Volume No:2, Issue No:9 (February-2017) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Protection Evaluation of Prototype Classifiers under Attack

Jadi Vasantha
Assistant Professor,
Department of CSE,
VIF College of Engineering and Technology.

Akhil Mohd
Assistant Professor,
Department of CSE,
VIF College of Engineering and Technology.

Manjula. A
Associate Professor & HOD,
Department of CSE,
VIF College of Engineering and Technology.

ABSTRACT:

Prototype categorization system are usually used in adversarial application, like biometric authentication, network interruption discovery, and spam filtering, in which data can be purposely manipulate by humans to challenge their process. As this adversarial situation is not engaged into account by traditional plan methods, prototype categorization system may show vulnerabilities, whose utilization may strictly affect their presentation, and consequently boundary, their practical utility. extend pattern categorization theory and plan methods to adversarial setting is thus a account and very relevant investigate direction, which has not yet been pursued in a systematic way.

In this paper, we speak to single of the major open issues: evaluate at plan phase the safety of pattern classifiers, namely, the performance poverty under possible attacks they may bring upon you during operation. We suggest a structure for experiential evaluation of classifier security that formalizes and generalizes the main ideas proposed in the literature, and give examples of its utilize in three real application. Report results show that safety assessment can provide an additional complete sympathetic of the classifier's behaviour in adversarial environment, and guide to improved design choice.

INTRODUCTION:

Prototype categorization system based on machine knowledge algorithms are usually used in security-related application like biometric verification, network intrusion recognition, and spam filter, to discriminate between a "legitimate" and a "malicious" prototype class (e.g., legitimate and spam emails).

Opposing to traditional ones, these application have an fundamental adversarial environment since the contribution information can be intentionally manipulated by an intellectual and adaptive opponent to undermine classifier operation. This often gives rise to an arms race between the opponent and the classifier exclusive. Well known examples of attacks against pattern classifiers are: submit a fake biometric trait to a biometric authentication system (spoofing attack) modifying network packets belonging to intrusive traffic to evade intrusion detection systems (IDSs) manipulate the content of spam e-mail to get them past spam filter (e.g., by misspelling common spam words to avoid their detection. Adversarial scenarios can also occur in clever data analysis and in order recovery.

EXISTING SYSTEM:

Prototype categorization system based on traditional theory and plan method do not obtain into account adversarial settings, they exhibit vulnerabilities to several possible attack, allowing adversary to challenge their effectiveness. A methodical and combined treatment of this subject is thus needed to agree to the trusted acceptance of pattern classifiers in adversarial environments, starting from the theoretical foundations up to novel design methods, extending the classical design cycle of. In exacting, three main open issues can be identified: (i) analyze the vulnerabilities of classification algorithms, and the corresponding attacks. (ii) initial novel method to assess classifier safety against these attack, which is not likely using usual performance assessment methods. (iii) initial novel design methods to assurance classifier safety in adversarial environment.

DISADVANTAGES OF EXISTING SYSTEM:

1. Unfortunate analyzing the vulnerabilities of categorization algorithms, and the matching attack.
2.A spiteful webmaster may stage-manage search mechanism ranking to artificially support her1 website.

PROPOSED SYSTEM:

During this occupation we address issue above by initial a structure for the experiential assessment of classifier safety at design stage that extend the model assortment and presentation assessment steps of the standard plan cycle .We review preceding work, and point out three main ideas that emerge from it. We then formalize and generalize them in our framework (Section 3). First, to pursue safety in the circumstance of an arms race it is not sufficient to react to observed attacks, but it is also necessary to proactively anticipate the adversary by predicting the most relevant, potential attacks through a what-if analysis; this allows one to expand suitable countermeasures before the assault actually occurs, according to the code of security by propose.

