Survey on Security Enhancement at the Design Phase

S.P.Mohana Priya[1], S.Pothumani[2]

Dept of CSE, Bharath University, 173, Agaram Road, Selaiyur, Chennai, India[1,2]

Abstract **-** Pattern classification is a branch of machine learning that focuses on recognition of patterns and regularities in data. In adversarial applications like biometric authentication, spam filtering, network intrusion detection the pattern classification systems are used [6]. In this paper, we have to evaluate the security pattern by classifications based on the files uploaded by the users. We have also proposed the method of spam filtering to prevent the attack of the files from other users. We evaluate our approach for security task of uploading word files and pdf files.

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

*****

I. INTRODUCTION

Machine learning is mainly used in security sensitive applications such as spam filtering and malware detection. These applications differ from classical machine learning setting to underlying the data distribution. In security applications samples can be actively manipulated by an intelligent adaptive learning to avoid detection and spam. This has led to an arms race between the designers of learning systems and adversaries evident by increasing complexity of modern attacks. For these reasons classical performance evaluation techniques are not suitable of learning algorithms. To better understand the security properties of machine learning systems in adversarial settings, paradigms from security engineering and cryptography have been adapted to the machine learning field [2, 5]. Following common security protocols, the learning system designer should use proactive protection mechanisms that anticipate and prevent the adversarial impact. This requires

(i) Finding potential vulnerabilities of learning before they are exploited by the adversary;
(ii) investigating the impact of the corresponding attacks (i.e., evaluating classier security); and
(iii) devising appropriate countermeasures if an attack is found to signicantly degrade the classier's performance.

Machine learning is used to prevent illegal or unsanctioned activity which is created from adversary. Machine learning is used in security related tasks involving classification, such as intrusion detection systems, spam filters, biometric authentication. Measuring the security performance of these classifiers is an essential part for facilitating decision making.

Evasion attacks are the most prevalent type of attack that may be encountered in adversarial settings during system operation. For instance, spammers and hackers often attempt to evade detection by obfuscating the content of spam emails and malware code. In the evasion setting, malicious samples are modified at test time to evade detection; that is, to be misclassified as legitimate. No influence over the training data is assumed. A clear example of evasion is image-based spam in which the spam content is embedded within an attached image to evade the textual analysis performed by anti-spam filters. Another example of evasion is given by spoofing attacks against biometric verification systems.

Machine learning algorithms are often re-trained on data collected during operation to adapt to changes in the underlying data distribution. For instance, intrusion detection systems (IDSs) are often re-trained on a set of samples collected during network operation. Within this scenario, an attacker may poison the training data by injecting carefully designed samples to eventually compromise the whole learning process. Poisoning may thus be regarded as an adversarial contamination of the training data. Examples of poisoning attacks against machine learning algorithms (including learning in the presence of worst-case adversarial label flips in the training data) can be found

II. RELATED WORK

Generation of training and test data sets from gathered data is an important task in developing a classifier with high generation ability. The investigation of Machine Learning paradigms for detecting attacks against networked computers was a response to the weaknesses of attack signatures. As a matter of fact, signatures usually capture just some characteristics of the attack, thus leaving room for the attacker to produce the same effects by applying slight variations in the way the attack is crafted. The generalization capability of machine learning algorithms has encouraged many researchers to investigate the possibility of detecting variations of known attacks. While machine learning succeeded in achieving this goal in a number of security scenarios, it was also a source of large volumes of false alarms. We learned that to attain the trade-off between detection rate and false alarm rate was not only a matter of the selection of the learning paradigm, but it was largely dependent on the problem statement.

