Minimizing Mobile Frauds by Enhancing Mobile Security

Amit Kalra[1], Kalpana[2] and Sungeeta Singh[1]
[1]Department of Mathematics/Statistics, Amity University, Gurgaon, Haryana, India
[2]Ganga Technical Campus, Soldha, Bahadurgarh, Haryana, India.

International Journal of Engineering & Technology Research
Volume 3, Issue 6, November-December, 2015, pp. 43-47
ISSN Online: 2347-4904, Print: 2347-8292, DOA : 15112015
© IASTER 2015, www.iaster.com

ABSTRACT

In today's world Mobile security is a big concern for everyone because with the lateral advancements in the mobile systems the security is still an area of opportunity. Now day's Mobile phones are used for Banking, Shopping, Storing the financial information's like credit card numbers & important passcodes. Mobile Devices are the replacements of computers in many instances. But no such advancement is being done in mobile security. Some of the ways that are commonly used for mobile security are Static Passwords; Pattern recognitions, Biometric, Face recognitions. It's very easy for the hackers to guess the passwords or break the backend algorithms of these applications.

So, there is a need to make the machine intelligent enough to decide the unauthorized user by artificial intelligence layer incorporated in to it with the help of data sciences. With the advancement in Data sciences various numbers of algorithms can be made which can learn the way a user uses a cell phone like typing speed on emails, typing speed on SMS, Dialing speed etc. In case of any deviation for a longer period of time in any of the above metric will ask for a security question that is only known to the authorized user. The Paper focuses on developing & integrating an algorithm in the mobile devices that will add an artificial intelligence layer in the mobile security.

Keywords: *Mobile Frauds, Mobile Security, Artificial Intelligence, Mobile Security Application.*

I. INTRODUCTION

Minimizing Mobile Frauds by Enhancing Mobile Security

In last few years mobile phone usage has been increased drastically. Apart from the normal calling mobile phones can be used for Surfing internet, Mobile Banking, Playing Games etc. For many of the users it is being used in place of computers in many instances. As per the data collected for 2013 there are more than 95% mobile users across the world (6,800,000,000+ Mobile phone users/7,012,000,000 (Total world Population). In the above figure, India constitutes to 74.6% mobile users (924318927 (mobile phone users)/1262090000(total population)).

Yet for every positive development in the market there is an associated risk. Mobile phone users have been broadly categorized into Smart Phone & Non Smart users. Irrespective of the usage a lot of financial & personal data is being stored by the individuals over the phones which are bit higher in Smart phones as compared to non-smart phones. Research shows the average smartphone user stores more than 740MB of data per month which is used for storing banking passwords, Credit card information, Contact storage, Real life applications etc.

 ISSN (O) 2347-4904
(P) 2347-8292

However, when it comes to mobile security the advancement has still not been realized for the devices & the mobile security is still a concern for millions of the users. More than 87.2% mobile systems today depend on static passwords to authenticate the user's identity. However, these Passwords has a major security concerns & easy to be cracked by the hackers. Users have a tendency to use easy-to-guess passwords, use the same password in numerous accounts, and write passwords or store them on their machines, etc. Lately many of the advancements have been done to increase the mobile security like Biometrics, Face Recognitions etc. but these are never been successful because of quality issues & easy to break algorithms working on the backend.

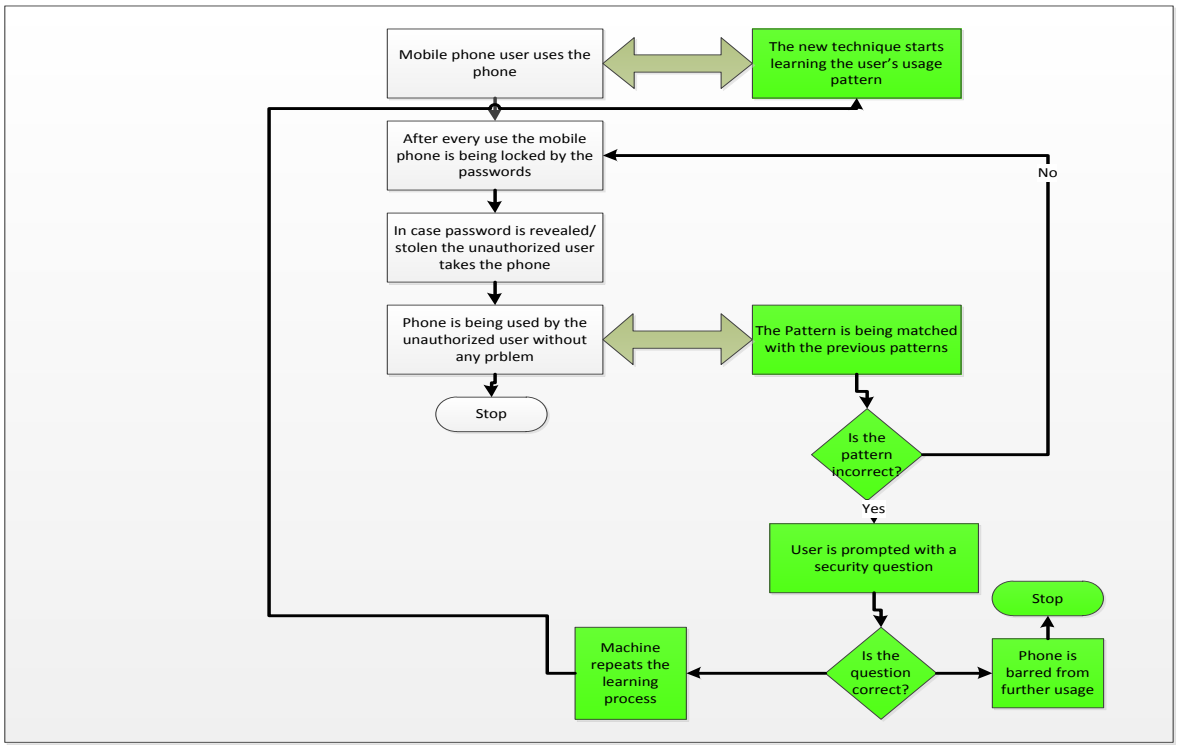
This Paper focuses on developing artificial intelligence to the mobile devices so that the unauthorized user can be barred with a different mobile usage pattern.