Second, to provide sensible guidelines for simulate realistic attack scenarios, we define a general model of the adversary, in terms of her objective information, and ability, which encompasses as well as generalize models future in preceding work. Third, since the presence of carefully under attack attacks may affect the allocation of training and testing data separately, we propose a model of the data distribution that can formally differentiate this behaviour, and that allow us to take into account a large number of potential attacks; we also suggest an algorithm for the production of training and difficult sets to be used for security assessment, which can of course accommodate application-specific and heuristic technique for simulate attack.

ADVANTAGES OF PROPOSED SYSTEM:

1. Prevent presently beginning original method to consider classifier safety against this attack.
2. The attendance of an quick and adaptive opponent make the categorization difficulty extremely non-stationary.

SYSTEM REQUIREMENTS:

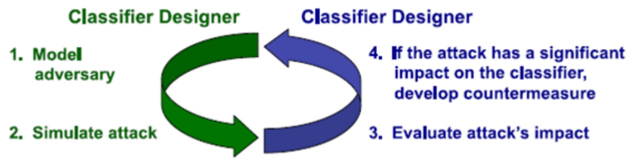
HARDWARE REQUIREMENTS:

➢ System	:	Pentium IV 2.4 GHz.
➢ Hard Disk	:	40 GB.
➢ Floppy Drive	:	1.44 Mb.
➢ Monitor	:	15 VGA Colour.
➢ Mouse	:	Logitech.
➢ Ram	:	512 Mb.

SOFTWARE REQUIREMENTS:

➢ Operating system	:	Windows XP/7.
➢ Coding Language	:	JAVA/J2EE
➢ IDE	:	Netbeans 7.4
➢ Database	:	MYSQL

SYSTEM ARCHITECTURE:


Classifier Designer
Classifier Designer
1. Model adversary
2. Simulate attack
3. Evaluate attack's impact
4. If the attack has a significant impact on the classifier, develop countermeasure

Modules:

IMPLEMENTATION:

MODULES:

1. Attack Scenario and Model of the Adversary
2. Pattern Classification
3. Adversarial classification:
4. Security modules

MODULES DESCRIPTION:

Attack Scenario and Model of the Adversary:

Although the definition of attack scenarios is ultimately an application-specific issue, it is possible to give general guidelines that can help the designer of a pattern recognition system.

Here we propose to specify the attack scenario in terms of a conceptual model of the adversary that encompasses, unifies, and extends different ideas from previous work. Our model is based on the assumption that the adversary acts rationally to attain a given goal, according to her knowledge of the classifier, and her capability of manipulating data. This allows one to derive the corresponding optimal attack strategy.

Pattern Classification:

Multimodal biometric systems for personal identity recognition have received great interest in the past few years. It has been shown that combining information coming from different biometric traits can overcome the limits and the weaknesses inherent in every individual biometric, resulting in a higher accuracy. Moreover, it is commonly believed that multimodal systems also improve security against Spoofing attacks, which consist of claiming a false identity and submitting at least one fake biometric trait to the system (e.g., a “gummy” fingerprint or a photograph of a user’s face). The reason is that, to evade multimodal system, one expects that the adversary should spoof all the corresponding biometric traits. In this application example, we show how the designer of a multimodal system can verify if this hypothesis holds, before deploying the system, by simulating spoofing attacks against each of the matchers.

Adversarial Classification:

Assume that a classifier has to discriminate between legitimate and spam emails on the basis of their textual content, and that the bag-of-words feature representation has been chosen, with binary features denoting the occurrence of a given set of words.

