Comparative Authentication Techniques Study for Smart Devices

Aakanksha Chopra[1], Megha Gupta[2]
[1]Department of Information Technology, JIMS, Rohini, Delhi, India
Email: aakankshachopra.spm@gmail.com
[2] Department of Information Technology, JIMS, Rohini, Delhi, India
Email: meghabis@gmail.com

Abstract – In today's world with the advancement of technology in InfoTech devices, everything is available on a finger touch. People have evolved accordingly by deviating from desktop to smart phones. In the era of smart thinking the technology is also becoming smart. With a blink of eye; things are getting obsolete and new versions of mobiles and their applications are introducing at high pace. In mobile phones countless sensitive data like mobile banking, shopping, health care etc. is stored, used, shared and misused. A very important concern attached with this data is Security. Security of information which is directly related to security of devices like-desktop, tablets, mobile phones, smart watches etc. have become an important factor. Dealing with data is still easy but dealing with security is a massive concern and hence there is requirement of an Efficient Security System. This paper has discussed about various security attacks on mobile's, authorization and authentication methods, old and new attacks. Passwords, an important aspect of security exist since their inception but they are not safe. This paper reviews all authentication methods and it has been found that graphical passwords are the most secured for mobile devices.

Keywords – Authentication, Authorization, Graphical Passwords, Old and New Attacks

I. INTRODUCTION

Today a mobile device is having diverse features, in other words "one device with multiple utilities", hence termed as "Smart Devices." One such smart device is Smart Phones. They contain all kinds of features of information creation, deletion, updating, uploading, and sharing etc. Masses have moved from old desktop to mobiles for their data access. The world has shifted from hefty and huge systems or desktops to compact and smart devices. Information accessing is a very easy task today. People create and store information and make it accessible over a click or a touch. As the world is growing; so is the information. An Ideal Security System considers security, reliability, usability and human factors [1].

Information on devices today is more sensitive. And sensitive information is supervened by attacks. Security breaches are not only restricted to individuals, now rather they have crossed borders and entered into organizations as well. The security risks have become evident and daunting due to speedy escalation in quantity of data constructed and exhausted away on mobiles.

The IDG Research Services Survey [5] reported that "82% of respondents majorly access their corporate data via mobile devices. Whopping 95% respondents agree that larger the size of employees & access to the data, higher is the perplexity and security breach." According to Zaidi et al. [2], "More than 30% mobile phone users do not use any PIN on their mobile phones"; irrespective of the fact that eminently voluble data is saved and percolated from mobiles only. Beside mobile payments and money transfer applications, enterprise data becoming available on mobile devices has become another security concern.

Expansion of mobile devices has incrusted with influx of new applications and their features. The number of available apps in Apple Store reached 1.5 million in June 2015, up 300,000 from June 2014. As the applications are coming out for mobile phones, correspondingly the internal space of mobile phones is also expanding. Due to the essence of apps behaving like swarms (that is, checking in regularly) most apps behave in the same way as a bot (or robot) would be on a computer. The author in [3] claims that, in today's day and age, approximate 2,30,000 open source SourceForge mobile software development projects have been used since 2009. It can be easily deduce that the application is another inception of threat to the mobile's data security.

Distinct mobile operating systems e.g. iOS, Android, Bada, Blackberry, MeeGo, Palm, Symbian, webOS have different threats. There are two attack vectors[3] first, when Mobile phone connects to the internet second, when mobile phone connects to the network.

This paper focuses on the best technique for authentication in mobile or smart phones. Section II discusses about how mobile security attacks are hampering various organizations and describing various mobile security attacks. Section III elaborates on authorization and authentication methods for mobile security. Section IV is explaining how password is an important security aspect for preventing smart phones from intrusions. Section V is giving an insight on graphical password technique of authentication. Section VI is a review of various available authentication methods. Section VII contains conclusion and future work.

II. MOBILE SECURITY ATTACKS

Escalation in smart phones has lead to many problems both at individual and at organizational levels. According to *Zaidi et al*. [2] there are four problems with smart phones- *Authentication, Vulnerability, Data Protection & Privacy, and Attacks.* According to IDG report published in late 2015 [5] "The security risk of Mobile Devices in organizations has increased tremendously." The potential risks in mobiles are increasing due to unsecured apps, malware and wi-fi. About 90% of organizations had made mobile security as their priority. Unpatched operating system also causes threats like – Stagefright, SSL library vulnerability. This report has highly recommended organizations to do authentication and authorization of data. Hence, it can be easily said that- "a compromised mobile device can bulge to oozing of essential information of a company." Apart from organizational menace, Smartphone's or mobiles which are easily stolen or lost, results in direct access and manipulation of sensitive data.

