INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 06 ISSUE: 05 | MAY - 2022 IMPACT FACTOR: 7.185 ISSN: 2582-3930

# EFFICIENT GRAPHICAL RANDOMIZED AUTHENTICATION (g-RAT) TECHNIQUE FOR SECURE FILE ACCESS IN CONSUMER STORAGE DEVICES

**Rakhi R [1,*] , Judith J.E [2]**
**[1] ME Student, Department of CSE, Noorul Islam Centre for Higher Education, Kumaracoil**
**[2] Associate professor, Department of CSE, Noorul Islam Centre for Higher Education, Kumaracoil**

***Abstract*—** Security is the main aspect for any application. The main aim is to protect the system from the illegitimate users. The proposed system is considered for study and two way authentication techniques are applied on it. Two way authentication techniques are used to protect the data by using both the text and graphical passwords. Graphical password scheme is used named as g-RAT. On both the text as well as graphical password, Improved Advanced Encryption Standard (IAES) algorithm is applied to provide better security. It means system provides two step authentications with the encryption technique. In IAES, one random generated key called as SALT is added with AES key. By adding the Salt key with AES the number of combinations of attack will increase. Even if the database is compromised then also attacker cannot gain the actual text password and g-RAT of the graphical password. g-RAT is used which generates a randomized set of images every time a user tries to authenticate him/herself by maintaining the security and usability at the same time. The gRAT technique is also tested by user-centric evaluation in terms of security, usability, usefulness, and utility, and the experimental results show that the proposed technique is more secure and useful in the real-life authentication applications.

***Keywords—:*** *Graphical password, authentication, security. Improved Advance Encryption Standard*

## I. INTRODUCTION

Several password authentication techniques have been designed so far, which are either difficult to memorize or weak for protecting the authenticity. In fact, with the technological advancement, a secure and memorable password is essential for every user. Authentication is usually the first step encountered by users for a security-focused system; during this process the system challenges the users to provide their passwords to get authenticated. The process begins with the identification, i.e., the user makes a claim of the identity and is followed by the authorization where the user provides credentials to prove the claimed identity. Authentication is vital as it determines whether a user could be granted access to a particular system or not .

Typically, alphanumeric are used for the authentication, which use a key combination as a password. However, as time goes by, users face security and usability problems. These kinds of passwords are hard to remember when a user tends to choose a difficult key combination for better security. On the other hand, these passwords can be easily memorized if a straightforward key combination is chosen. But in that case, the password can be easily cracked by the hackers. In 2005, a security team of computer world executed a password cracker network, where they succeeded to identify 80% passwords within 30 seconds.

For the last two decades, graphical password techniques have been developed as probable alternatives to text-based passwords, inspired by the fiction that a human can easily memorize photos than text. Moreover, a graphical password provides better resistance to dictionary attacks. The notion of graphical passwords was initially explored by Blonder in 1996. The idea behind introducing the graphical password was that humans have the ability to easily memorize the pictures and places that they have visited. Furthermore, graphical passwords are more user-friendly and have the ability to provide users with security and usability together. Beside all the advantages of graphical passwords, there are also some problems arise with the time, for example, shoulder surfing attack is a familiar issue with graphical passwords. It means that a bystander can steal the passwords of users by direct observations over someone's shoulder at the time of password typing. In the literature, numerous techniques have been proposed to minimize the problems and make the graphical password as the best substitute for the text based password, but the idea is still immature and needs a considerable attention from the research community.

In this project, two way authentication techniques are used to protect the data by using both the text and graphical passwords. A secure graphical authentication system named g-RAT that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of randomized set of images every time a user. The g-RAT provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of

their passwords rather than clicking on the password object directly.

This project elaborates on the existing graphical password techniques and reviews the potencies and pitfalls of these schemes. In addition, a novel graphical password authentication technique with Improved Advanced Encryption Standard (IAES) is proposed, which is more reliable and secure as compared to the available techniques. This project aims to design a two way authentication system using text and graphical in distributed systems having following objectives:

- To develop an application which provide security against shoulder surfing attacks during authentication.
- To achieve trade-off between usability and security for authentication systems.
- Evaluate the proposed framework and compare with the most promising techniques.

