Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Access Control for Cloud Platforms Using Multi-Tier Graphical Authentication

Yashika Sharma, Rekha Bhatia
PURCITM, Mohali,
Punjab, India

Abstract--The cloud platforms consists of a larger number of servers along with networking and security appliances connected together. The heavier amounts of data are stored on these cloud platforms. The data accessibility becomes the major issue in the cloud platforms. To solve the problem of the data access, the automatic data access control models are designed to restrict the user access to the unauthorized cloud resources and data sources. The literature is available on many access control models for the cloud platforms. The existing access control models are based on the Mandatory access control (MAC), Role based access control (RBAC), Rule based access control (RB-RBAC), Provenance based access control (PBAC), etc. or offered in the various combinations for the effective data access handling on the cloud platforms. In this paper the access control is provided by the graphical authentication. The two tier authentication mechanism here uses two methods; recall based authentication and recognition based authentication. We propose a model combining both of these techniques to provide access control.

Index Terms: Access Control, access models, cloud computing, Graphical authentication.

I. INTRODUCTION

Computer systems and the information that they create, process, transfer, and store have become indispensable to the modern enterprise. In today's on-demand, always connected, data-driven world—and especially in light of the transformation of entire national economies from manufacturing-based paradigms to knowledge-based ones—many organizations rightly count their information systems among their most important assets. Organizations often use these IT systems to store and process vast quantities of sensitive data, which, if disclosed, could be potentially damaging to an organization. At best, an organization may be embarrassed by an unauthorized disclosure; at worst, it may lose its competitive stance in the market if the information were a proprietary trade secret, or may be sued if the information were confidential customer information. Some companies have gone out of business when the damage from an unauthorized access proved too great for them.

Loss of competitive advantage, or even going out of business, is, of course, a very grave situation. However, it is not the worst outcome imaginable from an unauthorized access to an information system. IT systems now integrate with—and even control—critical national infrastructure components, such as the hardware components responsible for the safe operation of power plants, chemical manufacturing facilities, and transportation systems. Controlled access to these types of systems is critical because of the very real potential for loss of life or massive environmental and infrastructure damage that improper or malicious operation could cause. Organizations use access control mechanisms to mitigate the risks of unauthorized access to their data, resources, and systems. Several access control models exist. Their corresponding access control mechanisms—the concrete implementations of those access control models—can take several forms, make use of different technologies and underlying infrastructure components, and involve varying degrees of complexity. In some cases, the more complicated models expand upon and enhance earlier models, while in other cases they represent a rethinking of the fundamental manner in which access control should be done. In many cases, the newer, more complicated models arose not from deficiencies in the security that earlier models provide, but from the need for new models to address changes in organizational structures, technologies, organizational needs, technical capabilities, and/or organizational relationships. The business-to-business (B2B) relationships that enable organizations to successfully execute their missions, for example, sometimes require users or systems from one business to access resources from business partners. Simpler access control models often cannot adequately meet the complex access control requirements that such relationships require, and so more granular, powerful, dynamic models and mechanisms are needed to address these new realities. In short, increasingly complex data access and sharing requirements drive the need for increasingly complex access control models and mechanisms (see Figure 1). The rest of this paper discusses current and future access control models—including access control lists, role-based access control, attribute-based access control, policy-based access control, and risk-adaptive access control—and the infrastructure needed to support them.

Attribute Based Access Control (ABAC) is an access control model wherein the access control decisions are made based on a set of characteristics, or attributes, associated with the requester, the environment, and/or the resource itself. Each attribute is a discrete, distinct field that a policy decision point can compare against a set of values to determine whether

