Abstract

Objectives: Authenticating the MobiCloud users using traditional passwords, biometrics is prone to shoulder surfing attack and need external device. Pattern Based User Authentication (PBUA) mechanism is introduced to identify and authenticate the users in MobiCloud environment. Methods/Statistical Analysis: To authenticate the users, the whole process is divided into two phases namely, identification and authentication. Dynamic patterns are generated using random mathematical function to select the patterns from the Identity Management (IdM) Server. Pattern matching operation is done using the hash-based technique to match the image pattern sequences quickly with the actual pattern. Findings: Experimental results show that the proposed PBUA is strong enough against shoulder surfing attack. The time taken for pattern matching is very less when compared to existing pattern matching mechanisms. Application/Improvement: PBUA does not need any intermediate table as the patterns are matched directly with original patterns. The complexity of the algorithm is reduced by \( \frac{1}{n^2} \), thus the efficiency is improved \( n^2 \) times. Pattern updation is not required which reduces the user's burden.

Keywords: Authentication, Identity Management, Identification, Mobile Cloud, Pattern Matching

1. Introduction

Nowadays, PCs are no longer dominant as the world is shifting to the mobile platform. Mobile platform is flexible, portable and cheaper compared to PCs. Mobile Cloud Computing (MCC) is the combination of mobile computing, wireless networks and cloud computing where the computation are offloaded from the mobile devices. According to Vision gain report, 45 Billion dollars will be generated by the enterprises. At the same time, over 2,50,000 mobile users were compromised in the mobile attacks. As MCC integrates CC with mobile computing and networks, all the issues are inherited while accessing the cloud services. Due to these issues, the users are not willing to adopt the cloud services. The major security issues are Identity Management (IdM), authentication, confidentiality, integrity, availability, access control, application security and privacy. In order to strengthen the legitimate access over the cloud environment, proper authentication mechanism is needed. User authentication is the critical aspect of the security which prevents the unauthorized access to the MCC user resources. User authentication is the process of validating the identity of the user to ensure legitimacy of the user.

Several mechanisms were proposed to authenticate the users in MobiCloud environment. The following literatures reveal that the authentication fails to express how the adversarial users must be prevented in accessing the cloud resources. Author in suggested an authentication system based on Quick Response (QR) code for MobiCloud Environment. This mechanism allows quick decoding and has used Error Correction Code (ECC). No analysis was carried over the weak points in security and it is difficult to guarantee that the suggested system has higher effect on security. Author in presented an application that uses handwriting recognition as an authentication pattern to certify access in mobile cloud. In this model, the user is recognized by password and unique handwriting style.
This method was inappropriate due to poor accuracy. Author in\(^4\) projected a solution for authenticating mobile cloud consumers using the usual mobile device camera as a fingerprint sensor to get a fingerprint image, process it and realize it. This mechanism produced poor accuracy and inability to identify the unauthorized attempts. Author in\(^5\) proposed an Image based Authentication for secure key exchange between the user and the CSP. The proposed mechanism is resilient against various attacks. But, the burden exists on user as the key computation is performed by the user at their side. Author in\(^6\) designed a model to solve the identification problem of user in MCC environment. This mechanism is mainly based on the fingerprints of the user to prove the user’s identity. This mechanism combines each fingerprint with a password to form a multiple password scheme. This scheme produces poor accuracy and unable to read the fingerprints as the resolution is low. Author in\(^7\) proposed an algorithm where the users are authenticated using graphical password in Mobile Cloud environment. Their algorithm is prone to shoulder surfing attack and also the authentication would not be possible if the device is lost/stolen, as the images are stored locally.

From the analysis, it is evident that there is a need for a better user authentication technique in a MobiCloud environment with improved security, without the need for external devices.