## II LITERATURE SURVEY

With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank account anytime and anywhere. While logging into these services in public, they may expose their passwords to unknown parties unconsciously. Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as ”the weakest link” in the authentication chain [1].

Thomas Hanne, and Roman Schmidt introduces a novel framework for user authentication based on freehand sketches [2]. In order to resist unauthorized access, consumer storage devices are typically protected using a low entropy password. In order to protect the consumer’s confidential information that has been stored, Amin, R proposes a mutual authentication and key negotiation protocol that can be used to protect the confidential information in the device [3].

Author D. Giri, R. S. Sherratt, and T. Maitra intends to analyse the security of the proposed protocol through a formal analysis which proves that the information is stored confidentially and is protected offering strong resilience to relevant security attacks [6]. PassBYOP is a new graphical password scheme for public terminals that replaces the static digital images typically used in graphical password systems with personalized physical tokens, herein in the form of digital pictures displayed on a physical user-owned device such as a mobile phone [5].

Visual attention research shows that different people are attracted to the same predictable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain an issue. suggest that user choice in all types of graphical passwords is inadvisable due to predictability [7].

Author Vinod Alone explains a Scalable ShoulderSurfing Resistant Textual-Graphical Password Authentica-tion Scheme (S3PAS). S3PAS seamlessly integrates both graphical and textual password schemes and provides nearly perfect resistant to shoulder-surfing, hidden-came ra and spyware attacks. It can replace or coexist with con-ventional textual password systems without changing ex-isting user password profiles [8].

An examination of a previous attempt at solving the PIN entry problem, which was based on an elegant adaptive black-and-white coloring of the 10-digit keypad in the standard layout [9]. CAPTCHA is used in a graphical password scheme to resist spyware. A CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but are beyond the capabilities of current computer programs [10].

Traditional alphanumerical passwords have significant security issues, To provide an easy and more secure authentication technique, a graphical password has been introduced here for consumer electronic devices, which uses an image or a set of images for authentication. Graphical random authentication technique (gRAT), which generates a randomized set of images every time a user tries to authenticate him/herself by maintaining the security and usability at the same time [11].

Furkan Tari compares the real and perceived vulnerability to shoulder-surfing of two configurations of a graphical password [12]. While study participants believed that Passfaces™ with mouse data entry would be most vulnerable to shoulder-surfing attacks, the empirical results found that strong passwords were actually more vulnerable.

A highly secure authentication technique would be overkill for such a terminal because secure authentication in itself does not guarantee the security of the data accessed. Photographic authentication aims to be “secure enough” for casual data by providing the necessary level of security without compromising ease of use. Ideally, the complete system would not even allow a user to access high-security data through an untrusted terminal [13].

Authentication is the process to establish the identity of a communication partner. It is an essential security component

of today's many Internet applications. Among graphical password schemes click-based graphical passwords has gained popularity. In click-based graphical password schemes, users click a sequence of points on a pictorial background to create and use passwords. Systems are vulnerable to predictability. Different attack strategies are quite successful to guess click-based graphical passwords [15].

## III SYSTEM OVERVIEW

By considering all the limitations and problems of the graphical password techniques, we propose a Pure-Recall based system for the authentication. The key features of Pure Recall-based techniques are combined in the proposed gRAT system. The gRAT authentication method has three categories of pictures, i.e., animals, birds, and random, that users can use for password creation and saving. The proposed system is more secure, reliable, and user friendly while maintaining the usability and security.

The proposed system, gRAT, is based on the swipe-based authentication for the screen lock of consumer devices. However, gRAT uses a randomized algorithm that generates random images during the authentication process. The generation of random images helps gRAT fighting against the shoulder surfing attack better than the existing techniques. The proposed system model is given in Fig. 1.