or not to allow or deny access. The attributes do not necessarily need to be related to each other, and in fact, the attributes that go into making a decision can come from disparate, unrelated sources. They can be as diverse as the date an employee was hired, to the projects on which the employee works, to the location where the employee is stationed, or some combination of the above. One should also note that an employee's role in the organization can serve as one attribute that can be (and often is) used in making an access control decision.Cloud computing enables on-demand access to computing and data storage resources that can be configured to meet unique constraints of the clients with minimal management overhead. The recent rise in the availability of cloud services makes them attractive and economically sensible for clients with limited computing or storage resources who are unwilling or unable to procure and maintain their own computing infrastructure. The ever increasing need for computing power and storage accounts for the steady growth in popularity of companies offering cloud services. Clients can easily outsource large amounts of data and computation to remote locations, as well as run applications directly from the cloud.The earlier cloud surveys have provided a much more complete and thorough coverage of the research literature related to this topic. We give a broad overview of publications in the fields of cloud computing security and security of remote storage and computation. In particular, the topics covered in this work include:Client authentication and authorization: We cover the current body of work on methods for disrupting and exploiting the interface between a cloud provider and its clients, usually carried out via a web browser.Security shortcomings of hardware virtualization: We describe the problems that have surfaced along with the massive use of hardware virtualization by cloud providers.We indicate how virtualization can be exploited to obtain unauthorized information from vulnerable users, and also indicate mitigation techniques that can be employed. In addition, we also address vulnerabilities related to the usage and sharing of virtual machine (VM) images. Flooding attacks and denial of service (DoS): Because cloud computing systems are designed to scale according to the demand for resources, an attacker may use that characteristic to maliciously centralize large portions of the cloud's computing power, lowering the quality of service that the cloud provides to other concurrent users. We discuss different types of attacks on cloud availability and their potential consequences. Cloud accountability, or its ability to capture and expose wrongful activity: We discuss capabilities that an accountable system should have and solutions for achieving these capabilities. Challenges and solutions for remote storage protection: We describe several techniques that can be employed by cloud clients to verify integrity of their outsourced data. Protection of outsourced computation: Finally, we give an overview of current approaches for assuring privacy and integrity of outsourced computations.Existing graphical authentication methods take into account the fact that users are more capable of remembering pictures and patterns instead of text. Graphical authentication schemes are expected to be less vulnerable to specific hacker attack techniques that have greatly improved over the years. Graphical passwords were first introduced in the year 1999. The extent to which these passwords are remembered is confirmed by psychological tests and studies over recent years. The conclusion was that these passwords are processed in a different way in our mind. Text based passwords are represented by symbols, which have an associated meaning, and image based passwords have preconceived meaning on what is being observed.The methods of graphical authentication can be broadly classified into two types:Recognition-based method- the user has to recognize the images that were selected earlier during the registeration phase to go through the authentication phase.These methods are also called as "cognometric" and "searchmetric".Recall based method- the user has to enter the specific code as the password , which was earlier given in the registeration phase. These methods are also called as drawmetric systems.There is also another category which is the intermediate known as the cued-recall that is placed between the former mentioned methods as a combination of both of the methods.Our aim is to provide a system that has the feature:To improve the security as graphical passwords are easy to use and memorable. The textual passwords are short and easier to create hence are prone to attacks , hence to avoid them. To provide authorization to different privileged users. To implement the muti-tier scheme onto cloud based application. To provide access control of various data files.

II. LITERATURE REVIEW

Ruj, Sushmita [1] have proposed a decentralized access control with anonymous authentication of data stored in clouds. Authors proposed a new decentralized access control scheme for secure data storage in clouds, that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the ser without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. Bharathy, S. Divya [2] have developed securing data stored in clouds using privacy preserving authenticated access control. Authors proposed a privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme supports secure and efficient dynamic operation on data blocks, including: data update, creation, modification and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. We also provide options for file recovery. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against replay attacks. User revocation and access control policies highly contributes to avoid abuse of cloud services and shared technology issues. HAI TAO [3] proposed Pass-Go, a New Graphical Password Scheme", In this paper, authors are inspired by an old Chinese game, Go and they havedesigned a new graphical password scheme, Pass-Go, in which a user selects intersections on a grid as a way to

