Security Evaluation of Adversarial Applications

Ashwini Karde
Student
Department of Computer Engineering
JSPM'S BSIOTR College Wagholi, Pune

Ruksar Inamdar
Student
Department of Computer Engineering
JSPM'S BSIOTR College Wagholi, Pune

Pooja Sable
Student
Department of Computer Engineering
JSPM'S BSIOTR College Wagholi, Pune

Abstract

Security Evaluation system is used in adversarial applications, like biometric authentication, network intrusion detection, and spam filtering. The system is used to control physical access for high-security facilities The existing system in which data can be control by humans to execute their operation. In Adversarial Applications it prevents unauthorized person to gain access in account, system use the secure key for authentication purpose, also it only uploads the text file which are not harmful file for user account. The system scans the file and if it is harmful prevent it from uploading and send the report to system. In spam Filtering it converts all bad words into the good words. Reported results show that the system can provide a more secure platform for adversarial environments.

Keywords: adversarial classification, Pattern classification, performance evaluation, robustness evaluation, security evaluation

I. INTRODUCTION

Pattern classification is the system, based on machine learning algorithms, the system used in applications which are related to security. But in that existing system data can be control by humans to execute their operation, because of that more types of attacks are occurred like spoofing attack (submit a fake biometric pattern to a biometric authentication system) network packets modifying and sending unwanted or virus files to the users account. In our system we provide a security to Adversarial applications like biometric authentication, network intrusion detection, and spam filtering.

Three main open issues are identified:

1) According to pattern analyze and categorize the attacks.
2) Take the appropriate action on that.
3) Measure the performance.

In our Propose system we had focused on adversarial applications. By considering the drawback of our existing system we implement on it to provide more security to proposed system. There are four different modules in our system.

1) Adversarial classification Modules
2) Pattern classification Modules
3) Performance Modules
4) Security Modules

By using that module, it makes our system more secure. In section 2 we find out all drawback of previous work. in section 3 we describe our four modules and their examples in adversarial applications of proposed system. in section 4 we summarize the Limitations and some open issues of our system.

II. EXISTING SYSTEM

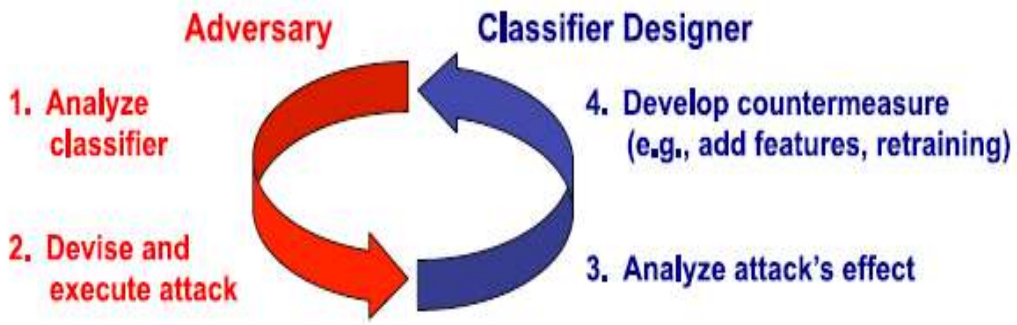

Fig. 1: Existing System

Existing system used pattern classification for security purpose. Existing system used some Security applications like, Biometrics is a field of technology it used in authentication of a user, is mostly based on physical attributes. But, sometime it does not give accurate result. Spam filtering in that spam message also saved in inbox. If attacker send the mails with malicious files then it is harmful for user account, sometimes it is very difficult to identify these type of system attack. NIDS is the application in which attacker send malicious files on network and create the traffic in the network. Mainly in existing system data control by humans to execute their operation, because of that more types of attacks are occur. Also in existing system they analyse the attack and provide security after completing attack.

A. Disadvantages of Existing System

1) Poor analyzation & classification of attacks.
2) It does not provide security accurately.