The architecture used in this work consists of presentation, logical and data tier. Fig. 2 shows the architecture diagram of the system

### A. Registration phase

Every system user is required to register to the system. The registration consists of a few easy steps. First, users choose the category of shapes in which they feel comfortable and then create passwords. Once the password is created, it is saved, and the same images are selected in a sequence for granting the authentication, where these shapes/images are randomized by the application during the authentication process.

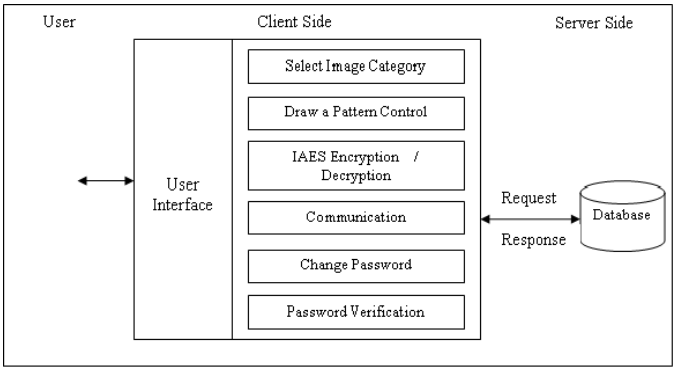


Fig 1 System Architecture

### B. Login phase

In the login phase, a few tasks can be performed, i.e., users can modify/change their passwords as well as change the category of shapes that they have chosen during the login phase. In the login process, authentication is granted on entering a correct password. In case a wrong password is entered, then users have several choices to enter their passwords.

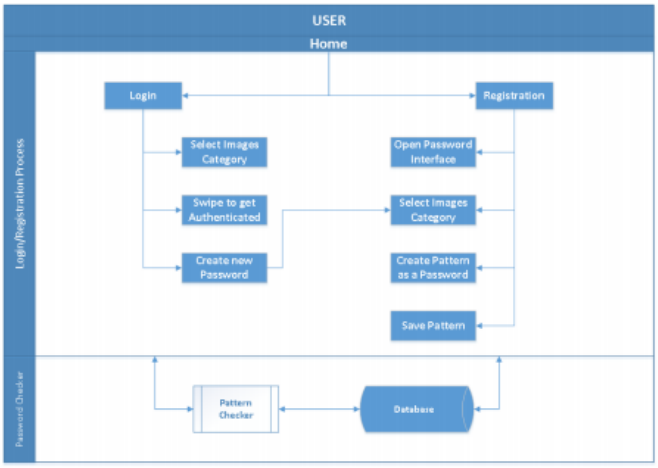


Fig 2 gRAT Architecture

### C. Working of gRAT

The gRAT system is a graphical password technique that uses images which are presented on the screen in a 3x3 grid. However, the highlighted part of the gRAT is that users always get a randomized set of figures. In other words, in the gRAT system the place of pictures changes every time a user wants to be authenticated. The randomized algorithm makes the gRAT resistant against the shoulder-surfing attack. The proposed system has three steps of registration and authentication. The first two steps are the registration and the last one is the authentication process, which are briefly explained below

**Step 1:** In the first step, a user selects a category of images that is provided by the gRAT application, as shown in Fig. 3.
**Step 2:** In the second step, the user chooses a password from a 3x3 grid picture, which is provided on the screen, and then draws a pattern by swiping on images. The password can be minimum of two and maximum of nine images. The gRAT displays the notification of "Draw a pattern to save" when the user selects a category (see Fig. 4).
**Step 3:** This step is about the authentication, where users draw the same pattern that has already been selected during step 2 to validate their profile. During the authentication process, a randomized set of images is presented to the users, but they need to draw the same pattern using the same set of images. The randomized set of images helps gRAT to fight against the shoulder-surfing attack. If users draw a correct pattern, then the application displays a message "correct pattern drawn" (Fig. 5), and thus they are authenticated.