input a password The new scheme supports most application environments and input devices, rather thanbeing limited to small mobile devices (PDAs), and can be used to derive cryptographickeys. The study the memorable password space and show the potential power of thisscheme by exploring further improvements and variation mechanisms. Lee, Keunwang, and Haeseok [4] have conducted a research project on access control method by user authority using two-factor authentication. The important information of individuals and businesses is leaked or processed by outside attacks or personal mistakes, thus misused, and thereby considerable damage is occurring. For this reason, the necessity of how to effectively manage personal and corporate information is emerging. This study intends to suggest a method that can protect servers and media information, which requires security. The access control method suggested here uses a way that grants users authority by grade and authenticates users through Two-Factor Authentication method. Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz [5] proposed Quantifying the Security of Graphical Passwords:The Case of Android Unlock Patterns.In this paper, authors has studied the security of Android unlock patterns. By performing a large-scale user study, we measure actual user choices of patterns instead of theoretical considerations on password spaces. From this data they have constructed a model based on Markov chains that enables users to quantify the strength of Android unlock patterns. S.balaji, lakshmi.a, v.revanth, m.saragini, v.venkateswara reddy [6] proposed authentication techniques for engendering session passwords with colors and text.In this paper, authors have proposed two authentication schemes for generating the session passwords which is identified as the primary level of authentication. Once the user has cleared the primary level, he is then allowed to deal with the secondary level of authentication involving a graphical password scheme. This method is most apposite to the PDAs besides other computing devices, as it is resistant to shoulder surfing. Wayne A. Jansen [7] proposed Authenticating Users on Handheld Devices. Handheld devices, being designed for mobile workers, offer unique opportunities for user authentication. Several suitable authentication mechanisms exist as password replacements for PDA devices. Perhaps the most promising authentication mechanisms are visual login, signature verification, and fingerprint verification. For organizational security infrastructures that rely on smart cards, a limited number of possibilities also exist to apply them to handheld devices. Kabir, M.E [8] have worked on a role-involved purpose-based access control model. The structure of a CPAC model is defined and investigated. Access purpose is verified in a dynamic behavior, based on user attributes, context attributes, and authorization policies. Intended purposes are dynamically associated with the requested data object during the access decision. An algorithm is developed to achieve the compliance computation between access purposes and intended purposes and is illustrated with role-based access control (RBAC). Access purpose authorization and authentication in the model are studied with the hierarchical purpose structure. Abhijit Kumar and Dipankar Dasgupta [9] have worked on adaptive approach for active multi-factor authentication. This paper focuses on describing a framework for continuous authentication where authentication modalities are selected adaptively by sensing the users' operating environment (the device and communication media, and historical data). Empirical studies are conducted with varying environmental parameters and the performance of the adaptive MFA is compared with other selection strategies. The empirical results appear promising, which reflects that such a multi-factor decision support technique can be applied to real world identity management and authentication systems. Krikelas, Ilias and Ioannis Xydas [14] have developed graphical user authentication in mobile device using the web RGB color palette. This paper describes a prototype system providing graphical authentication of mobile devices over the Internet, covering both usability and security aspects. Color images are assigned to the mobile users and authentication is achieved by modifying the Red-Green-Blue (RGB) color intensity values of the assigned image.The literature review gave us the idea of developing a multi-tier authentication system for access control on cloud platforms for various devices. The combining of different ideas provided in these papers gave the idea to device such graphical authentication method.

III. IMPLEMENTATION

As the trend of mobile devices is on the rise, every kind of internet application is being easily accessible locally using mobile apps. The proposed technique will be using multi-tier double-trap image based authentication for the login protection in cloud platforms on mobile devices. The first-level authentication scheme consists of various small images of different objects and colors in 2x3 or 3x3 or other similar grid formation. The grid points will be used in the random positioning based grid formation to add more security to the first level of authentication. The first stage will be also capable of mitigating the autobot/botnet/spam threats by differentiating between the user and the bots using its unique graphical password input method. The second stage authentication will be used to access the more private data and sensitive operation according to access control model design. The second level authentication will be based on android lock screen. The users will have to draw a pattern acting as the password for registration. The user will have to draw the pattern with the same keys for login in the second level of the system. To add more security and to lower the probability of breaking into, some of the fake object images as well as the fake secure images can be also added to the front-end interface, where the user will have to first recognize the correct objects selected during signup and then provide their secure codes correctly in order to gain the access to the sensitive data on the cloud application. The proposed will improve the efficiency of data access control models on the cloud platforms by removing the hindrance of the repeated text password inputs. First step towards the research is the literature study of the existing algorithms for graphical passwords, especially password patterns. Literature study will lead towards the development of the algorithm for the touch screen devices. This is also very important to get the architecture of the existing graphical authentication techniques. This would be implemented in HTML, JavaScript and PHP.. A thorough performance and feature testing model would be formed and utilized to analyze the performance of the security model, to detect the flaws and to recover them.