Pattern recognition systems are increasingly being used in adversarial environments like biometric authentication and spam filtering tasks, in which data can be manipulated by humans to understand the outcomes of the automatic analysis. Current pattern recognition design methods do not explicit the intrinsic of these problems. This may be limiting their widespread adoption as potentially useful tools in many applications. If for instance, a more secure biometric of high quality gives a low match score and a less secure biometric gives a high match score, then there is a high likelihood of a spoof attack. It is commonly understood that one of the strengths of a multimodal system is in its ability to accommodate for noisy sensor data in an individual modality. In contrast, a more secure algorithm, in order to address the issue of a spoof attack on a partial subset of the biometric modalities, must require adequate performance in all modalities. This type of algorithm would invariably negate, to some extent, the contribution of a multimodal system to performance in the presence of noisy sensor data. A multimodal system improves the performance aspect but increases the security only slightly since it is still vulnerable to partial spoof attacks. Enhanced fusion methods, which utilize approaches to improve security, will again suffer decreased performance when presented with noisy Data

III. COMPARATIVE STUDY

In this section analyzed the various research works on several parameters and presented their comparison in the table below.

Table 1. COMPARISON OF VARIOUS RESEARCH WORKS

S.NO	TITLE	AUTHOR	ISSUE	METHOD USED	TOOLS	ADVANTAGE & DISADVANTAGE
1.	Robustness of multimodal biometric fusion methods against spoof attacks	Ricardo N. Rodrigues, Lee Luan Ling, Venu Govindaraju	In order to take full advantage of the multimodal approach, it is essential to implement a good method for fusing different sources of biometric information. .	Fuzzy logic fusion scheme for sake of simplicity, we describe the fusion schemes for combining two biometric systems (M¼2) and indicate what should be modified for the case of an arbitrary number of biometric systems	gamma distributio n to model the genuine and impostor distributio n	**Advantages:** 1) the weighted sum and LLR fusion methods have the overall best results. 2) The LLR fusion had the overall best result. The methods that use the sample quality score had a smaller increase in the FRR. **Disadvantages:** Many fusion methods have being recently proposed, being that all them show that multimodal biometric systems can significantly increase the recognition rates when compared to unimodal biometric systems.
2.	On Attacking Statistical Spam Filters	Gregory L. Wittel and S.Felix Wu	The efforts of Anti-spammers and spammers has often been described as arms race. As we devise new ways to Stem the flood of Bulk mail,	Attack Methodology A major advantage filter developers have over spammers Is that most of the content resulting from evasion methods are unique to spam	Tokenizati on With this attack, the Spammer is working Against the feature Selection (tokenizati on) of a message by	**Advantage:** While the categorization method between statistical filters, their basic functionality is similar. The basic model is often known as the bag of words (multinomial) or multivariate model. **Disadvantage:** As the volume of

			spammers respond by working their Way around the new mechanisms		splitting or modifying key message features	unsolicited bulk e-mail increases, it is becoming increasingly important to apply techniques that mitigate the cost of spam. With the increasing popularity of anti-spam measures, spammers have been forced to new ways to ensure delivery of their messages .
3.	Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters	P. A. Johnson, B. Tan, 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. .	Partial Spoof Assessment Framework	Score Normalization, Fusion, Assessment	**Advantage:** The key to creating a secure multimodal biometric system is in how the information from the different modalities is fused to make a final decision. . **Disadvantage:** The problem with any human trait that meets these criteria is in the performance, acceptability, and circumvention of the biometric trait .
4.	Good Word Attacks on Statistical Spam Filters	Daniel Lowd, Christopher Meek	Unsolicited commercial email is a significant problem for users and providers of email services.	Statistical Spam Filters	Filter Training	**Advantage:** 1) In passive attacks, the attacker constructs a word list without any feedback from the spam filter. 2) Attacks of this type amount to educated guesses regarding which words are "good" and which are "bad." **Disadvantage:** Unfortunately, most empirical evaluations of spam filters ignore this adversarial problem.
5.	Machine Learning in Adversarial Environments	Pavel Laskov, Richard Lippmann	Whenever machine learning is used to prevent	The articles selected for this special issue reflect the diversity of	Machine learning algorithms	**Advantage:** 1) The theoretical foundations of machine learning are largely built on the assumption that