In the case of a wrong pattern drawn, the user has to draw the pattern again with a randomized set of images. When the user draws a wrong pattern, the application displays a warning of the wrong pattern drawn, as shown in Fig. 6

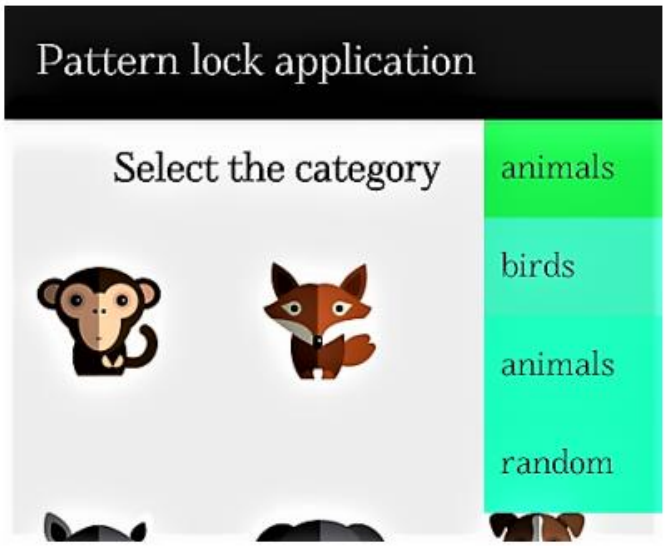


Fig 3 Categories of gRAT


Fig 4 Draw-a-Pattern to Save


Fig 5 gRAT Correct Pattern Drawn


Fig 6 Wrong Pattern Drawn in gRAT

### D. Improved Advanced Encryption Standard

A cryptographic system should be designed in such a way that no outsiders can attack the system. But a major attack that has been reported to many complex crypto systems is Brute force attack which is a kind of key guessing attack which tries to find the original key by trying all possible combinations of letters, numbers and symbols till the correct combination is obtained. Larger the key size, more the time and combinations needed to crack the system. It has been reported that the Data Encryption Standard (DES) faced this attack some years ago, and was the reason for replacing DES with IAES as it supports larger key sizes

Since IAES algorithm uses a key length of 128 bits, the possible number of combinations for the key searching will be 2x128 which is equal to 3.4x1038. Here we can see the exponential increase in possible combinations compared to the 56 bit key used in DES. Even with a super computer, it will take 1 billion years to crack the 128 bit AES key using brute force attack .So the security of AES is more than DES. This work is aimed to improve the security level of existing AES (128 bit) by incorporating a secret password based processing along with the usual way of AES encryption of 128 bit Data and Key. American Standard Code for Information Interchange (ASCII) is the character encoding technique where each character is mapped into a numerical value as described in the standard ASCII table. As the user password contains characters as well as numbers the ASCII method of encoding can be effectively used in this work to get their equivalent numerical values.

For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four

different byte-oriented transformations: 1) byte substitution using a substitution table (S-box), 2) shifting rows of the State array by different offsets, 3) mixing the data within each column of the State array, and 4) adding a Round Key to the State


Fig. 7. Improved Advanced Encryption

**Encryption (Cipher Generation):** At the start of the Cipher, the input is copied to the State array using the conventions. After an initial Round Key addition, the State array is transformed by implementing a round function 10, 12, or 14 times (depending on the key length), with the final round differing slightly from the first Nr -1 rounds. The final State is then copied to the output. The round function is parameterized using a key schedule that consists of a one-dimensional array of four-byte words derived using the Key Expansion routine. The individual transformations- SubBytes (), ShiftRows (), MixColumns (), and AddRoundKey () – process the State and are described in the following subsections. The array w [] contains the key schedule. All Nr rounds are identical with the exception of the final round, which does not include the MixColumns () transformation

**1) SubBytes () Transformation:** The SubBytes () transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box). This S-box, which is invertible, is constructed by composing two transformations.

**2) ShiftRows () Transformation:** In the ShiftRows () transformation, the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets). The first row, r = 0, is not shifted. This has the effect of moving bytes to "lower" positions in the row (i.e., lower values of c in a given row), while the "lowest" bytes wrap around into the "top" of the row (i.e., higher values of c in a given row).