IV. RESULTS

The system has been tested with the 25 random persons of 16 years to 42 years of age. Most of the people become available for the test lies between the 23 and 33. The age variation has been counted as the factor towards testing the ease of access to the proposed graphical password scheme. The graphical password scheme has been tested for average login time, Login success rate, probability of failed login attempts, choice of features, etc.

Table 1: List of 25 persons undergone the login system test

Sr. No.	Name	Age
1	Navjot Kumar	27
2	Aseem Arora	30
3	Rohit Thapar	28
4	Roopali Punj	24
5	Meenakshi	23
6	Navdeep Kaur	21
7	Rajdeep Singh	18
8	Simranjot Singh Sandhu	16
9	Sachin Arora	18
10	Rahul Singhal	22
11	Paramvir Singh	25
12	Shweta Jain	33
13	Amanpreet Kaur	38
14	Swati Sharma	23
15	Bikramjit Singh	26
16	Rahul Devgan	42
17	Namrata Singh	25
18	Raunil Singh	21
19	Pawan Sharma	27
20	Pawandeep Kaur	31
21	Lovepreet Kaur	19
22	Jatinderjit Singh	17
23	Harjinder Mann	25
24	Joginder Singh	35
25	Aman Arora	32

Table 2: Average login time without password of people from different age groups on single level

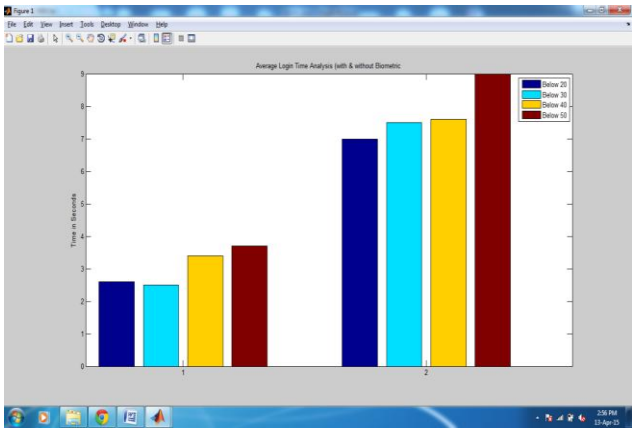
Sr. No.	Age Group	Total Persons in the Age Group	Average Login Time (in seconds)
1	<20	5	2-3
2	<30	13	2-3
3	<40	6	3-4
4	<42	1	3-4

Table 3: Average login time with password of people from different age groups on both levels

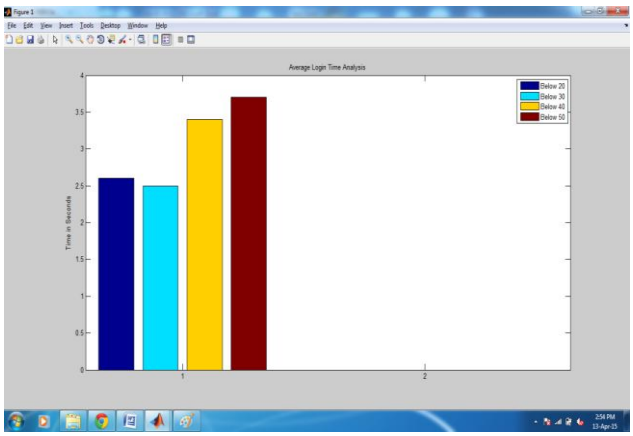
Sr. No.	Age Group	Total Persons in the Age Group	Average Login Time (in seconds)
1	<20	5	6-8
2	<30	13	7-8
3	<40	6	7-8
4	<42	1	8-10

For the login option without password, the results have been observed for the all 25 people. The quickest login times has been achieved by the youngsters under age of 20 years. But there is no significant difference found between the people in their 30s and 40s, where the people below 30 have taken significantly lower time than the people in 30s and 40s. The average login time describes the quickness of the person to understand and respond to the login screen. For the login option with password, again the quickest login times has been achieved by the youngsters under age of 20 years. But