			illegal or unsanctioned activity and there is an economic incentive, adversaries will attempt to circumvent the protection provided.	scientific methodology in the various application domains of adversarial learning		training data adequately describes the underlying phenomena addressed by learning. 2) Protection against adversarial data may seem to be a "mission impossible". Indeed, an unconstrained adversary who can arbitrarily alter data and labels can induce an error rate of up to 100%. **Disadvantage:** A classical example is spam filtering where spammers tailor messages to avoid the most recent spam detection techniques.
6	The security of machine learning	Marco Barreno· Blaine Nelson· Anthony D. Joseph· J.D. Tygar	Machine learning's ability to rapidly evolve to changing and complex situations has helped it become a fundamental tool for computer security	SECURITY VIOLATION Integrity attacks compromise assets via false negatives	Causative Integrity attack: The spam foretold	**Advantage** Machine learning advocates have proposed learning-based systems for a variety of security applications, including spam detection and network intrusion detection. **Disadvantage** If we hope to use machine learning as a general tool for computer applications, it is incumbent on us to investigate how well machine learning performs under adversarial conditions.
7	Polymorphic Blending Attacks	Prahlad Fogla Monirul Sharif RobertoPerdisci Oleg Kolesnikov WenkeLee	A very effective means to evade signature-based intrusion detection systems (IDS) is to employ polymorphic	PAYL, a byte frequency-based anomaly IDS	frequency -based network anomaly IDS	**Advantage** Defenses against polymorphism Looking for instruction semantics, detect known code transformations **Disadvantage** For 1-gram blending greedy algorithms are proposed that generate small padding and can closely match the

			techniques to generate attack instances that do not share a fixed signature.			target byte frequency
8	A survey and experimental evaluation of image spam filtering techniques	Battista Biggio, Giorgio Fumera, Ignazio Pillai and Fabio Roli	In their arms race against developers of spam filters, spammers have recently introduced the image spam trick to make the analysis of emails' body text ine ective	Image spam detection techniques	spam filtering and image spam	**Disadvantage** content-based filtering of multimedia documents is a problem of great relevance, given the already huge and yet increasing amount of multimedia contents available on the Internet, **Advantage** We propose a categorisation of these techniques and discuss their potential advantages
9	Security Evaluation of Biometric Authenticati on Systems Under Real Spoofing Attacks	Battista Biggio, Zahid Akhtar, Giorgio Fumera, Gian Luca Marcialis, and Fabio Roli	Multimodal biometric systems are commonly believed to be more robust to spoofing attacks than unimodal sys-tems, as they combine information coming from different biometric traits.	Spoofing attacks, Fingerprint spoofing	Face spoofing	**Advantage** we focus on biometric identity verification. In this kind of task, the user claims the identity of an enrolled client, and provides his biometric traits to the system **Disadvantage** potential vulnerabilities of biometric systems and related attacks have been detected. Some works have revealed that not only individual modules of a biometric system can be attacked, but also the channel connecting them
10	Support Vector Machine Active Learning with Applications to Text Classificatio n	Simon Tong, Daphne Koller	Support vector machines have met with significant success in numerous real-world learning tasks.	Email filtering. The user wishes to create a personalized automatic junk email filtering	Support Vector Machines	**Disadvantage** In many supervised learning tasks, labeling instances to create a training set is time consuming and costly **Advantage** Here, the learner can actively choose the training data.

 ISSN: 2321-8169
1582 - 1588

						It is hoped that allowing the learner this extra flexibility will reduce the learner's need for large quantities of labeled data

IV. FUTURE WORK

Attacks against pattern recognition systems emerged only recently as the application and popularity of these technologies generated sufficient incentives for attackers. Nowadays, we have many reported attacks against biometric recognition systems based on fake biometric traits, e.g., a printed picture is used to fool a facial recognition system. Besides face and fingerprint recognition, the European project TABULA RASA demonstrated successful attacks against systems using speech and gait. Therefore, additional biometric systems could be the next targets soon. Another little-known type of attack likely to emerge in the near future is an evasion attack against biometric video surveillance systems used to recognize targeted individuals (e.g., individuals on a watch-list). To date this avenue of attack has received little attention because evading a face recognition system is still quite easy (wearing hats or glasses is often sufficient to evade it). However, the arms race to evade these pattern recognition systems has already begun as is evident in the creative CV Dazzle project that proposes new facial makeup and hair styling to evade face recognition systems.

