 27:1–27:8. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/1968613.1968647

[28] J. Nicholson, P. Dunphy, L. Coventry, P. Briggs, and P. Olivier, "A security assessment of tiles: A new portfolio-based graphical authentication system," in *CHI '12 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '12. New York, NY, USA: ACM, 2012, pp. 1967–1972. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2212776.2223737

[29] Y.-S. Jeong, H.-W. Kim, and J. H. Park, "An effective locking scheme of smart multimedia devices with convenience and enhanced security," *Multimedia Tools and Applications*, vol. 75, no. 23, pp. 15 171–15 183, Dec 2016. [Online]. Available: https://doi.org/10.1007/s11042-014-2208-7

[30] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '13. New York, NY, USA: ACM, 2013, pp. 2389–2398. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2470654.2481330

[31] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, "Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2937–2946. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2556288.2557097

[32] A. Colley, T. Seitz, T. Lappalainen, M. Kranz, , and J. Häkkilä, "Extending the touchscreen pattern lock mechanism with duplicated and temporal codes," *Advances in Human-Computer Interaction*, vol. 2016.

[33] H.-Y. Chiang and S. Chiasson, "Improving user authentication on mobile devices: A touchscreen graphical password," in *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, ser. MobileHCI '13. New York, NY, USA: ACM, 2013, pp. 251–260. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2493190.2493213

[34] T. Takada and Y. Kokubun, "Mtapin: multi-touch key input enhances security of pin authentication while keeping usability," *International Journal of Pervasive Computing and Communications*, vol. 10, no. 3, pp. 276–290, 2014. [Online]. Available: https://doi.org/10.1108/IJPCC-07-2014-0041

[35] L. Kraus, R. Schmidt, M. Walch, F. Schaub, and S. Möller, "On the use of emojis in mobile authentication," in *ICT Systems Security and Privacy Protection*, S. De Capitani di Vimercati and F. Martinelli, Eds. Cham: Springer International Publishing, 2017, pp. 265–280.

[36] H. Sun, K. Wang, X. Li, N. Qin, and Z. Chen, "Passapp: My app is my password!" in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, ser. MobileHCI '15. New York, NY, USA: ACM, 2015, pp. 306–315. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2785830.2785880

[37] W. A. van Eekelen, J. van den Elst, and V.-J. Khan, "Picassopass: A password scheme using a dynamically layered combination of graphical elements," in *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '13. New York, NY, USA: ACM, 2013, pp. 1857–1862. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2468356.2468689

[38] Y. Higashiyama, N. Yanai, S. Okamura, and T. Fujiwara, "Revisiting authentication with shoulder-surfing resistance for smartphones," in *2015 Third International Symposium on Computing and Networking (CANDAR)*, Dec 2015, pp. 89–95.

[39] A. E. S. Tafreshi, S. C. S. Tafreshi, and A. S. Tafreshi, "Tiltpass: Using device tilts as an authentication method," in *Proceedings of the 2017 ACM International Conference on Interactive Surfaces and Spaces*, ser. ISS '17. New York, NY, USA: ACM, 2017, pp. 378–383. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/3132272.3134112

[40] H. Tupsamudre, S. Vaddepalli, V. Banahatti, and S. Lodha, "Poster: Tinpal - an enhanced interface for pattern locks," Feb 2018, last accessed on 4th August 2018. [Online]. Available: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018posters_paper_8.pdf

[41] S. Azad, M. S. A. N. Ranak, and M. A. Rahman, "Vap code: A secure graphical password scheme for smart devices," in *Proceeding of International Competition and Exhibition on Computing Innovation 2016*, ser. iCE-CInno 2016, 2016, pp. 443–450. [Online]. Available: http://icecinno.ump.edu.my/index.php/en/documents/pdf-files/proceeding-2016/201-443-450/file

[42] C. Ling, X. Hei, K. Kong, M. Peays, and M. Guizani, "You cannot sense my pins: A side-channel attack deterrent solution based on haptic feedback on touch-enabled devices," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–7.

[43] J. Gugenheimer, A. De Luca, H. Hess, S. Karg, D. Wolf, and E. Rukzio, "Colorsnakes: Using colored decoys to secure authentication in sensitive contexts," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, ser. MobileHCI '15. New York, NY, USA: ACM, 2015, pp. 274–283. [Online]. Available: http://doi.acm.org/10.1145/2785830.2785834

[44] S. Shen, T. Kang, S. Lin, and W. Chien, "Random graphic user password authentication scheme in mobile devices," in *2017 International Conference on Applied System Innovation (ICASI)*, May 2017, pp. 1251–1254.

[45] I. Leftheriotis, "User authentication in a multi-touch surface: A chord password system," in *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '13. New York, NY, USA: ACM, 2013, pp. 1725–1730. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2468356.2468665

[46] T. Kuribara, B. Shizuki, and J. Tanaka, "Vibrainput: Two-step pin entry system based on vibration and visual information," in *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '14. New York, NY, USA: ACM, 2014, pp. 2473–2478. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2559206.2581187

[47] J. Bermudez, A. Abdulaal, L. Xu, and B. Quach, "Innovative spiral lock design for smartphone security," last accessed on 4th August 2018. [Online]. Available: http://www.cs.utoronto.ca/ xuliwenx/files/Final_Paper_Spiral_Lock.pdf

[48] E. von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "Swipin: Fast and secure pin-entry on smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 1403–1406. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/2702123.2702212

[49] T. Kwon and S. Na, "Switchpin: Securing smartphone pin entry with switchable keypads," in *2014 IEEE International Conference on Consumer Electronics (ICCE)*, Jan 2014, pp. 23–24.

[50] 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 *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction*, ser. TEI '11. New York, NY, USA: ACM, 2011, pp. 197–200. [Online]. Available: http://doi.acm.org.ezproxy.uniten.edu.my/10.1145/1935701.1935740

[51] S. Yi, Z. Qin, N. Carter, and Q. Li, "Wearlock: Unlocking your phone via acoustics using smartwatch," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, June 2017, pp. 469–479.