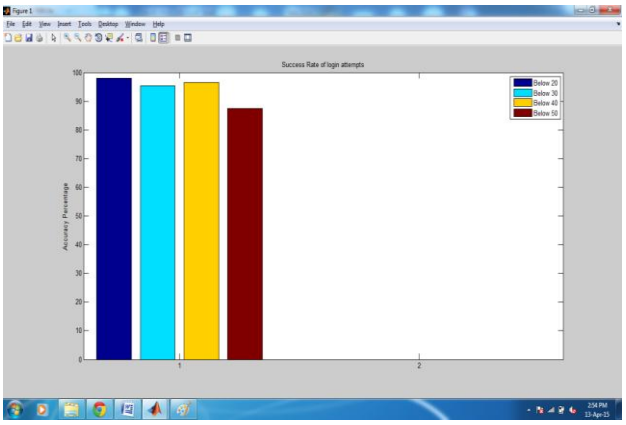
there is no visible difference found between the people in their 20s and 30s, where the person above 40 has taken significantly higher time. The average login time describes the quickness of the person to understand and respond to the login screen.



Bar Graph 1: The average login time analysis after several attempts on single and both levels



Bar Graph 2: The average login time



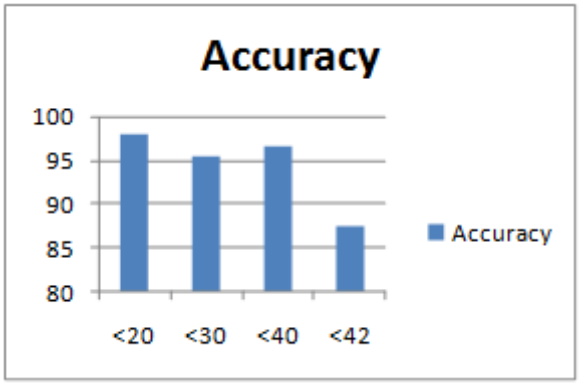
Bar Graph 3: The login accuracy by the testing users of various age groups

Table 4: The successful attempts and success rate by the testing user set for single level (first-level)

s.o	Age Group	Total Persons in the Age Group	Total Attempts	Successful Attempts	Success Rate
1	<20	5	102	100	98.03%
2	<30	13	280	267	95.35%
3	<40	6	115	111	96.52%
4	<42	1	16	14	87.50%

Table 5: The successful attempts and success rate by the testing user set for both levels (first & second levels)

Sr. No.	Age Group	Total Persons in the Age Group	Total Attempts	Successful Attempts	
1	<20	5	50	49	98%
2	<30	13	82	79	96.34%
3	<40	6	102	95	93.13%
4	<42	1	16	14	87.5%



Bar Graph 4: The login accuracy by the testing users of various age groups for both levels

The testing users have been measured in the terms of accuracy, which represents the probability of remembrance of the graphical password patterns. The accuracy has been measured higher in terms of number of successful attempts and success rate in percentage.

V. CONCLUSION

Comparison with other methods:The proposed scheme has been evaluated for various applications under various situations. The comparison of the proposed techniques has been made with the previous techniques in order to understand the functional or security differences between the proposed model and the existing models. The proposed model has been evaluated for its method of working, ease of use, merits and demerits. The merits and demerits of the proposed model have been evaluated as the best model among the others. The access vulnerabilities have been overcome by adding the password option, which can be copied or stolen. The proposed scheme can be rated as the most secure among the evaluated ones under our performance evaluation.

Schemes	Method	Ease of use	Advantages	Disadvantages
Image- based scheme	Single or multiple images are used	Selection of images	Easily remember the password	Very long process selection of number images.
Grid- based scheme	Grid platform is used to accommodate pixels	Simple take and draw scheme	No extra displays are needed grid is sufficient.	sequence can be changed or grids may be different
Triangle scheme	Set of images on convex surface	Complex as convex triangle	Crowded Display	convex surface assigning process takes longer time
Hybrid textual authentication	Colors with sequence number is combination	Complex as confusion with colors	Given user only have to remember the rating.	Difficult to remember colors with sequence.
Signature based scheme	User signature on grid platform	Own signature	Denied the access for mistake	Remembering the grid if not simple
Username and image password scheme [BASE PAPER]	Username with selection of images as password	Username password remembrances	More strong authentication process	Access can be given if anyone knows sequence with username

Proposed scheme	Password based two-level graphical scheme	Image and pass-go pattern remembrance is easier.	Using Password and pass-go pattern have made it more secure than the existing graphical schemes	Not known

Comparisons of methods used for graphical authentication.