II) PROPOSED MOBILE SECURITY APPLICATION THROUGH INTEGRATING MACHINE LEARNING ALGORITHMS & ARTIFICIAL INTELLIGENCE

Mobile security is related with loss or theft of the device, Virus attacks to the system, operating system problems etc. Here the major concern to be focused on is mobile access confidentiality i.e. only authorized users would be able to access the device. Instead of various prevention techniques i.e. through passwords, Biometrics, there is no detection technique available that will detect the unauthorized user by itself. This technology is very well possible by integrating Machine Leanings through statistical analysis with the artificial intelligence to be incorporated in the machine itself.

There is a need to build some algorithms into the mobile systems which will learn from the previous patterns of the authorized users. Basis these algorithms it builds some intelligence within itself which backed by statistical concepts. In case any unauthorized user tries to access the device it clashes with the already learnt algorithms & prompts with the security question (only known to the authorized user) and restricts the entry.

The below mentioned process explains the entire process. The highlighted ones are the newly added high level steps apart from the normal process being followed currently (In grey boxes).



 ISSN (O) 2347-4904
(P) 2347-8292

The concept has several challenges which are resolved with the following solutions

1. Machine Learning Algorithm

Definition:
Machine learning is defined as a task where system automatically learns from the past data & records.

Problem:

- How the machine will learn?
- Which algorithm to be deployed?
  Integrating different machine learning techniques is a future direction. For example, integrating neural networks with advanced statistical techniques creates the possibility of creating the robust system.

  The following example shows the working of the algorithm:-

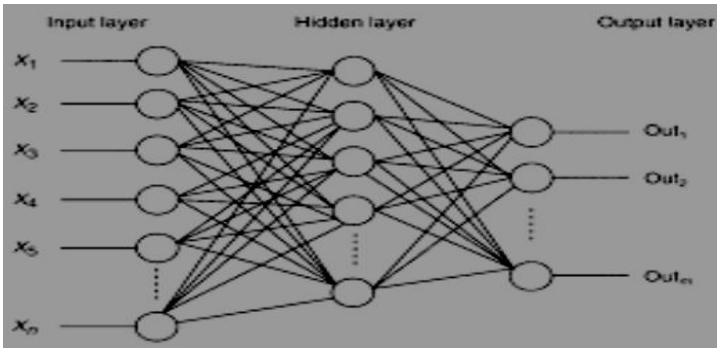


Figure 2 – Working of the Algorithm

Input layers constitute of various input variables to be incorporated for the leanings & hidden layer comprises of the activation function to be deployed. The Output layers are the final variables to be derived from the analysis.

Problem needs to be encountered are no. of input variables & no. of output variables to be deduced.

2. Artificial Intelligence Development

Definition:
Artificial intelligence (AI) is an area that emphasizes on creation of intelligent machines that work and reacts like humans. Some of the activities computers with artificial intelligence are designed for include:

- Recognition
- Learning
- Planning
- Problem solving

Problem instance:

- Variables: Creation of variables that act as an intelligent layer between user & machine
  - How many variables to be created
  - What all activation function they will carry
- Constants:
  - What is the value to be assigned to a constant
  - Controlling the constant behavior basis user's access

 ISSN (O) 2347-4904
(P) 2347-8292

3. Tolerance

Whenever authorized user tries to access the mobile device with some other pattern then the system should have defined tolerance beside the output that machine learning algorithm is providing. Problem to be encountered is the limit of the tolerance to be baked in.