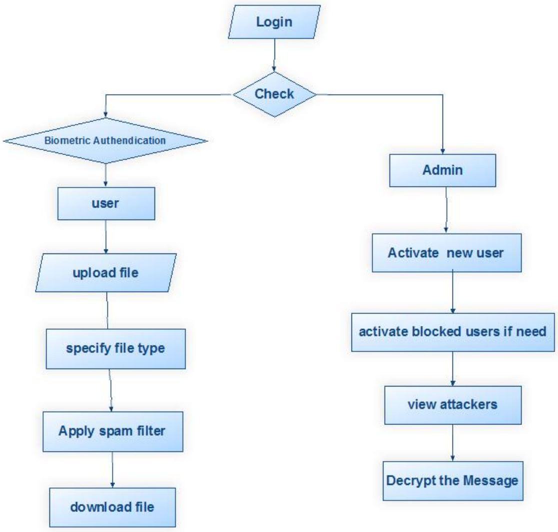
Security Modules:

Intrusion detection systems analyze network traffic to prevent and detect malicious activities like intrusion attempts, ROC curves of the considered multimodal biometric system under a simulated spoof attack against the fingerprint or the face matcher. Port scans, and denial-of-service attacks. When suspected malicious traffic is detected, an alarm is raised by the IDS and subsequently handled by the system administrator. Two main kinds of IDSs exist: misuse detectors and anomaly-based ones. Misuse detectors match the analyzed network traffic against a database of signatures of known malicious activities. The main drawback is that they are not able to detect never-before-seen malicious activities, or even variants of known ones. To overcome this issue, anomaly-based detectors have been proposed. They build a statistical model of the normal traffic using machine learning techniques, usually one-class classifiers, and raise an alarm when anomalous traffic is detected. Their training set is constructed, and periodically updated to follow the changes of normal traffic, by collecting unsupervised network traffic during operation, assuming that it is normal (it can be filtered by a misuse detector, and should)

DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels

that represent increasing information flow and functional detail.



UML DIAGRAMS:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML. The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

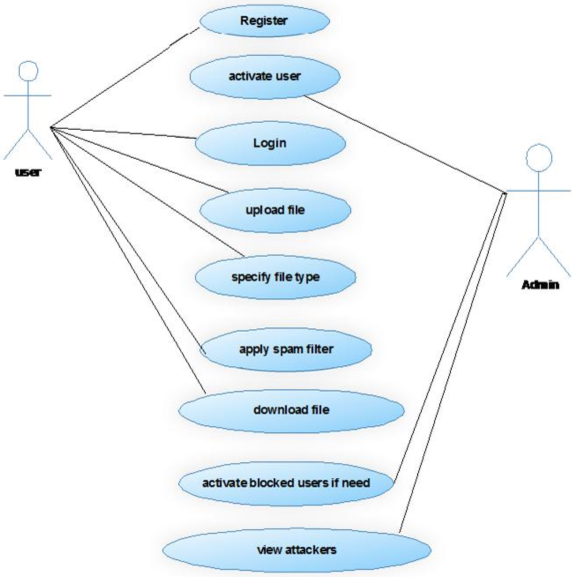
GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

USE CASE DIAGRAM:

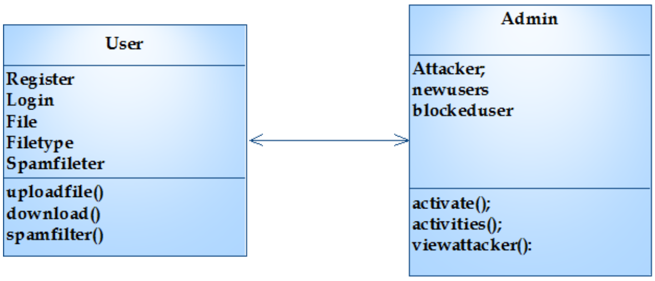
A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



Volume No:2, Issue No:9 (February-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