2. Problem Definition

It is important to identify and authenticate the users to prevent unauthorized access of data in MobiCloud Environment. Most of the cloud players use traditional system such as static passwords, Digital Signatures (DS), biometric, digital certificates, etc. for authentication. Typically, the users are authenticated through the username and password that can be verified by the CSP (Server). It would not be sensitive as it can be easily tampered by the malicious user. The problem with the usual passwords are that it can be stolen/lost and also these techniques are not secure enough against vulnerability attacks like shoulder surfing attacks, Password guessing attack, dictionary attack, etc. Moreover, it should not be device dependent. So, there is a vital need for a mechanism to identify and authenticate the users in MobiCloud environment. To eliminate these problems, Pattern Based User Authentication (PBUA) mechanism is proposed to authenticate the user in MobiCloud environment.

3. Importance of Pattern based Authentication

Several areas of research are being presented that the use of image patterns to authenticate users or encrypt information. Textual passwords are sufficient enough to protect against Brute-force attack but needs to be updated often. Pattern based passwords can use set of images and generate a new pattern value to be associated with the image password. Pattern based password bids several paybacks over the traditional textual password system. The user just needs to select the set of images that builds up the pattern sequence instead of using the keyboard characters. By associating the image to the numerical value, the numerical probability can be increased. Thus, the pattern based password will be much tougher to determine programmatically. The use of image passwords makes the user to use the stronger passwords than the textual passwords. The user could not write down the image passwords is an added benefit.

4. PBUA Mechanism

Passwords are not sent through the open unsecured network channel. Key Based Mutual Authentication (KBMA) will be helpful in providing secure communications over the internet and to authenticate the identity of each other in a secure manner\(^8\). Only after that, the user is authenticated. This could prevent the network sniffing, man-in-the-middle attack, etc. Several key techniques have been integrated into the proposed PBUA mechanism for efficient and secure user authentication in MobiCloud environment. Pattern Based User Authentication (PBUA) Mechanism is easier to use than traditional password mechanisms. The PBUA is divided into two phases namely, Identification Phase and Authentication Phase.

4.1 Identification Phase

Initially, the user gives the user ID as input. The Identity Management (IdM) server checks for the desired user ID into the Cloud Server. Figure 1 depicts the work flow of identification phase in MobiCloud environment.

The computation and matching time are reduced as the user ID of the user is checked instantly. Once the given user ID is matched, the user is prompted with a grid of images on their mobile screen, otherwise the user will be denied instantly. The number of images in the grid
varies according to the screen element of the devices. The images are randomly selected from the IdM server and provided to the user.

4.2 Authentication Phase

Figure 2 depicts the work flow of authentication phase in MobiCloud environment.

Now, the user will select the images under the categories which he/she has already selected during the registration process. Each image is mapped with a pattern value. After the selection of images, the cloud server performs the pattern matching. The pattern matching process is offloaded into the cloud environment to overcome energy consumption issue and to reduce the computation time. If the selected pattern is matched, then the user is found to be legitimate and allowed to access the desired cloud resources. Here, the pattern is dynamic to tackle the shoulder surfing attack.

4.3 Procedure of PBUA

Step 1: User submits User ID (UID) as input.
Step 2: IdM Server checks UID instantly.
Step 3: If given UID is matched, user is provided with grid of images.
Step 4: User will select the images from grid.
Step 5: Pattern Matching (PM) operation is done after pattern selection.
Step 6: PM is done using hash-based technique.
Step 7: A hash table is created using following mathematical functions,

\[
h(i,j) = \frac{ij}{10} \text{ for group ID}
\]

\[
h_1(i,j) = ij%10 \text{ for Pattern ID}
\]

Step 8: If the selected patterns are matched, user is legitimate.

5. Experiment and Findings

The following Table 1 shows the sample image pattern which contains the images grouped under the categories. Here, the Table is limited with 10 images under each categories (i.e., 100 images) which is maintained in Identity Management (IdM) Server by the CSP.

Let \( X_0, X_1, \ldots, X_n \) be the group ID and \( 0, 1, 2, \ldots, n \) be the images.