Table1 and Table 2 show list of old and new security attacks. Since the inception of internet access and data availability; security attacks have increased. Intruders try to peep into sensitive information in our systems or mobiles through these attacks only. Table 1 is showing various old attacks e.g. physical attacks, backdoor entries, worms, virus etc with their vulnerabilities and impact on systems.

TABLE 1. VARIOUS OLD ATTACKS, VULNERABILITIES AND IMPACT

Attack Name	Vulnerability	Impact
Physical Attacks	System error / fault	✓ Mobile Security becomes very fragile and performs abnormally.
	Unsatisfactory APIS Management	✓ Malicious code can infect user's data or files.
Radio Wireless attack	Eavesdropping sniffing and spoof computing blocking.	✓ Hacking of data is easy. ✓ Minimise computer security.
	Insecure Wireless network.	Information can be hacked during transmission.
Backdoor	System bugs and disclosure.	✓ Safeguarding smart phone becomes ambiguous. ✓ Viruses can enter through backdoor.
Virus	Target finding, replication file with unknown source	✓ Abnormal behavior of application. ✓ Information or applications may be corrupted
Worms	✓ Transferring information. ✓ Transferring malicious program.	✓ Backdoor entry for hackers is created. ✓ Travels with the system files.
Malware	Downloading file from interested resources	✓ Effects computer activity. ✓ Extracts delicate information
Trojan	✓ Downloading Apps from untrusted resources. ✓ Hidden malicious functionality.	✓ Effects computer activity. ✓ Gather sensitive information.
Spam	✓ Any attachment with malicious code transfer via b. E-mail or MMS. ✓ Attacker can advertise phishing links.	✓ Inbox gets stacked with plenty of junk emails. ✓ Deteriorates Internet speed. ✓ Steals personal information like –your Contact list. ✓ Modifies any search engine results.
Threat	Spoofing, Information disclosure.	✓ Corrupt data. ✓ Computer security becomes fragile. ✓ Provide back doors into protected networked.

Table 2 depicts all new security attacks like- Relay attack, brute force attack; smudge attack, DOS attack, USB connection attack etc. with their vulnerabilities and impact. New attacks are more dangerous in terms of data and password leaking. Data can be accessed through any point once leaked.

TABLE 2. VARIOUS NEW ATTACKS, VULNERABILITIES AND IMPACT

Attack Name	Vulnerability	Impact
Relay Attack	✓ Insecure network environment. ✓ Use of unauthentic proxy service.	Information hacked during communication.
Cold Boot Attack	Unauthorized access to RAM and encryption / decryption key of system	✓ Encryption key may be hacked. ✓ Weak data security
Brute Force Attack	Try again and again to unlock phone using many combination and no limit to prevent from hacking.	✓ Password cracked. ✓ Slowing the CPU speed.
Smudge Attack	By keep touch screen dirty or using oily hands	✓ Easily guess the pattern password. ✓ Data unsecure
Denial of Service Attack	✓ By using other device dismiss the supply of mobile broadband connection. ✓ Link to bogus Wi-Fi connection	✓ Busy the network. ✓ Busy smartphone and block other services.
XSS Attack	HTML 5 based malicious code inserted into an application or software	✓ Smartphone infected by inject malicious code via HTML page or any other untrusted script. ✓ Cause of hacking information or provide backdoor.
SMS based Attack	Attacker can advertise phishing links.	Sensitive information can be fetch.
USB Connection Attack	Root access, enable ADB(open command tool and avail both developer and attacker)	✓ Sensitive information can be fetch easily. ✓ Any malware can be injected easily
ABD Attack	Open command tool and avail both developer and attacker	Sensitive information can be fetch easily
Camera based attacks	✓ Malicious program, unauthentic source and etc. ✓ Use camera of smart phone as spy cam by malicious program	✓ Weak the smart phone security. ✓ Can fetch data or information.
Control Flow attacks	Code injection, data over flow in Memory	✓ Can be exploited to snip the user's SMS or contacts database, to open a remote reverse shell. ✓ Exploiting memory corruption.