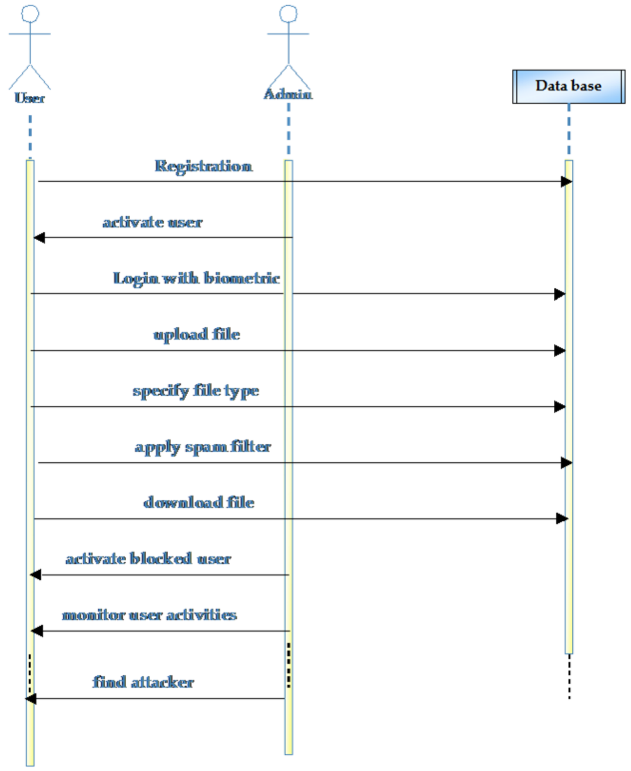
CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.



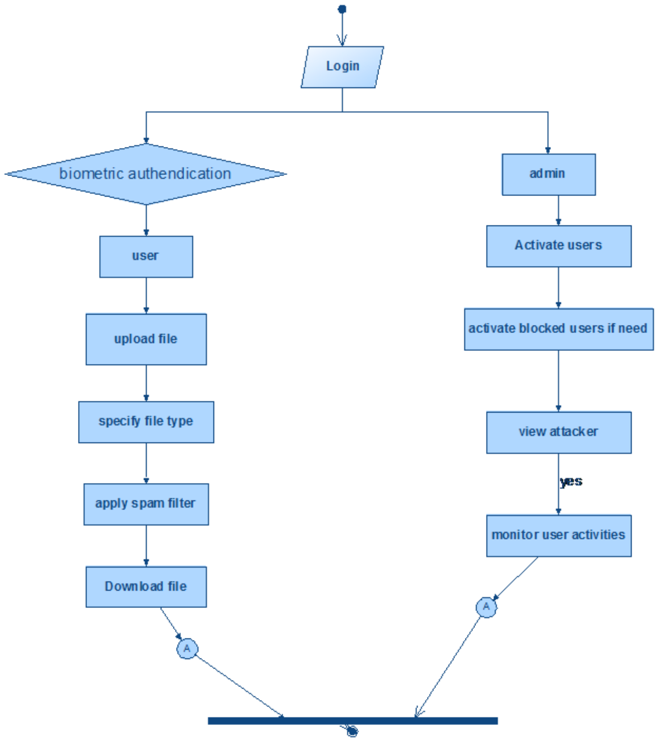
SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.



ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.



LITERATURE SURVEY

1) Robustness of Multimodal Biometric Fusion Methods against Spoof Attacks

AUTHORS: R.N. Rodrigues, L.L. Ling, and V. Govindaraju

In this paper, we address the security of multimodal biometric systems when one of the modes is successfully spoofed. We propose two novel fusion schemes that can increase the security of multimodal biometric systems. The first is an extension of the likelihood ratio based fusion scheme and the other uses fuzzy logic. Besides the matching score and sample quality score, our proposed fusion schemes also take into account the intrinsic security of each biometric system being fused.

Experimental results have shown that the proposed methods are more robust against spoof attacks when compared with traditional fusion methods

2) Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters

AUTHORS: P. Johnson, B. Tan, and S. Schuckers

In biometric systems, the threat of "spoofing", where an imposter will fake a biometric trait, has lead to the increased use of multimodal biometric systems. It is assumed that an imposter must spoof all modalities in the system to be accepted. This paper looks at the cases where some but not all modalities are spoofed. The contribution of this paper is to outline a method for assessment of multimodal systems and underlying fusion algorithms. The framework for this method is described and experiments are conducted on a multimodal database of face, iris, and fingerprint match scores.