To improve the efficiency of the proposed PBUA mechanism, Hash-based technique is used. This is to hash the item sets into the corresponding buckets which obviously reduces the computation complexity. The following example illustrates how the user is identified and authenticated.

| Images | 0   | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   |
|--------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Categories | X_0  | X_10 | X_20 | X_30 | X_40 | X_50 | X_60 | X_70 | X_80 | X_90 |
|         | X_01 | X_11 | X_21 | X_31 | X_41 | X_51 | X_61 | X_71 | X_81 | X_91 |
|         | X_02 | X_12 | X_22 | X_32 | X_42 | X_52 | X_62 | X_72 | X_82 | X_92 |
|         | X_03 | X_13 | X_23 | X_33 | X_43 | X_53 | X_63 | X_73 | X_83 | X_93 |
|         | X_04 | X_14 | X_24 | X_34 | X_44 | X_54 | X_64 | X_74 | X_84 | X_94 |
|         | X_05 | X_15 | X_25 | X_35 | X_45 | X_55 | X_65 | X_75 | X_85 | X_95 |
|         | X_06 | X_16 | X_26 | X_36 | X_46 | X_56 | X_66 | X_76 | X_86 | X_96 |
|         | X_07 | X_17 | X_27 | X_37 | X_47 | X_57 | X_67 | X_77 | X_87 | X_97 |
|         | X_08 | X_18 | X_28 | X_38 | X_48 | X_58 | X_68 | X_78 | X_88 | X_98 |
|         | X_09 | X_19 | X_29 | X_39 | X_49 | X_59 | X_69 | X_79 | X_89 | X_99 |
• Let ‘A’ be the user with the user ID “gartner85”.
• During registration, user ‘A’ has selected the categories as X₇, X₉, and X₈ as shown in Table 2.
• (i.e.,) So the image patterns must be (X₁₀, X₁₁, X₁₂, X₁₃, X₁₄, X₁₅, X₁₆, X₁₇, X₁₈, X₁₉, X₂₀, X₂₁, X₂₂, X₂₃, X₂₄, X₂₅, X₂₆, X₂₇, X₂₈, X₂₉, X₃₀, X₃₁, X₃₂, X₃₃, X₃₄, X₃₅, X₃₆, X₃₇, X₃₈, X₃₉, X₄₀, X₄₁, X₄₂, X₄₃, X₄₄, X₄₅, X₄₆, X₄₇, X₄₈, X₄₉, X₅₀, X₅₁, X₅₂, X₅₃, X₅₄, X₅₅, X₅₆, X₅₇, X₅₈, X₅₉, X₆₀, X₆₁, X₆₂, X₆₃, X₆₄, X₆₅, X₆₆, X₆₇, X₆₈, X₆₉, X₇₀, X₇₁, X₇₂, X₇₃, X₇₄, X₇₅, X₇₆, X₇₇, X₇₈, X₇₉, X₈₀, X₈₁, X₈₂, X₈₃, X₈₄, X₈₅, X₈₆, X₈₇, X₈₈, X₈₉)
• If the user A logs in, the user ID of the user will be checked with the Cloud Server.
• After matching the user ID, the user will be prompted with the UI containing a grid of images. The grid of images is given to the user using random function for dynamic sequences.
• The user has to select the images under the categories which he has already selected during registration process. Figure 3 shows the selection of image patterns by the user.
• After the selection of images, the Cloud Server (CS) computes and performs pattern matching operation. The pattern matching operation is done using the hash based technique.

Table 2. Registered user’s image pattern

| Registered Users | User ID        | Registered Image Patterns |
|------------------|----------------|--------------------------|
| A                | gartner85      | X₁, X₇, X₉               |
| B                | rahul_amazon12 | X₄, X₈, X₉               |
| C                | 28_sharmapate | X₅, X₆, X₇               |
| D                | Patel_86       | X₁₄, X₁₆, X₅₀            |
| E                | Techno061175   | X₁₀, X₁₁, X₁₂            |

For matching operation, a hash table H is created using a hash function. Group ID is generated using

\[ h(ij) = ij/10 \]

Pattern ID is generated using

\[ h₁(ij) = ij\%10 \]

Let Xᵢ represents the image where i \( \rightarrow \) Group ID and \( j \rightarrow \) Pattern ID.

