Score based Decision System for Imposter Identification using Non-Biometric Authentication Factors

Arivazhagan Nagarajan* and V. S. Shankar Sriram

School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India; yogan.89@gmail.com

Abstract

Objectives: An imposter identification system allows authenticated user to request for regeneration of password while restricting users who possess imposter properties. Existing system in the literature either allows the users to request for regeneration of password or denies access to the users. So the imposter acceptance and genuine rejection percentage is high in the existing system. Methods: The proposed system improves the performance of imposter identification system by adding three levels of non biometric factors to it. Fuzzy score is calculated on each level and the scores are accumulated with its own weight at last level. Using weighted score the threshold is compared and evaluated to make further decisions. Based on the evaluations made with respect to the threshold, the user will be allowed or denied to regenerate the password. Neural Network is applied to find out the threshold value whereas initially the threshold value is randomly assigned. The neural system works on two modes; one is learning mode in which the developer has to validate the system using training and testing dataset. Findings: With the validation, the threshold value is set to the most accurate value. Secondly, the system works on production mode where the end user uses the system. The proposed system increases the performance of imposter identification algorithm by increasing the rate of genuine user acceptance and imposter rejection. Applications: For all, ID-Password based authentication applications which supports Forget password as a sub module for the authentication module.

Keywords: Bio-metric, Imposter, Neural System

1. Introduction

The authentication process is currently providing security in almost all applications and fields. So, the important and head first step to enter into a system illegally is breaking the authentication of that system. There are so many types of authentication now available in the field today. Each and every method focuses its own unique factors to provide security to get access to the system. Breaking an authentication requires much knowledge on the factors which have been deployed to construct the authentication. Few uses biometric factors which needs factors like Retina scan, iris recognition, fingerprint scanning, finger vein ID, facial recognition, voice recognition, etc. which needs the presence of the actual user at the authentication process. And in order to break it, there have been so many hacking tricks have been found. Similarly, non biometric factors are also exists in the scenario, which will not use any biometric factors. On comparing both, the security is bit less in non biometric factors as the presence of user is not mandatory in the process of authenticating user to get access to the system. Out of so many methods to hack into system of an organization or online banking, being the passive listener of email to get into required system is quite difficult to control as the passive listening will not be known the original user. And for the imposter, it is very comfortable and less effort method once after the imposter started listening emails. So, the imposter can wait till the required information is shared in mail without the knowledge of the user. Once the user received any mail...
that the imposter actually wants the process of hacking by impostor to get into the system will starts and after that the impostor can be active or passive.

The authentication allows genuine user to get into system and denies impostor to access the system. So, the impostor has to act as a genuine user to get into the system which is having strong authentication methods. In order to do that, impostor will try to act as genuine user in some other means. In our problem, when the impostor get access to the email of the user and being as passive listener of the email. Whenever the required information about the system which the impostor needs to get access is available through current conversation or found by the impostor through the existing conversation of the mail, the chances are high that the impostor can get into the system.

**Figure 1.** Traditional system.

### 1.1 Traditional Authentication Methods

In our problem, the scenario is the impostor accesses the mail and when the username of the online banking is found by the impostor through the existing conversation in the mail as described in Figure 1. So, now the user can pretend as the genuine user to the online banking system and provides the username to the system and request for password reset link as like the password has been forgot. The online banking system will send a link to the registered mail ID as if it can be accessed only by the genuine user. But as the email is already accessed by the impostor, the impostor can reset password using that link and can enter into system. So, the authentication method failed to deny the impostor to get access to the system. Other methods to get into system are when the user forgets the password, answering for hint questions or some other ways like prompting for last known passwords. But all these methods requires deterministic answer and it should be cent percent matching to get into system, as it allows user to get into system once the process is completed without error. But, expecting deterministic answer for the hint questions and last known password makes the system a tough one to get through, again the issue is sometimes it becomes tough for genuine user itself as it requires deterministic, cent percent matching answers. As, the methods allows user directly into the system, it has to be more secured.