III. PROPOSED SYSTEM

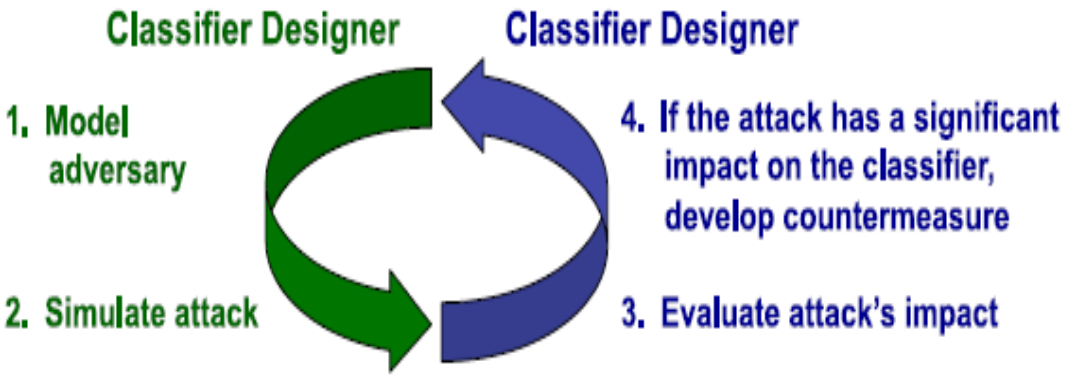

Fig. 2: Proposed System

We create a new system to provide security to adversarial application. In this we used the algorithm for security evaluation and also generate training and testing data sets. We use Divide & conquer strategy for the system, means we divide our system in four modules provide security to that.

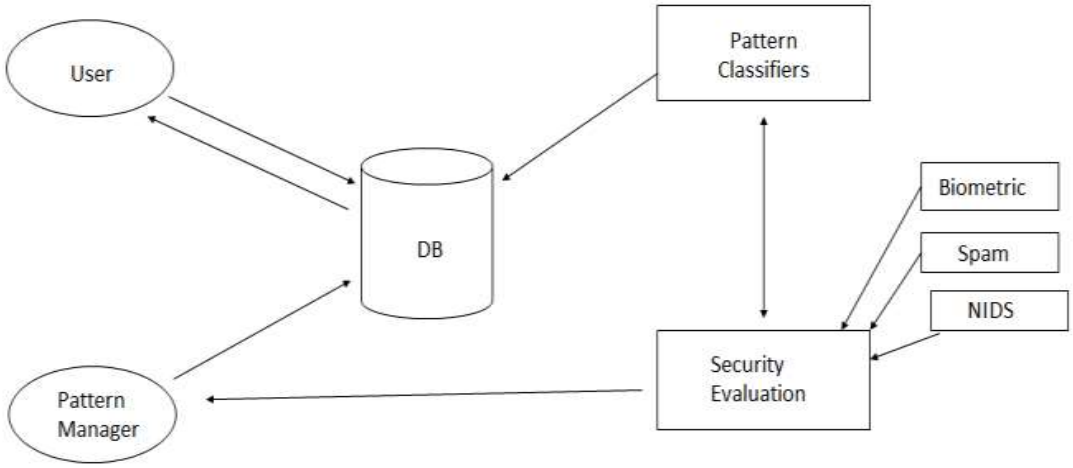

Fig. 3: System Architecture

when user wants to enter into the system first user log in into the system if user is an authenticated person and he enter correct user id, password, correct pattern and also security key which is received on Gmail account only then system permit user to access the system. If entered key is wrong, then access is denied and provide more security to the user account. And also provide account information to admin. In the system admin scan the file and see the malicious file which is send by the attacker.

A. Pattern Classification Modules

Biometric authentication is a type of system it used only unique biological characteristics of person to verify identity for secure access to electronic systems, by which a person can identified uniquely Multimodal biometric systems for authorized identification have received great interest in the past few years. In Biometric authentication it provides security to user account. By giving a

unique user Id and password also pattern to that system. At the log in time when user enter all those things which is entered at the time of registration at that time secrete key has been generate & it will be send on user Gmail, only by using that secrete key user can access the account. If user enter wrong secrete key or password, then access denied.

B. Adversarial Classification Modules

In that a system has to discriminate between legitimate and spam emails on the basis of their textual content, and the bag-of-words feature representation is used. attacker upload a file which contain spam words then, system scan that file, replace that bad words with good words. The system sends the account information to the admin. Admin classify the attack and provide security to system.

C. Security Modules

Network Intrusion detection systems are used to analyze network packets. Then it to prevent and detect the harmful or mischievous activity done by attacker. Multimodal biometric systems are best suited for particular situations, like biometric authentication. To fulfill this condition, some solutions are used to capture images of biometric organs at the time of registration and match these at the time of login. Port scans, and denial-of-service attacks are the examples of NIDS Attack. When suspected harmful data is detected, some notification is given by the system and simultaneously handled by the system administrator.

Two main types of IDSs exist: anomaly-based ones and misuse detectors. Misuse detectors is used to analyze the network traffic against a malicious Activities. The main disadvantage is that they can't detect the harmful activities which not seen previously. To overcome this drawback anomaly-based detectors have been used.

IV. PERFORMANCE MODULES

The performance is generally computed in terms of genuine acceptance rate (GAR) and false acceptance rate (FAR). GAR and FAR are measured by using the ROC curve which indicate the GAR, under the upper model selection process. Eight kinds of classifier modes should be evaluated.

V. CONCLUSION

Our system divided into the four modules by using that we provide the security to the Adversarial applications such as Biometric Authentication, Spam Filtering, Network Intrusion Detection. System permit only authorized person to gain access the account. System used the secret key to gain access in the account.

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.