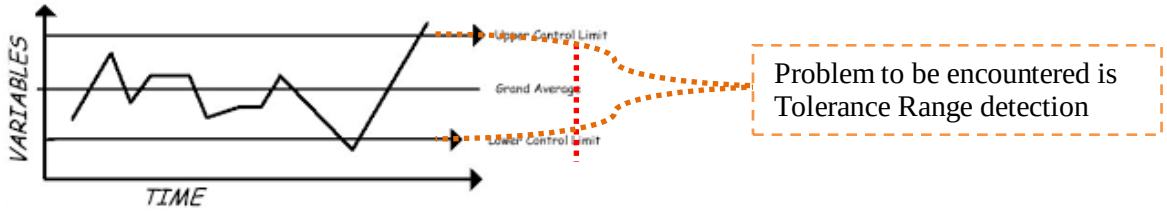


Figure 3 Tolerance

4. Possible Applications / Case Studies of the Proposed Solution

This part covers the current preventive security features & reviews the new research w.r.t. employment of proactive ways to automatically detect & prevent the security concerns.
The effectiveness of the new solutions is also covered in the section.

The methodology integrates the machine learning, Artificial intelligence & various statistical concepts to protect the devices for any of the misuse without being known to the user. The User uses the cell phone for multiple purposes i.e. Dialing the phone number, typing & sending the SMS, uses various applications, types & sends email(only for smart phones) etc. Every user has a different typing speed, different no. dialing speed, different time between the keystrokes etc. Various Machine learning algorithms can be deployed (discussed later in the section) which can learn the user pattern for a certain period of days i.e. 30 days & a layer of artificial intelligence can be formed which are derived from the learnt data for example 40% of typing speed+40% of no. dialing speed+20% of time between keystrokes. The standard deviation of the outcome is added & subtracted from the final layer to compute the upper & lower control limits.

At any point of time if any of the particular input parameter gets changed say typing speed & it reaches beyond UCL or LCL for 10 consecutive entries then user would be prompted with the security question. If the security question is not entered or found incorrect the device automatically get locked & won't be accessed again In case security question is correct then the machine revises its learning & the entire cycle continues again. The below mentioned figure elaborates the concept:-

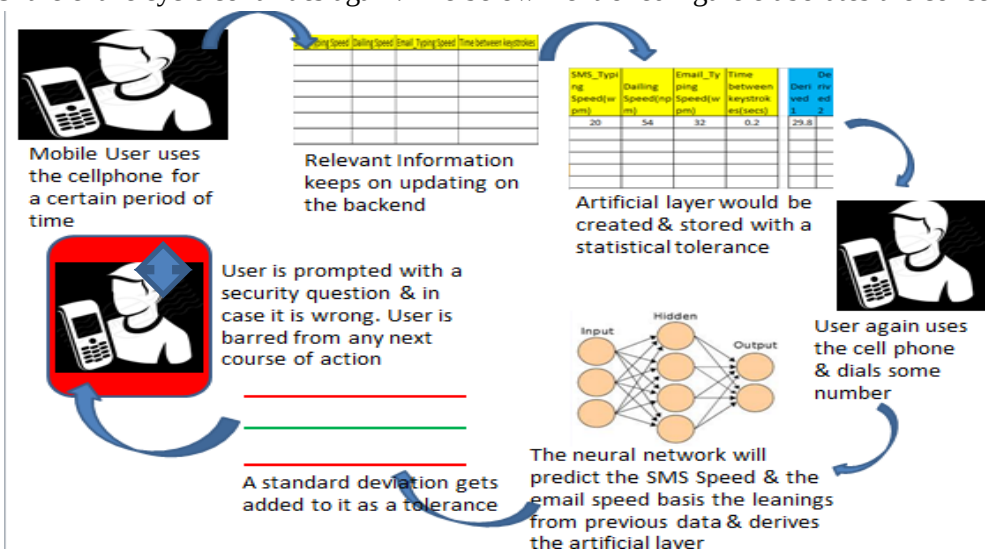


Figure 4

 ISSN (O) 2347-4904
(P) 2347-8292

II) STEPS IN THE PROPOSED ALGORITHM

The steps to be followed in the MINIMIZING MOBILE FRAUDS BY ENHANCING MOBILE SECURITY are as follows:

1. User uses the phone for a certain period of time.
2. A backend database is maintained for the same regarding various information like Time taken for keystrokes in dialing, Text typing speed,Email typing speed.
3. An artificial layer gets derived from the extracted variables mentioned in step 2 & post that it stops learning.
4. Whenever user uses the phone further for every 3-4 instances it matches the results with already fed data & in case user uses the phone for a specified use only(like only for calling purpose) then machine learning algorithm predicts the other variables basis the already learnt data. Basis this new artificial layer gets formed.
5. A certain specified tolerance (standard deviation) is added & subtracted from the derived artificial layer.
6. A security question is prompted to the user in case the layer crosses the tolerance & device is barred for further usage in case the question is incorrect. If question is correct than algorithm starts learning again.

III) SIGNIFICANCE OF THE PROPOSED RESEARCH

1) The proposed solution is an auto detection technique which has never been used ever in the telecom industry. This has the capability of auto detecting the mobile frauds without being known to the user.

2) It does not require any password authentication & very easy to implement.

3) It guarantees to find the unauthorized user without any complications.

4) The results provided by the algorithm can be further improvised to control the Laptop frauds & in many more applications.

REFERENCES

[1] Census.gov. Retrieved 2009-11-10

[2] 053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report

[3] Zipnet, Zonnal Integrated Police Network

[4] 2013 Cost of Data Breach Study: Global