3) Polymorphic Blending Attacks

AUTHORS: P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee

A very effective means to evade signature-based intrusion detection systems (IDS) is to employ polymorphic techniques to generate attack instances that do not share a fixed signature. Anomaly-based intrusion detection systems provide good defense because existing polymorphic techniques can make the attack instances look different from each other, but cannot make them look like normal. In this paper we introduce a new class of polymorphic attacks, called polymorphic blending attacks, that can effectively evade byte frequency-based network anomaly IDS by carefully matching the statistics of the mutated attack instances to the normal profiles. The proposed polymorphic blending attacks can be viewed as a subclass of the mimicry attacks. We take a systematic approach to the problem and formally describe the algorithms and steps required to carry out such attacks. We not only show that such attacks are feasible but also analyze the hardness of evasion under different circumstances. We present detailed techniques using PAYL, a byte frequency-based anomaly IDS, as a case study and demonstrate that these attacks are indeed feasible. We also provide some insight into possible countermeasures that can be used as defense.

4) On Attacking Statistical Spam Filters

AUTHORS: G.L. Wittel and S.F. Wu

The efforts of anti-spammers and spammers has often been described as an arms race. As we devise new ways to stem the flood of bulk mail, spammers respond by working their way around the new mechanisms. Their attempts to bypass spam filters illustrates this struggle. Spammers have tried many things from using HTML layout tricks, letter substitution, to adding random data. While at times their attacks are clever, they have yet to work strongly against the statistical nature that drives many filtering systems. The challenges in successfully developing such an attack are great as the variety of filtering systems makes it less likely that a single attack can work against all of them. Here, we examine the general attack methods spammers use, along with challenges faced by developers and spammers. We also demonstrate an attack that, while easy to implement, attempts to more strongly work against the statistical nature behind filters.

5) Good Word Attacks on Statistical Spam Filters

AUTHORS: D. Lowd and C. Meek

Unsolicited commercial email is a significant problem for users and providers of email services. While statistical spam filters have proven useful, senders of spam are learning to bypass these filters by systematically modifying their email messages. In a good word attack, one of the most common techniques, a spammer modifies a spam message by inserting or appending words indicative of legitimate email. In this paper, we describe and evaluate the effectiveness of active and passive good word attacks against two types of statistical spam filters: naive Bayes and maximum entropy filters.

We find that in passive attacks without any filter feedback, an attacker can get 50 % of currently blocked spam past either filter by adding 150 words or fewer. In active attacks allowing test queries to the target filter, 30 words will get half of blocked spam past either fi

Conclusion:

In this paper we focused on experiential safety assessment of prototype classifiers that contain to be deployed in adversarial environment, and future how to revise the usual presentation assessment plan step, which is not appropriate for this reason. Our main giving is a structure for experiential safety assessment that formalizes and generalizes ideas from previous work, and can be practical to different classifiers, knowledge algorithms, and categorization tasks. It is stranded on a official model of the opponent, and on a representation of information sharing that can stand for all the attack considered in previous work; provides a systematic method for the generation of preparation and testing sets that enables security assessment; and can contain application-specific techniques for attack simulation.

This is a clear progression with respect to previous work, since without a general framework most of the proposed techniques (often tailored to a given classifier model, attack, and application) could not be directly applied to other problems. An intrinsic limitation of our work is that security evaluation is carried out empirically, and it is thus information dependent; on the other hand, model-driven analyses [12], [17], [38] require a full analytical model of the difficulty and of the adversary's behavior, that may be very difficult to develop for real-world applications. Another intrinsic limitation is due to fact that our method is not application-specific, and, therefore, provides only high-level guidelines for simulate attacks. Indeed, detailed guidelines require one to take into account application-specific constraints and adversary model. Our future occupation will be dedicated to develop techniques for simulating attacks for different applications. though the design of secure classifiers is a distinct problem than security evaluation, our framework could be also exploited to this end. For instance, simulated attack samples can be included into the training data to improve security of discriminative classifiers (e.g., SVMs), while the proposed data model can be exploited to intend more safe generative classifiers. We obtain encouraging beginning outcome on this theme.