III. AUTHORIZATION AND AUTHENTICATION

Authentication is a process which allows a user to confirm his/her identity to an application, the person requesting a resource is the one who he/she claims to be. Password equips security structure for authentication and protection methods against unwanted access to data and resource [7].

Authentication can be procured by three different methods. These methods are listed below-

1. Knowledge-Based Passwords - Also called alphanumeric passwords i.e. combination of alphabets and numbers, and graphical based password

- Token Based Passwords- Text password, PIN no. and Pattern

- Biometric Passwords - Can be contact biometric and contact less biometric, Finger printing, retina scan, etc.,

To avoid this authentication problems, *Graphical passwords* have been designed to make passwords more memorable and easier for people to use and be more secure amongst all. Present usable systems are more prone to attacks as they mostly ignore the importance of human factors in security [7].

IV. PASSWORD: AN IMPORTANT SECURITY ASPECT

Data is gigantic and paramount to handle so is its authentication. For authentication we may use different pattern and passwords. Passwords can be defined as a simple secret provided by the user upon request by the recipient, it is then shared by the verifier and stored on a server in an encrypted form so that a penetration of the file system does not reveal the password details.

Alphanumeric Passwords are common means of authentication because they do not require any special hardware for execution and implementation. Text passwords which are strings of char or alphanumeric are hard to remember and weak passwords are vulnerable to dictionary attack & brute force attack [1].

Passwords are crucial as well as becoming very problematic as they are prone to attacks. These attacks can be online or offline both. William et. Al [6] described about offline attacks that these attacks can be damaging because users often reuse passwords, sometimes with small modifications, across different accounts. Offline attacks are those in which attacker's pirate or steal databases of hashed passwords and then "crack" these passwords by making up to trillions of guesses. Offline attacks also endure to be successful although many efforts have been taken to use slow hashes to limit attackers' ability to crack stolen passwords. Hence, mobile password security technique is very weak. Security of passwords created and used on mobile devices with respect to offline guessing attacks is almost negligible [6].

Alphanumeric password has shown security and usability drawbacks, which are listed below-

A. *Easy to guess*- a user may pick an easy to remember alphanumeric password that may also be easy to guess.

B. *Short passwords*- Previous studies have shown that users tend to choose short alphanumeric passwords that are easy to remember but that password can be easily guessed.

C. *Hard to remember*- On the other hand, if an alphanumeric password is hard to guess, then it is often hard to remember too.

D. *Repetitive passwords*- Since users can remember a limited number of alphanumeric passwords, they often write down their passwords or use same password for multiple accounts [8].

Hence, graphical passwords are considered more over alphanumeric pattern and alphanumeric passwords today.

V. GRAPHICAL PASSWORDS (GP)

Graphical passwords were given in 1996 by Greg Blonder. Graphical Passwords is an advance version of text-password. In text-passwords, the user has to go through two phases - *registration phase* and *authentication phase*. Registration phase consist of username and text- password setting; Authentication phase consist of user verification if user enters correct username and password.

Graphical password also consists of two phases like text-based (*Registration phase and Authentication phase*). In Registration phase; user consists of clicking images or drag the images, or rotating the images as a password and not typing the text in textual passwords [9]. After that the user is supposed to draw same object using stylus on touch sensitive screen. In Authentication Phase user is supposed to give username, password, and graphical password by drawing it in same object way as at time of authentication phase. Hence, we can say that graphical passwords are user friendly, reliable, high secured and provides robust authentication. Graphical passwords cannot be stolen or compromised since the user is also drawing the graphical password.

Graphical passwords are easy to remember as pictures are better than text [8]. Because of memorability advantage, there is significant interest in graphical password.

Fig. 1 shows Classification of Graphical passwords. Graphical based passwords schemes can be broadly classified into four main categories [7]:

- **Recognition Based Systems/ Cognometric Systems**- This techniques involve identifying whether one has seen an image before or not. The user must only be able to recognize previously seen images.
- **Pure Recall-Based Systems**- In this the system users need to reproduce their passwords without being given any reminder, hints or gesture. Although this category is easy and convenient, but it seems that users hardly can remember their passwords similar to other techniques.
- **Cued Recall-Based Systems/ Icon metric Systems**- In cued recall-based system, a user is provided with a hint so that he or she can recall his/her password.
- **Hybrid Systems**- Hybrid systems are the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes.