**3) MixColumns () Transformation:** The MixColumns () transformation operates on the State column-bycolumn, treating each column as a four-term polynomial. The columns are considered as polynomials over GF (28 ) and multiplied modulo x4 + 1 with a fixed polynomial a(x), given by, a(x) = {03} x3 + {01} x2 + {01} x+ {02}. 4) AddRoundKey () Transformation: In the AddRoundKey () transformation, a Round Key is added to the State by a simple bitwise XOR operation. Each Round Key consists of Nb words from the key schedule. Those Nb words are each added into the columns of the State.

**Key Expansion:** Each round key is a 4-word (128-bit) array generated as a product of the previous round key, a constant that changes each round, and a series of S-Box lookups for each 32-bit word of the key. The Key schedule Expansion generates a total of Nb (Nr + 1) words

**Decryption (Inverse Cipher Generation)**

The Cipher transformations can be inverted and then implemented in reverse order to produce a straightforward Inverse Cipher for the AES algorithm. The individual transformations used in the Inverse Cipher - InvShiftRows (), InvSubBytes (), InvMixColumns (), and AddRoundKey () – process the State and are described in the following subsections. The Inverse Cipher, the array w [] contains the key schedule

**1) InvShiftRows ()** Transformation: InvShiftRows () is the inverse of the ShiftRows () transformation. The bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets). The first row, r = 0, is not shifted. The bottom three rows are cyclically shifted by Nb - shift(r, Nb) bytes, where the shift value shift (r, Nb) depends on the row number.

**2) InvSubBytes ()** Transformation: InvSubBytes () is the inverse of the byte substitution transformation, in which the inverse Sbox is applied to each byte of the State. This is obtained by applying the inverse of the affine transformation (2.2.5.1) followed by taking the multiplicative inverse in GF (28 ).

**3) InvMixColumns ()** Transformation: InvMixColumns () is the inverse of the MixColumns () transformation. InvMixColumns () operates on the State column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF (28 ) and multiplied modulo x^4 + 1 with a fixed polynomial a-1(x), given by a-1 (x) = {0b}x3 + {0d}x3 + {09}x + {0e}.

**4) Inverse of the AddRoundKey () Transformation:** AddRoundKey (), which is its own inverse, since it only involves an application of the XOR operation

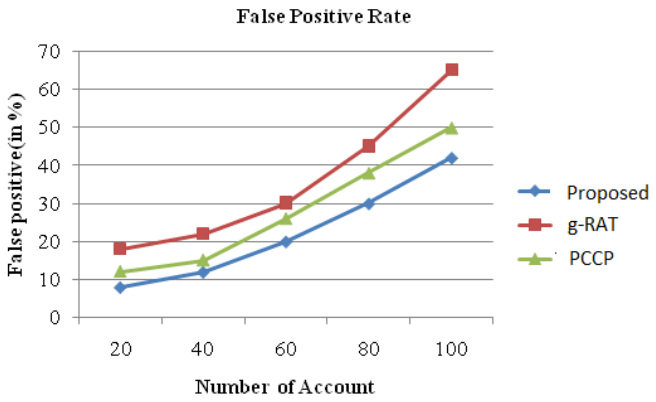


Fig. 8 Comparison Chart of false positive rate

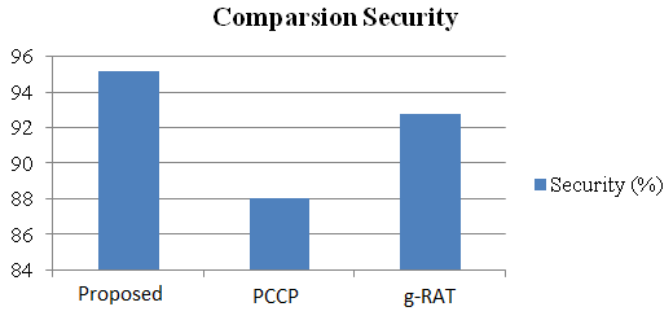


Fig. 9 Comparison Chart of Security

## 1V RESULT

It is possible to use fixed subset of the alphabet to generate sketch based password image for a user if the server receives her user ID before sending image. In this case, the authentication server allows a user to create her password from the full alphabet. Once the password is created, the server find a suitable subset of a reasonable size, which contains all the symbols in the password. The server stores the subset or its index for the account, and retrieves it later when the account attempts to log in to generate a sketch image.