REFERENCES:

[1] R.N. Rodrigues, L.L. Ling, and V. Govindaraju, "Robustness of Multimodal Biometric Fusion Methods against Spoof Attacks," J. Visual Languages and Computing, vol. 20, no. 3, pp. 169-179, 2009.

[2] P. Johnson, B. Tan, and S. Schuckers, "Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters," Proc. IEEE Int'l Workshop Information Forensics and Security, pp. 1-5, 2010.

[3] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee, "Polymorphic Blending Attacks," Proc. 15th Conf. USENIX Security Symp., 2006.

[4] G.L. Wittel and S.F. Wu, "On Attacking Statistical Spam Filters," Proc. First Conf. Email and Anti-Spam, 2004.

[5] D. Lowd and C. Meek, "Good Word Attacks on Statistical Spam Filters," Proc. Second Conf. Email and Anti-Spam, 2005.

[6] A. Kolcz and C.H. Teo, "Feature Weighting for Improved Classifier Robustness," Proc. Sixth Conf. Email and Anti-Spam, 2009.

[7] D.B. Skillicorn, "Adversarial Knowledge Discovery," IEEE Intelligent Systems, vol. 24, no. 6, Nov./Dec. 2009.

[8] D. Fetterly, “Adversarial Information Retrieval: The Manipulation of Web Content,” ACM Computing Rev., 2007.

[9] R.O. Duda, P.E. Hart, and D.G. Stork, Pattern Classification. Wiley-Interscience Publication, 2000.

[10] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, “Adversarial Classification,” Proc. 10th ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining, pp. 99-108, 2004.

[11] M. Barreno, B. Nelson, R. Sears, A.D. Joseph, and J.D. Tygar, “Can Machine Learning be Secure?” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 16-25, 2006.

[12] A.A. C_ardenas and J.S. Baras, “Evaluation of Classifiers: Practical Considerations for Security Applications,” Proc. AAAI Workshop Evaluation Methods for Machine Learning, 2006.

[13] P. Laskov and R. Lippmann, “Machine Learning in Adversarial Environments,” Machine Learning, vol. 81, pp. 115-119, 2010.

[14] L. Huang, A.D. Joseph, B. Nelson, B. Rubinstein, and J.D. Tygar, “Adversarial Machine Learning,” Proc. Fourth ACM Workshop Artificial Intelligence and Security, pp. 43-57, 2011.

[15] M. Barreno, B. Nelson, A. Joseph, and J. Tygar, “The Security of Machine Learning,” Machine Learning, vol. 81, pp. 121-148, 2010.

[16] D. Lowd and C. Meek, “Adversarial Learning,” Proc. 11th ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining, pp. 641-647, 2005.

[17] P. Laskov and M. Kloft, “A Framework for Quantitative Security Analysis of Machine Learning,” Proc. Second ACM Workshop Security and Artificial Intelligence, pp. 1-4, 2009.

[18] NIPS Workshop Machine Learning in Adversarial Environments for Computer Security, http://mls-nips07.first.fraunhofer.de/, 2007.

[19] Dagstuhl Perspectives Workshop Mach. Learning Methods for Computer Sec., http://www.dagstuhl.de/12371/, 2012.

[20] A.M. Narasimhamurthy and L.I. Kuncheva, “A Framework for Generating Data to Simulate Changing Environments,” Proc. 25th Conf. Proc. the 25th IASTED Int’l Multi-Conf.: Artificial Intelligence and Applications, pp. 415-420, 2007.