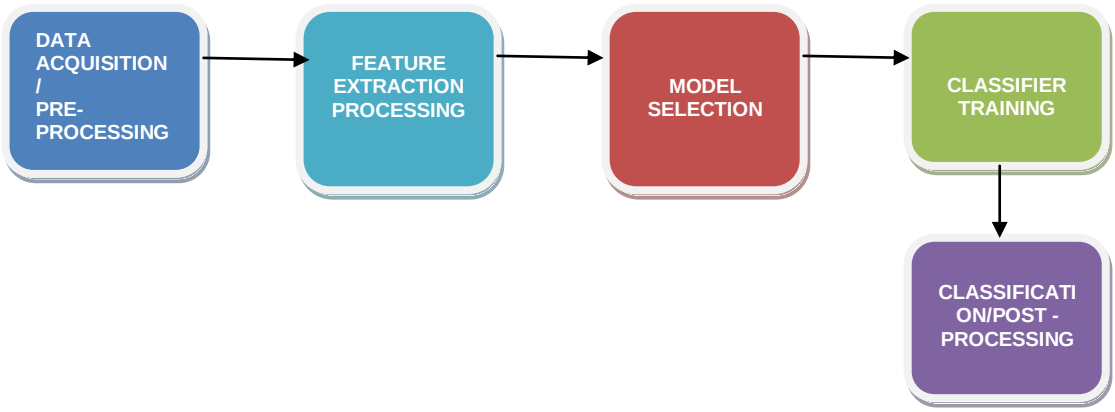

Fig. 1 Emergence of areas in evaluation of pattern classifiers

V. CONCLUSION

In this paper we pointed out some of the issues related to the adoption of pattern recognition systems in security-sensitive settings, and advocated a proactive approach to security evaluation that can be exploited complementarily to the well-known reactive paradigm to understand their security guarantees. Thinking proactively, we also discussed some novel potential sources of vulnerabilities, such as data clustering algorithms. For the same reason, one may also think of attackers that combine carefully crafted attacks against specific system components (e.g., data clustering, feature selection, and classier training) to develop more complex, stealthy attacks.

REFERENCES

[1] Attar, A., Rad, R.M., Atani, R.E.: A survey of image spamming and filtering techniques. Artif. Intell. Rev. 40(1), 71{105 (2013)
[2] Barreno, M., Nelson, B., Sears, R., Joseph, A.D., Tygar, J.D.: Can machine learning be secure? In: Proc. of the 2006 ACM Symp. on Information, Computer and Comm.Sec. pp. 16{25. ACM, NY, USA (2006)
[3] Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G.L., Roli, F.: Security evaluation of biometric authentication systems under real spoofing attacks. IET Biometrics 1(1), 11{24 (2012)

[4] Biggio, B., Didaci, L., Fumera, G., Roli, F.: Poisoning attacks to compromise face templates. In: 6th IAPR Int'l Conf. on Biometrics. pp. 1{7. (2013)
[5] Biggio, B., Fumera, G., Pillai, I., Roli, F.: A survey and experimental evaluation of image spam filtering techniques. Pattern Rec. Letters 32(10), 1436 {1446 (2011)
[6] Biggio, B., Fumera, G., Roli, F.: Security evaluation of pattern classiers under attack. IEEE Trans. on Knowledge and Data Engineering 99(PrePrints), 1 (2013)
[7] D. Lowd and C. Meek, "Good Word Attacks on Statistical Spam Filters," Proc. Second Conf. Email and Anti-Spam, 2005
[8] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee,"Polymorphic Blending Attacks," Proc. 15th Conf. USENIX Security Symp., 2006
[9] P. Johnson, B. Tan, and S. Schuckers, "Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters," Proc. IEEE Int'l Workshop Information Forensics
[10] and Security, pp. 1-5, 2010
[11] 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

BIOGRAPHY

S P Mohana Priya pursuing M.Tech Computer Science and Engineering at Bharath University, received the B.E degree in Computer Science & Engineering from Info Institute Of Engineering, Coimbatore in 2011. She participated in workshops on Android and she has presented the paper in National conference in Bharath University

S Pothumani is working as an Assistant professor in the Department of CSE at Bharath University from 2011. She has 3 years of experience in teaching.