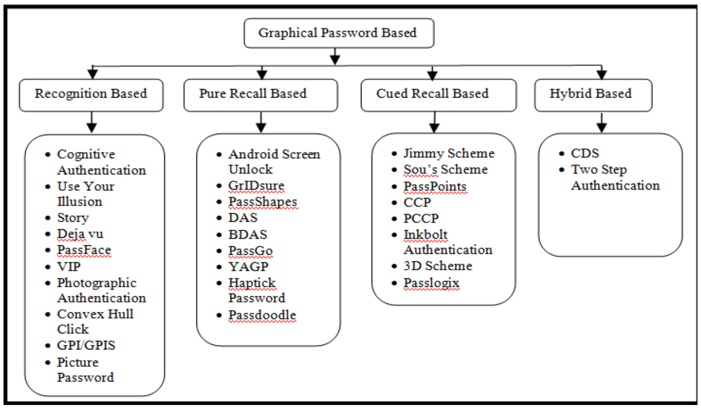

Fig.1 Classification of Graphical Passwords

Wazir et al. [1] proposed a hybrid graphical password based system that is combination of recognition and recall based techniques. This system is less prone to brute force attack, dictionary attacks, guessing, spy-ware, and social engineering. This system is better than two step authentication systems and it prevents hacking and other attacks. Three major drawbacks of this technique are; firstly, this technique is resistant to shoulder surfing attack; secondly, it takes longer to input graphical passwords than textual passwords and thirdly login process is slow which may irritate the user.

Graphical passwords are also sometimes referred as graphical user authentication as they work according to Graphical User Interface (GUI).

VI. COMPARATIVE ANALYSIS STUDY

This paper constructs review of observations of various authentication methods. Based on the literature review, this comparative Analysis has been done as shown in Table 3. Knowledge based Method has been taken as base for comparison. In Table 3, comparison has been presented based on several factors like- ***Authentication Method, Password Generation Time, Memorability, Login Time, Login Success Rate, Old/New Password, Accuracy Rate (Probability of successful login), Limitations/Essential factors/Pre-requisites, Security.***

There are various Authentication Methods used for providing authentication in mobile passwords like Token based, Biometric based (Contact-Less Biometric Technologies and Contact Biometric Technologies), Knowledge based methods [1, 2, 6, 7, 9,14,15,16].

Password Generation Time- It is the time required to create screen lock or pattern or password on mobile device. Since Knowledge based Authentication method has been taken as base for comparison, consider time ‘T’ to Generate text passwords in Knowledge based methods. Finger printing method is taking 3T time to generate password i.e. thrice more than standard token based method.

Memorability- It is the factors that describe how much user remembers the password. It is measured on four factors- *Average, Good, High, and System Dependent*. System Dependent means that the authentication method like- finger printing, facial recognition, voice recognition, iris scan, retinal scan are dependent on the authentication software.

Login Time- Time required to login in mobile. After successful password generation how much time user takes to login into mobile is login time. Here also Knowledge based Authentication Method is used as base for comparison and considered time ‘T’ as base login time.

Login Success Rate- It describes the login success rate as per depending upon authentication method. There are only two factors- *medium and high*. Login Success rate is directly dependent on essential factors/ prerequisites required for each method. If the conditions are fulfilled the success rate will be high else it will be medium or low. It has been found that majorly Login Success rate is either high or medium.

Old/New Password- while generating new passwords or patterns user may or may not use already existing passwords. Depending upon methods this factor has been concluded. For example if it is a Token Based Method or Knowledge based method then the user can use old passwords also. If user is using old passwords the generation time and Login time will automatically reduce. But techniques like Graphical where new images are shown and Biometric like finger printing or iris or retinal scan or hand geometry is used, the user will be generating new passwords, hence increasing the password generation time.

Accuracy Rate- It is the approximate successful chances of login. It is the probability of successfully login into mobile out of 10 chances. *Higher the security higher is the accuracy rate*.

Limitation/ Essential factors/ prerequisites- These are the important factors which must exist to create a password or pattern.

Security (from old and new Attacks) - It is one of the most essential factors of measuring security of mobile passwords. Depending upon various attacks by intruders Security here is measured on scale of Low, Medium and High.

