



Security Evaluation of Adversarial Application

¹Ashwini Karde, ²Pooja Sable, ³Ruksar Inamdar, ⁴A. G. Baviskar

^{1, 2, 3} B.E. COMP & SPPU, ⁴Asst. Prof. in CSE

^{1, 2, 3, 4} JSPM'S Bsiotr Wagholi, Pune, Maharashtra, India

Abstract— *In this article, we review previous work of security evaluation and proposed new system. The system used for three common adversarial applications, like biometric authentication, network intrusion detection, and spam filtering. The systems is being increasingly used to control physical access to high-security facilities. In the case of biometrics authentication there are many vulnerabilities which harm the system, in the proposed system framework provide security by using pattern classifier approach. Also provide secure authentication service for NIDS application. In spam filtering the important problem is that Intruder harm the system using Spam email, and the spam email is directly save in the inbox. The framework used good-word and convert malicious email into the legitimate mail.*

Keywords: - *Pattern classification ,adversarial classification, security appraise.*

I. INTRODUCTION

Pattern classifiers are mostly used in those applications on which attacks are happens, like biometric authentication, spam filtering, NIDS etc. In those applications the information is modified by peoples according to their purposes. In this paper, we are creating a framework which is prevent to the attack which are happens earlier. We are creating a framework with the help of testing and training datasets. We are providing a authentication through the biometric organs (face pattern) for biometric authentication.

We are preventing the attacker to upload the .exe file in the NIDS and we are taking the Gmail scenario to classify the legitimate and illegal mails in Spam Filtering. We are trying to improve the performance of existing system and make it the live application. We are taken into consideration the vulnerabilities, the attacks, the countermeasures, and defense mechanisms. Also we uses the machine learning algorithms for that. We are given the attacks as input and take output as a security measure.

There are three main open issues:

1. Categorize the attacks according to pattern.
2. Find the countermeasure for that.
3. Apply the defense mechanism.
4. Measure the performance.

In this paper, firstly we taken into consideration the existing system then we find the drawback of existing system and then we decided our proposed system. The most focus is given on NIDS and Spam filtering. We are taking the review of previous work done related to those applications in section 2. In section 3, we are consisting the proposed system. Also we are developing the framework for security. In section 4, we are taken the application examples. For example- Biometric Authentication, Spam Filtering, NIDS. In section 5, we are taken the performance measure using the testing and training datasets. In section 6, we summarize the Assistance, Limitations and some open issues of our system.

II. EXISTING SYSTEM

In Existing system they classify the pattern for security purpose. Existing system used some adversarial application like Spam filtering in that spam message also saved in inbox. If intruder send some malicious files with mails it is harmful for user account sometime that system attack is not identify easily. Biometrics is a field of technology is used in the identification of individuals it based on some physical attribute. But it not gives accurate result. NIDS is another application, NIDS is a network security system used to focus on the attacks that come from the inside of the network but intruder send malicious files on network and create the traffic in the network. In existing system they analyse the attack and provide security after completing attack.

Disadvantages of Existing System:

1. Poor analysis of attacks and their classification.
2. It does not provide security accurately .

III. PROPOSED SYSTEM

Framework:-

We create a new framework to provide security to adversarial application. In this work we address issues developing a framework for the empirical evaluation of classifier security. we also propose algorithm used for security evaluation and generation of training and testing sets.

when user wants to enter into the system first user log in into the system if user is a authenticated person and he enter correct user id, password and also correct pattern only then system permit user to access the system. If enter pattern is wrong then pattern manager manage or classify the pattern and provide more security the user account. And also provide account information to user. In the proposed system pattern manager find out the pattern of attack and provide security to user account before attack is completed.

We define a general models :-

1. Pattern classification Modules
2. Adversarial classification Modules
3. security Modules
4. Performance Modules

SYSTEM ARCHITECTURE:

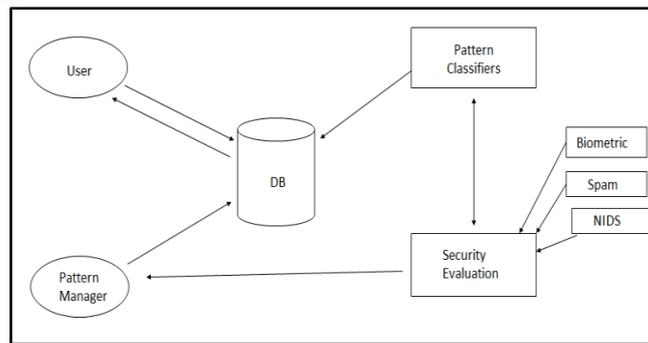


Fig: System Architecture:-

IV. APPLICATION EXAMPLES

- **Biometric authentication:**

In this firstly, our system take the pattern from the user at the time of registration. Then this pattern is saved into the database .Later on when the user trying to use his account, he has to give only this pattern which is entered at the time of registration. Then and then only permission is granted to system particular user. If the attacker try to attack on the account of user, our system firstly match this pattern to the pattern saved in database. If these matches then and then only access is granted otherwise it is consider as attack and access is denied. The admin take appropriate action .We are take pattern as face recognition and trying to improve the performance.

- **Spam filtering:**

A spam filter is a program is used to detect unwanted email and prevent those messages from getting to a user's inbox. Some methods are not especially effective, too often omitting perfectly legitimate messages and letting actual spam through. More sophisticated programs. Regarding to the Spam filtering the list of bad words are provided. When the mail is occur, if there are most number of links provided or a single word is repeated again and again, then our system is consider that this is a spam mail. Then the system compares those bad words to the bad word list. If some words are matches then we definitely tell that it is really a spam mail. Then our system replaces those bad words by good words so that it is become the legitimate mail and we send it into inbox. Then this mail submitted to the legal mails i.e. in inbox. If those mails are not useful then it send to the illegal mails i.e. spam.

- **NIDS:**

NIDS is a network security system used to focus on the attacks that come from the inside of the network (authorized users). Network Intrusion Detection Systems (NIDS) are placed within the network to monitor traffic to and from all devices on the network. It analysis of passing traffic on the entire subnet and match the traffic that is passed on the subnets to the known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert send to the administrator. In this article, our system prevented to uploading the .exe file which is attach to the mail by attacker. So that the network intrusion does not occur. And if the attack happens, it is handled by our system and Administrator.

V. CONCLUSIONS

The current applicants which are using the Adversarial applications such as Biometric Authentication, Network Intrusion Detection, Spam Filtering in which data can be purposely manipulated by humans to undermine their operations. They don't know the ongoing things such as attacks on these data by Intruder. This can be resolved by evaluating the security of pattern so that the applicant gets benefited.

REFERENCES

- [1] Kong,A.W.K.; Zhang, D.; Kamel, M, "Analysis of Brute-Force Break-Ins of a Palmprint Authentication System",2006.
- [2] HaiyingShen; ZeLiComputers, IEEE Transactions on" Leveraging Social Networks for Effective Spam Filtering",2014

- [3] Pinto, A.; Robson Schwartz, W.; Pedrini, H.; De Rezende Rocha, A. "Using Visual Rhythms for Detecting Video-Based Facial Spoof Attacks",2015.
- [4] Nwanze, N. ; Electr.&Comput. Eng., State Univ. of New York at Binghamton, Vestal, NY, USA ; Sun-il Kim ; Summerville, D.H. "Payload modeling for network Intrusion Detection Systems ",18-21 Oct. 2009
- [5] Biggio, B. ; Dept. of Electr.& Electron. Eng., Univ. of Cagliari, Cagliari, Italy ; Akhtar, Z. ; fumera, g. ; Marcialis, G.L. "security evaluation of biometric authentication systems under real spoofing attacks " , March 2012.
- [6] Cardenas, A.A. ; Dept. of Electr.&Comput. Eng., Maryland Univ., College Park, MD ;Baras, J.S. ; Seamon, K. "A framework for the evaluation of intrusion detection systems ",21-24 May 2006.
- [7] Zolotukhin, M. ; Dept. of Math. Inf. Technol., Univ. of Jyvaskyla, Jyvaskyla, Finland ; Hamalainen, T. ; Kokkonen, T. ; Siltanen, J. "Analysis of HTTP Requests for Anomaly Detection of Web Attacks",2014
- [8] Detection for Zero-Day Attacks: (Not) A Closed Chapter?",2014.
- [9] Biggio, B.; Fumera, G.; Russu, P.; Didaci, L.; Roli, F. "Adversarial Biometric Recognition",2015.
- [10] Das, A.; Nguyen, D.; Zambreno, J.; Memik, G.; Choudhary, A. "An FPGA- Based Network Intrusion Detection Architecture",2008.