[21] S. Rizzi, “What-If Analysis,” Encyclopedia of Database Systems, pp. 3525-3529, Springer, 2009.

[22] J. Newsome, B. Karp, and D. Song, “Paragraph: Thwarting Signature Learning by Training Maliciously,” Proc. Ninth Int’l Conf. Recent Advances in Intrusion Detection, pp. 81-105, 2006.

[23] A. Globerson and S.T. Roweis, “Nightmare at Test Time: Robust Learning by Feature Deletion,” Proc. 23rd Int’l Conf. Machine Learning, pp. 353-360, 2006.

[24] R. Perdisci, G. Gu, and W. Lee, “Using an Ensemble of One-Class SVM Classifiers to Harden Payload-Based Anomaly Detection Systems,” Proc. Int’l Conf. Data Mining, pp. 488-498, 2006.

[25] S.P. Chung and A.K. Mok, “Advanced Allergy attacks: Does a Corpus Really Help,” Proc. 10th Int’l Conf. Recent Advances in Intrusion Detection (RAID ’07), pp. 236-255, 2007.

[26] Z. Jorgensen, Y. Zhou, and M. Inge, “A Multiple Instance Learning Strategy for Combating Good Word

Attacks on Spam Filters," J. Machine Learning Research, vol. 9, pp. 1115-1146, 2008.

[27] G.F. Cretu, A. Stavrou, M.E. Locasto, S.J. Stolfo, and A.D. Keromytis, "Casting out Demons: Sanitizing Training Data for Anomaly Sensors," Proc. IEEE Symp. Security and Privacy, pp. 81-95, 2008.

[28] B. Nelson, M. Barreno, F.J. Chi, A.D. Joseph, B.I.P. Rubinstein, U. Saini, C. Sutton, J.D. Tygar, and K. Xia, "Exploiting Machine Learning to Subvert Your Spam Filter," Proc. First Workshop Large- Scale Exploits and Emergent Threats, pp. 1-9, 2008.

[29] B.I. Rubinstein, B. Nelson, L. Huang, A.D. Joseph, S.-h. Lau, S. Rao, N. Taft, and J.D. Tygar, "Antidote: Understanding and Defending against Poisoning of Anomaly Detectors," Proc. Ninth ACM SIGCOMM Internet Measurement Conf. (IMC '09), pp. 1-14, 2009.

[30] M. Kloft and P. Laskov, "Online Anomaly Detection under Adversarial Impact," Proc. 13th Int'l Conf. Artificial Intelligence and Statistics, pp. 405-412, 2010.

[31] O. Dekel, O. Shamir, and L. Xiao, "Learning to Classify with Missing and Corrupted Features," Machine Learning, vol. 81, pp. 149- 178, 2010.

[32] B. Biggio, G. Fumera, and F. Roli, "Design of Robust Classifiers for Adversarial Environments," Proc. IEEE Int'l Conf. Systems, Man, and Cybernetics, pp. 977-982, 2011.

[33] B. Biggio, G. Fumera, and F. Roli, "Multiple Classifier Systems for Robust Classifier Design in Adversarial Environments," Int'l J. Machine Learning and Cybernetics, vol. 1, no. 1, pp. 27-41, 2010.

[34] B. Biggio, I. Corona, G. Fumera, G. Giacinto, and F. Roli, "Bagging Classifiers for Fighting Poisoning Attacks in Adversarial Environments," Proc. 10th Int'l Workshop Multiple Classifier Systems, pp. 350-359, 2011.

[35] B. Biggio, G. Fumera, F. Roli, and and L. Didaci, "Poisoning Adaptive Biometric Systems," Proc. Joint IAPR Int'l Conf. Structural, Syntactic, and Statistical Pattern Recognition, pp. 417-425, 2012.

[36] B. Biggio, B. Nelson, and P. Laskov, "Poisoning Attacks against Support Vector Machines," Proc. 29th Int'l Conf. Machine Learning, 2012.