TABLE 3: COMPARATIVE ANALYSIS OF DIFFERENT AUTHENTICATION TECHNIQUES DEPENDING UPON VARIOUS FACTORS

Authentication Method		**Password generation time**	**Memorability**	**Login time**	**Login success rate**	**Old/new password (identical password)**	**Accuracy Rate (Probability of successful login out of 10)**	**Limitation/ essential factors/ prerequisites**	**Security (from old and new Attacks)**
1. Knowledge based Method [9]									
1.1 Text based Passwords [6]	**1.1.1Alphanumeric Text Based Password**	T	Average	T	Medium	Old/ new	6	✓ Text passwords created on mobile devices are 32% weaker as compared to traditional devices. ✓ Also it depends on password policies	Low
1.2 Graphical Based System [1,6,7,8,9]	**1.2.1 Recognition Based System/ Cognometric System**	6T	Medium	4T	High	New	9	✓ Hash Visualization technique-stores and retrieve images from server hence delays authentication process. ✓ Selecting pictures from database is very time consuming ✓ Another algorithm-Requires the user to memorize alphanumeric codes for each pass-object variants.	Low (as password are stored in database which can easily be seen)
	1.2.2 Pure-Recall Based System [8,9]	5T	High	4T	High	New	9	✓ Time required to draw password in same grid is very challenging ✓ Reproduce or draw something as their password without producing any hint at the time of login phase ✓ Syukri algorithm- Should have mouse to draw a signature. ✓ Pass Doodle- User has to draw hand written designs or text on a stylus sensitive touch screen. ✓ DAS Algorithm- same shape must be drawn on 2D grid touching on a stylus sensitive touch screen with strokes that touch on the grid must be the same as authentication phase.	High
	1.2.3 Cued Recall Based System [8,9]	6T	High	5T	High	New	10	✓ Blonder, Pass point ,Cued Click points - Click on several pre-registered locations of a picture in the right sequence and can be hard to remember. ✓ Blonder- The number of clickable points position is relatively small, so the password becomes quite long to secure ✓ Pass point- While login to the system, user has to select the same click points with the same order that the user has been selected the same sequence of click points chosen at the registration phase. The disadvantage of pass point scheme is login time is longer than the usual password.	High
2. Token Based Methods	**2.1. Text Password**	2T	Average	2T	Medium	Old/ new	6	✓ It depends on various password policies	Low
	2.2. PIN No.	2T	Average	T	Medium	Old/ new	7	✓ Only numbers ✓ Easy to crack PIN no.	Low
	2.3. Pattern	2T	High	T	Medium	Old/ New	7	✓ Should not remove hands while generating pattern.	Low

3. Biometric based Method [10, 11,12]									
3.1 Contact Biometric Technology [10,11,12,13]	**3.1.1 Finger Print** [10]	3T	System Dependent	3T	High	New	7 (hands should be kept in proper angle)	✓ It is system dependent. ✓ Fingers should be kept in proper angle for right impression. ✓ Fingerprints are compared with stored templates & increases score with each match. If the score is larger than a predefined threshold, the user is permitted to access the target device.	High
	3.1.2 Hand Geometry [11,13]	4T	Good	4T	Medium	New	7	✓ Cannot be used in identification system. ✓ Cannot be used for growing children as their hand marks may change. ✓ Performance decreases if light falls directly on camera lens. ✓ Registration process is lengthy as it is based on many measurements of hand-shape, size, palm, length, width.	Low (not used these days)
	3.1.3 Dynamic Signature Verification [13]	3T	Good	2T	High	New	8	✓ Signatures are a behavioral biometric, influenced by physical & emotional conditions hence, can get changed over a period of time. ✓ Professional forgers may be able to reproduce signatures that fool the system.	Low
	3.1.4 Keystroke Dynamics [12,13,15]	3T		3T	Medium	New	7	✓ Depends on how people behave and is not unique, its type, their age, gender - needs to categorise this into groups for improving accuracy of existing systems.	Medium
3.2. Contact Less Biometric Technology [11,13]	**3.2.1 Facial Recognition (FR**) [11]	5T	System Dependent	3T	High	New	10	✓ 2D FR technology is having low reliability. ✓ Dependence on the light, low resolution, sometimes form of hair, facial expression, specs, beard makes this method fragile. ✓ 3D FR method is expensive & change of face expression reduces the statistical authentication.	High
	3.2.2 Voice Recognition [11]	5T	System Dependent	3T	High	New	7	✓ Lengthy process as it takes more than 100 different voice features for reliable data. ✓ Considers 2 samples and 2 algorithms for identification process	Medium
	3.2.3 Iris Scan [11,13]	4T	System Dependent	2T	High	New	10	✓ Since iris is a mini organ the process of scanning from a gap is not possible. ✓ It's difficult to read the iris in recognition process of people having blindness or cataract. ✓ Without proper amount of lights it is tough to capture image.	High
	3.2.4 Retinal Scan [13]	4T	System Dependent	2T	High	New	10	✓ It's difficult to scan retina in recognition process of people having blindness or cataract. ✓ Acceptability is very low of this method because requires support in scanning from user. ✓ Reveals some medical conditions of user.	High