**1) Security:**

The Cracking result that the passwords the participants selected for Text and proposed were reasonably strong, which match our expectation of the password complexity requirement.

**2) False positive rate (FPR)**

Finally, each of the 100 user accounts (selected for the experiment with skilled forgeries) is attacked with the corresponding skilled forgeries. That is, we verify whether or not a login with the skilled forgeries is successful on these accounts. For this second experiment only the FPR is reported.

## V CONCLUTION AND FUTURE WORK

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect users' digital property, authentication is required every time they try to access their personal account and data. Even a complicated password can be cracked easily through shoulder surfing.
To overcome this problem, proposed a shoulder surfing resistant authentication system based on graphical passwords, named gRAT by adding the features with Improved AES. The gRAT system fights against the most common attack on graphical passwords, i.e., shoulder-surfing attack, because it uses a randomized image algorithm. In the randomized image system, an observer cannot judge user's password as it generates a set of randomized pattern every time a user wants to authenticate him/herself. Finally, we examined the gRAT system through user-centric evaluation and observed that the proposed model was found more secure and useful. In future, the g-RAT application can be extended to the architecture layer of consumer devices (smartphones), which may replace the swipe application and introduce a new swipe based graphical application for smartphone users.

## V1 REFERENCES

[1] D. Lin, N. Hilbert, C. Storer, W. Jiang, and J. Fan, "Uface: Your universal password that no one can see," Computers & Security, vol. 77, pp. 627– 641, 2018.
[2] R. Amin, R. S. Sherratt, D. Giri, S. Islam, and M. K. Khan, "A software agent enabled biometric security algorithm for secure file access in consumer storage devices," IEEE Trans. Consum. Electron., vol. 63, no. 1, pp. 53–61, 2017.
[3] D. Giri, R. S. Sherratt, T. Maitra, and R. Amin, "Efficient biometric and password based mutual authentication for consumer usb mass storage devices," IEEE Trans. Consum. Electron., vol. 61, no. 4, pp. 491–499, 2015.
[4] F. Tari, A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in Proc. 2nd ACM symposium on Usable privacy and security, 2006, pp. 56–66.
[5] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, p. 2005, 2005.
[6] G. Blonder and P. GRAPHICAL, "United states patent 5559961," Graphical Passwords, 1996.

[7] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes." in USENIX Security Symposium, vol. 13, 2004, pp. 11–11.
[8] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication," in USENIX Security Symposium, vol. 9, 2000, pp. 4–4.
[9] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, "Towards usable solutions to graphical password hotspot problem," in IEEE 33rd Int. Computer Software and Applications Conf. (COMPSAC'09), vol. 2, 2009, pp. 318–323.
[10] D. Weinshall, "Cognitive authentication schemes safe against spyware," in IEEE Symp. Security and Privacy, 2006, pp. 6–pp.
[11] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems," Int. jour. human-computer studies, vol. 63, no. 1, pp. 128–152, 2005.
[12] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig, "Use your illusion: secure authentication usable anywhere," in Proc. 4th ACM symposium on Usable privacy and security, 2008, pp. 35–45.
[13] T. Pering, M. Sundar, J. Light, and R. Want, "Photographic authentication through untrusted terminals," IEEE Pervasive Computing, vol. 2, no. 1, pp. 30–36, 2003.
[14] W. Jansen, S. I. Gavrila, V. Korolev, R. P. Ayers, and R. Swanstrom, "Picture password: a visual login technique for mobile devices," NIST Interagency/Internal Report (NISTIR)-7030, 2003.
[15] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords." USENIX Association, 1999.