[37] M. Kearns and M. Li, "Learning in the Presence of Malicious Errors," SIAM J. Computing, vol. 22, no. 4, pp. 807-837, 1993.

[38] A.A. C_ardenas, J.S. Baras, and K. Seamon, "A Framework for the Evaluation of Intrusion Detection Systems," Proc. IEEE Symp. Security and Privacy, pp. 63-77, 2006.

[39] B. Biggio, G. Fumera, and F. Roli, "Multiple Classifier Systems for Adversarial Classification Tasks," Proc. Eighth Int'l Workshop Multiple Classifier Systems, pp. 132-141, 2009.

[40] M. Br€uckner, C. Kanzow, and T. Scheffer, "Static Prediction Games for Adversarial Learning Problems," J. Machine Learning Research, vol. 13, pp. 2617-2654, 2012.

[41] A. Adler, "Vulnerabilities in Biometric Encryption Systems," Proc. Fifth Int'l Conf. Audio- and Video-Based Biometric Person Authentication, pp. 1100-1109, 2005.

[42] B. Efron and R.J. Tibshirani, An Introduction to the Bootstrap. Chapman & Hall, 1993.

[43] H. Drucker, D. Wu, and V.N. Vapnik, "Support Vector Machines for Spam Categorization," IEEE

Trans. Neural Networks, vol. 10, no. 5, pp. 1048-1054, Sept. 1999.

[44] F. Sebastiani, “Machine Learning in Automated Text Categorization,” ACM Computing Surveys, vol. 34, pp. 1-47, 2002.

[45] C.-C. Chang, C.-J. Lin, “LibSVM: A Library for Support Vector Machines,” http://www.csie.ntu.edu.tw/~cjlin/libsvm/, 2001.

[46] K. Nandakumar, Y. Chen, S.C. Dass, and A. Jain, “Likelihood Ratio-Based Biometric Score Fusion,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 30, no. 2, pp. 342-347, Feb. 2008.

[47] B. Biggio, Z. Akhtar, G. Fumera, G. Marcialis, and F. Roli, “Robustness of Multi-Modal Biometric Verification Systems under Realistic Spoofing Attacks,” Proc. Int’l Joint Conf. Biometrics, pp. 1-6, 2011.

[48] B. Biggio, Z. Akhtar, G. Fumera, G.L. Marcialis, and F. Roli, “Security Evaluation of Biometric Authentication Systems under Real Spoofing Attacks,” IET Biometrics, vol. 1, no. 1, pp. 11-24, 2012.

[49] K. Wang and S.J. Stolfo, “Anomalous Payload-Based Network Intrusion Detection,” Proc. Seventh Symp. Recent Advances in Intrusion Detection (RAID), pp. 203-222, 2004.

[50] B. Sch€olkopf, A.J. Smola, R.C. Williamson, and P.L. Bartlett, “New Support Vector Algorithms,” Neural Computation, vol. 12, no. 5, pp. 1207-1245, 2000.

[51] K. Ingham and H. Inoue, “Comparing Anomaly Detection Techniques for http,” Proc. 10th Int’l Conf. Recent Advances in Intrusion Detection, pp. 42-62, 2007.

[52] D. Sculley, G. Wachman, and C.E. Brodley, “Spam Filtering Using Inexact String Matching in Explicit Feature Space with on-Line Linear Classifiers,” Proc. 15th Text Retrieval Conf., 2006.

[53] Encyclopedia of Biometrics, S.Z. Li, and A.K. Jain, eds., Springer US, 2009.

[54] B. Biggio, G. Fumera, and F. Roli, “Adversarial Pattern Classification Using Multiple Classifiers and Randomisation,” Proc. Joint IAPR Int’l Workshop Structural, Syntactic, and Statistical Pattern Recognition, pp. 500-509, 2008.

Author’s Details:

Jadi Vasantha
Assistant Professor, Department of CSE,
VIF College of Engineering and Technology.