VII. CONCLUSION

After studying various authentication methods and their technique it can be easily deduce that the method which is taking more time for password creation are highly secured against all old and new security attacks Another important factor is that the passwords which are newly created are more secured for the mobiles. It is observed that though the schemes like biometric which are having highest accuracy rate (probability of successful login out of 10), are highly secured too but they require many pre-requisites to be followed. The best technique out of all authentication methods is Graphical Based Technique. This technique is creating a unique graphical picture representation which is helping user to be more secured from all old and new password attacks. In future, more deep analyze of the graphical password methods and hybrid techniques will be performed. Also, a new secure technique will be proposed for *Smart Devices*.

VIII. REFERENCES

[1] W. Z. Khan, Mohd. Y. Aalsalem and Y. Xiang, “A Graphical Password Based System for Small Mobile Devices,” *International Journal of Computer Science,* Vol. 8, Issue 5, No 2, pp.145-154, Sept 2011, ISSN (Online): 1694-0814, Website: www.IJCSI.org. Last Accessed on: Sept 13, 2018. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1110/1110.3844.pdf

[2] S. F. A. Zaidi, M. A Shah, M. Kamran, Q. Javaid and S. Zhang, “A Survey on Security for Smartphone Device,” *International Journal of Advanced Computer Science and Applications*, Vol. 7, No.4, 2016, pp 206-219, Website: www.ijacsa.thesai.org. Last Accessed on: Sept 13, 2018. [Online]. Available: http://thesai.org/Downloads/Volume7No4/Paper_26-A_Survey_on_Security_for_Smartphone_Device.pdf

[3] C. Beyer, “Mobile Security: A Literature Review,” *International Journal of Computer Applications (0975 – 8887,)* Vol. 97, No.8, July 2014, pp.9-11, Website: www.ijcaonline.org, Last Accessed: Sept 13, 2018. [Online]. Available: https://pdfs.semanticscholar.org/09d0/3ae6f8edc5f0c123f50770093f22cd281cb1.pdf

[4] P. Redhu and D. Goyal, “Hacking Via Password Cracking,” *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue 6, pp. 830-836, June- 2014, ISSN 2320–088X, Website: www.ijcsmc.com. Last Accessed on: Sept 13, 2018. [Online]. Available: https://ijcsmc.com/docs/papers/June2014/V3I6201499a65.pdf

[5] White paper- "IDG Whitepaper: IT Leaders Buying into Mobile Security," *IDG Lookout (online)*, pp.1-4. Last Accessed on: Sept 13, 2018. [Online]. Available: https://www.lookout.com/info/idg-whitepaper-lp

[6] W. Melicher *et al.,* “Usability and Security of text Passwords on Mobile Devices” *CHI’16, May 07-12, 2016, San Jose, CA, USA*,2016, pp.1-13, ACM 978-1-4503-3362-7/16/05. Last Accessed on: Sept 13, 2018. [Online]. DOI: http://dx.doi.org/10.1145/2858036.2858384

[7] Er.A. Kumar and Er.N. Bilandi, “A Graphical Password Based Authentication Based System For Mobile Devices,” *International Journal of Computer Science and Mobile Computing,* Vol.3 Issue.4, Apr 2014, pp. 744-754, ISSN 2320–088X, Website: www.ijcsmc.org. Last Accessed on: Sept 13, 2018. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1110/1110.3844.pdf