VI. FUTURE WORK

The drawbacks or limitations concerned with the different geometrical shapes can be mitigated in the future researches, which can be considered as the critical enhancement or improvement in the proposed system. A new scheme can be developed following the design and pattern schemes of the proposed scheme. The scheme can be made compatible with various devices, ranging from handheld devices to laptops and personal computer.

REFERENCES

[1] Ruj, Sushmita, Milos Stojmenovic, and Amiya Nayak. "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds." Parallel and Distributed Systems, IEEE Transactions on 25, no. 2 (2014): 384-394.

[2] Bharathy, S. Divya, and T. Ramesh. "Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control." (2014).

[3] HAI TAO, "Pass-Go, a New Graphical Password Scheme", Thesis, University of Ottawa, June, 2006.

[4] Lee, Keunwang, and Haeseok Oh. "Research on access control method by user authority using two-factor authentication." In Proceedings of the 1st International Conference on Convergence and It's Applicatio (ICCA'013), vol. 24, pp. 172-175. 2013.

[5] Sebastian Uellenbeck, Markus Demuth, Christopher Wolf, and Thorsten Holz, "Quantifying the Security of Graphical Passwords:The Case of Android Unlock Patterns", 2012.

[6] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini,V.venkateswarareddy"authentication techniques for engendering session passwords with colors and text", acsa, 2012.

[7] Wayne A. Jansen, "Authenticating Users on Handheld Devices", CNIST, 2002

[8] Kabir, M.E., Wang, H., and Bertino, E. (2012), "A Role-involved Purpose-based Access Control Model", Information Systems Frontiers, 14(3), 809-822

[9] Nguyen, Dang, Jaehong Park, and Ravi Sandhu. "A provenance-based access control model for dynamic separation of duties." In Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, pp. 247-256. IEEE, 2013.

[10] Wazan, Ahmad Samer, Gregory Blanc, Hervé Debar, and Joaquin Garcia-Alfaro. "Attribute-based Mining Process for the Organization-Based Access Control Model." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 421-430. IEEE, 2013.

[11] Malik, Jyoti, Dhiraj Girdhar, Ratna Dahiya, and G. Sainarayanan. "Multifactor Authentication Using a QR Code and a One-Time Password." Journal of Information Processing Systems 10, no. 3 (2014).

[12] Nag, Abhijit Kumar, Dipankar Dasgupta, and Kalyanmoy Deb. "An Adaptive Approach for Active Multi-Factor Authentication." In 9th Annual Symposium on Information Assurance (ASIA'14), p. 39. 2014.

[13] Krikelas, Ilias, Ioannis Xydas, and Pierre-François Bonnefoi. "Graphical User Authentication in Mobile Device using the web RGB color palette." In BCI (Local), p. 65. 2013.

[14] Nguyen, Dang, Jaehong Park, and Ravi Sandhu. "Adopting provenance-based access control in OpenStack cloud IaaS." In Network and System Security, pp. 15-27. Springer International Publishing, 2014.

[15] Alexander De Luca, Aliant Hang, Frederic Brudy, Christian Lindner, Heinrich Hussmann "Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns", CHI, 2012.

[16] Gajbhiye s.k. and Ulhe p."authentication schemes for session passwords using colour and gray-scale images", JSIP, 2012.

[17] Susan Wiedenbeck, Jean-Camille Birget, Alex Bordskiy "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice", ACM, 2004.

[18] Dej,a Vu: A User Study Using Images for Authentication. Rachna Dhamija Adrian Perrig, SIMS / CS, University of California Berkeley.

[19] S. Wiedenbeck, J. Waters, J-C. Birget, A. Brodskiy, N. Memon,"PassPoints: Design and longitudinal evaluationof a graphical password system "www.elsevier.com/locate/ijhcs,2005.

[20] Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang," A Graphical Password Based System for Small Mobile Devices " International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.