### 2. Proposed Secondary Authentication Module

The proposed project introduces a module before requesting link to reset password and that module is used to identify percentage of genuine property and percentage of impostor property that the requested user possesses. The module prompts users to feeds information in order to find the genuine percentage of user in 1, 2. For the users who score more than the threshold score only allowed to even request link to regenerate password as showed in Figure 2. As passing the module, make the user just to request link to regenerate password, it need not to be more deterministic. The answers to the hint question and the last known password doesn’t need to be cent percent matching. So that the genuine user is provided with some cushioning for answering hint questions and last known passwords and also as the new intermediate module intervention makes the system more secured then the existing system. Answering the last known password and hint questions cent percent matching is difficult as the spelling may vary. So, the lenient character matching algorithm is used to calculate score from answering them. This algorithm doesn’t expect cent percent matching answers, whereas it provides some cushion by excluding Capital-small characters confusion and excluding the spaces, special characters and symbols for hint answers and also it matches with dictionary words and also with internet results for location name. For passwords, the algorithm provides cushion on the special characters changes, dictionary word matching, sequences of words...
and the numbering sequences matching. Through this algorithm, the fuzzy score will be calculated and the calculated score is compared with the threshold score to decide whether the user is imposter or genuine. If the score calculate is higher than the threshold, then the user possesses more genuine property and so the user is allowed to request link to email to regenerate password. If the score is less than the threshold score, then the user possesses more imposter property and so that user will not be allowed to even request for link to regenerate password. Initially, the threshold score is assigned randomly with the references of literatures. To find the exact and accurate threshold, the system is trained with neural network system in learning mode and by passing the already known training and testing dataset. After several times of training the system, threshold score is set to most accurate value. The threshold score is more accurate as the number of times the system got trained. And the threshold defines the system accuracy as the decision is made by comparing with threshold score.

Figure 2. Proposed system.

3. Results

3.1 Comparison of Existing and Proposed System

Compared to the existing system methodologies to send password reset link without any authentication system, the proposed system provides more security by including an intermediate module which identifies the genuine characteristic of the user requested for the password regeneration link to email. And also, as the non-deterministic answers were used to calculate the fuzzy score of the user to find his genuine percentage provides a cushion for the user to feed the answer, as all users cannot be assured to remember the long known password exactly and spelling of the hint answers. So, the security has been increased when a new intermediate module is introduced to even request for password reset link and the hint question and last known password answers is treated in non-deterministic way provides relaxation for the user and it will not reduce security as the result of passing the module is only used to request for reset link to email.

4. Conclusion

As the proposed system provides secondary authentication module, compared with all existing system which allows user to request password reset link directly without authentication, the proposed system is more secured when compared with existing system which allows user to reset password after successful hint answer or last known password entry. The proposed system provides cushion for user to feedback their answers in a non-deterministic way.

5. References

1. Grover J, Hanmandlu M. Hybrid fusion of score level and adaptive fuzzy decision level fusions for the finger-knuckle-print based authentication. Applied Soft Computing. 2015 Jun; 31:1–13.
2. Murofushi T, Sugeno M. A theory of fuzzy measures: Representations, choquet integral and null sets. Journal of Mathematical Analysis and Applications. 1991 Aug; 159(2):532–49.
3. Dass SC, Nandakumar K, Jain AK. A principled approach to score level fusion in multimodal biometric systems. Springer Berlin Heidelberg; 2005 Jul. p. 1049–58.
4. Gao Y, Maggs M. Feature-level fusion in personal identification. Proceeding of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05); 2005. p. 1–6.
5. Goyal M, Yadav D, Tripathi A. Intuitionist fuzzy genetic weighted averaging operator and its application for multiple attribute decision making in E-Learning. Indian Journal of Science and Technology. 2016 Jan; 9(1):1–15.
6. Ross TJ. Fuzzy logic with engineering applications. 2nd ed. John Wiley and Sons Ltd; 2004 Jun.