[8] Mohd Anwar and Ashiq Imran, “A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication,” in *Proc. of the 26th Modern {AI} and Cognitive Science Conference, Greensboro, NC, USA*, April 25-26, 2015, pp 13-18, Website: http://ceur-ws.org/Vol-1353/ . Last Accessed on: Sept 13, 2018. [Online]. Available: http://ceur-ws.org/Vol-1353/paper_11.pdf

[9] P. B. Maruthi and Dr. K. S. Rani, “Recall Based Authentication System- An Overview,” *International Journal of Advanced Scientific Technologies, Engineering and Management Sciences,* Vol. 3,Special Issue 1,pp. 121-125, March 2017, ISSN: 2454-356X, Website: www.ijastems.org. Last Accessed on: Sept 13, 2018. [Online]. Available: http://www.ijastems.org/wp-content/uploads/2017/03/v3.si1_.24.Recall-Based-Authentication-System-An-Overview.pdf

[10] Y.H. Jo, S.Y. Jeon, J. H. Im and M.K. Lee, “Security Analysis and Improvement of Fingerprint Authentication for Smartphones,” *Mobile Information Systems,* Hindawi Publishing Corporation, Mobile Information Systems, Vol. 2016, Article ID 8973828, pp. 1-12, 2016. Last Accessed on: Sept 13, 2018. Available: https://www.hindawi.com/journals/misy/2016/8973828/abs/ . DOI: http://dx.doi.org/10.1155/2016/8973828

[11] A. Babich, “Biometric Authentication. Types of biometric identifiers,” Bachelors thesis, Degree Programme in Business Information Technology, Haaga- Helia, University of Applied Sciences, 2012. Last Accessed on: Sept 13, 2018. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/44684/Babich_Aleksandra.pdf

[12] S. P. Banerjee and D. L. Woodard, “Biometric Authentication and Identification using Keystroke Dynamics: A Survey,” *Journal of Pattern Recognition Research 7 (2012)*, pp. 116-139, July 2012, Website: www. jprr.org. Last Accessed on: Sept 13, 2018. [Online]. Available: https://pdfs.semanticscholar.org/f797/1a4341f968263a1d7d6ea219f3266bc7fcf9.pdf

[13] A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions On Circuits And Systems For Video Technology*, Vol. 14, NO. 1, pp. 4-20, Jan 2004. Last Accessed on: Sept 4, 2018. [Online]. DOI: 10.1109/TCSVT.2003.818349

[14] A. Agarwal and A. Patidar, “Smart Authentication for Smart Phones,” *International Journal of Computer Science and Information Technologies*, Vol. 5 (4) , pp. 4839-4843, 2014, ISSN: 0975-9646, Website: www.ijcsit.com. Last Accessed on: Sept 13, 2018. [Online]. Available: https://pdfs.semanticscholar.org/a749/beb7854e1e9ccc6c846fc1626d1f8fa94f26.pdf

[15] G. Kambourakis, D. Damopoulos, D. Papamartzivano and E. Pavlidakis, “Introducing Touchstroke: Keystroke-based Authentication System for Smartphones,” pp.1-5, 2013, John Wiley & Sons Ltd. Last Accessed on: Sept 13, 2018. [Online]. Available: https://pdfs.semanticscholar.org/d41c/bd82006d1e52a0303a8c0d35727f575bc421.pdf

[16] W.H. Lee and R. B. Lee, “Multi-sensor Authentication to Improve Smartphone Security,” in *Proc. of International Conference on Information Systems Security and Privacy,* Feb 2017, pp.1-12 Website: http://arxiv.org/abs/1703.03378v1. [Online]. Available: https://www.researchgate.net/publication/282785492_Multi-sensor_Authentication_to_Improve_Smartphone_Security.

Dr. Megha Gupta is a PhD holder in Computer Engg. from University of Delhi. Her area of expertise include wireless ad-hoc networks, sensor networks, cognitive networks and opportunistic networks. During her studies of Bachelor and M.Tech, she was rank holder in the respective Universities. Holding more than 10 years of experiences that includes both academic and corporate. She has presented papers in international conferences and published research work in various international journals.

.

Ms. Aakanksha Chopra is MCA, BSc(Hons) COputer Science. She is currently pursuing her PhD in Mobile intrusion, detection and prevention systems. She has published many research papers on Network security in various national and international journals holding an experience of 6 years