5.1 Complexity Analysis

For the proposed PBUA, the computation complexity will be \( O(m) \)

Where \( m = k \cdot k_i \)

\( k \) be the number of images selected by the user.

\( k_i \) be the total number of images given to the user.

For the Anurag’s pattern matching mechanism, the computation complexity will be \( O(m^n+n^2) \)

Where, \( n \) be the total number of images in the cloud server.

Then, the computation complexity \( C \) is calculated using the formula

\[
C = \frac{M}{M \cdot n^2} = \frac{1}{n^2}
\]

It is evident that the complexity \( C \) is reduced by \( \frac{1}{n^2} \) times. Table 4 shows the comparison of image patterns between existing Anurag’s pattern matching mechanism and proposed PBUA mechanism.

As represented in Table 4, the registered users A, C, B are legitimate users as the patterns selected by them were
matched exactly with the patterns in Cloud IdM Server. But the users D, E are found to be adversarial users as their selected patterns were not matched with the patterns in IdM Server.

Moreover, existing Anurag’s pattern matching mechanism takes more comparisons for pattern matching operation which consumes more time and the computation complexity is high. This increases the waiting time of the user. This affects the basic characteristics (pay-as-you-go) of Cloud Computing which also violates Service Level Agreement (SLA). Figure 4 shows the number of comparisons between the existing and proposed mechanisms.

From the Figure 4, it is evident that the complexity is reduced by $\frac{1}{n^2}$. It is important to note that the efficiency of proposed PBUA is improved by $n^2$ times than the existing Anurag’s mechanism.

### 6. Conclusion

Researchers presented several mechanisms (i.e., passwords, image pass codes, biometric, two-factor authentication, etc.) to authenticate users. Those existing mechanisms are static, need extra hardware and prone to shoulder surfing attacks. The Pattern Based User Authentication (PBUA) mechanism deals in providing the dynamic patterns for authenticating the users in MobiCloud environment. This dynamic image patterns prevents the shoulder surfing attack. This mechanism involves two process namely, Pattern generation and pattern matching. The dynamic patterns are generated using the mathematical function and pattern matching is done using the hash-based techniques. Another advantage of using PBUA is, the users are not able to store their passwords in their mobile devices. The interpretation results show that the computation complexity is reduced by $\frac{1}{n^2}$ and the efficiency of the mechanism is improved by $n^2$ times.

### 7. References

1. Fernando N, Seng W, Loke L, Rahayu W. Mobile cloud computing: A survey. Future Generation Computer Systems. Elsevier. 2013; 29(1):84–106.
2. Park P, James J, Yang Y, Laurence T, Lee L, Changhoon C. A study on authentication system using QR code for mobile cloud computing environment. Proceedings of CCIS. Springer Berlin Heidelberg. 2011; 184:500–7.
3. Abid S, Hussain M. Security issues and challenges of mobile cloud computing. International Journal of Grid and Distributed Computing. 2013; 6(6):37–50.
4. Rassan IA, Shaher HAL. Securing mobile cloud using fingerprint authentication. International Journal of Network Security and Applications. 2013; 5(6):41–53.
5. Tomar AS, Tak GK, Chaudhar R. Image based authentication with secure key exchange mechanism in cloud. IEEE Proceedings of International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom); India. 2014. p. 428–31.
6. Al-Hamami AH, Al-Juneidi JY. Secure mobile cloud computing based-on fingerprint. WCSIT. 2015; 5(2):23–7.

7. Guo M, Liaw L, Hsiao H, Huang L, Yen C. Authentication using graphical password in cloud. IEEE Proceedings of 15th International Symposium on Wireless Personal Multimedia Communications (WPMC); Taiwan. 2012. p. 177–81.

8. Cecil DA, Arockiam I. Key Based Mutual Authentication (KBMA) mechanism for secured Access in MobiCloud environment. MATEC Web of Conferences, EDP Sciences; 2016. p. 1–5.