ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

# Collaborative Attack Detection Using KID System

Vishakha V. Kharche[1], Prof. Virendra P. Nikam[2], Prof. Yogesh B. Jadhao[3]

P.G. Student, Department of Computer Engineering, VBKCOE Malkapur, Maharashtra, India[1]

Assistant Professor, Department of Computer Science and Engineering, Dr.Sau. K.G.I.E.T. Darapur, Maharashtra, India[2]

Assistant Professor, Department of Computer Engineering, VBKCOE Malkapur, Maharashtra, India[3]

**ABSTRACT**:In recent era the use of internet become more. Most of people used internet to transfer their data and used cloud to save that data. There is chance that the data may get scythe and misused by some unauthorized user. So to prevent from such unauthorized users various Anomaly intrusion detection schemes are introduced recently. To fight against such attacks Keyed Intrusion Detection System is used. Since most current network attacks happen at the application layer, analysis of packet payload is necessary for their detection. KIDS core idea is to make defense against evasion attacks. Proposed system provides security from such attacks and also protects stored data. Proposed system used to save data of various domains in cloud. By adding mystery component in to plan so that a couple of operations are becomes impractical without knowing the key. For each implementation of the methodKey is different and is set aside secret. KIDS observe all activity and inform to authorize node about unusual activity.

**KEYWORDS**: Anomaly detection, intrusion detection systems, Adversarial classification, machine-learning.

## I. INTRODUCTION

Day by day many computer security problems can be mostly reduced to separating malicious from non-malicious activities. The case of spam filtering, intrusion detection or the identification of fraudulent behaviour is the example. But defining accurately and estimating useful way that is what is dangerous or what is not dangerous is many time too complex. To overcome these difficulties, machine-learning approach is use as the solution to such problems notably through the use of classifiers to automatically derive models of behaviour which are later used to recognize the occurrence of potentially anonymous events.Anomaly detection systems are of two types Network Intrusion Detection System and Host based Intrusion Detection System.NIDS mainly related to network and it monitors the network activity for multiple machines.HIDS monitor single host.KIDS is an application layer network anomaly detection system. Core idea of KIDS is to make defence against evasion attacks [7].Proposed system provides security from such attacks and also protects stored data.

Recent work has precisely pointed out that security problems are different from other application domains of machine learning in, one fundamental feature that is the occurrence of an enemy who can strategically fight against the algorithm to accomplish his goals. For example, major aim for the attacker is to avoid his detection. Evasion attacks feat weaknesses in the fundamental classifiers, which are often unable to detect a malicious sample that has been appropriately altered so as to look normal. For instance, spammers regularly obfuscate their emails in various ways to avoid detection e.g., by changing words that are normally present in spam or by including a large number of words that do not [12], [13]. Similarly, to avoid intrusion detection systems (IDS) without compromising the functionality of the attack malware and other pieces of attack code can be carefully adapted [6], [14]. A few detection schemes proposed over the last few is not entirely new, Wang et al. introduced in Anagram, another payload-based anomaly detection system that addresses the evasion problem in quite a similar manner [15].A KIDS is an application-layer network abnormality detection system that extracts a number of words from each payload. After that the system builds a model of normality which is based on both the frequency of observed features and their qualified positions in the payload [1].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

For better network security Anomaly detection system is used which observe activity and inform to themain station about unusual activity to take action. In anomaly detection system if attacker knows the rules then they create new set of rules to attack on the system.In Key intrusion detection system secret key is require to know behavior of model. In KIDS one issue is that attacker gets thekey after interaction with the system so improvement in KIDS is needed. With Improvement in Key intrusion detection system provides better security from suchattacks. Data is stored in encrypted format in KIDS system and keys are known only to authorize user to make sure confidentiality of the data. If any attack occurs then it prevent attacker and inform to authorize node about unusual activity.

## II. LITERATURE SURVEY

Barreno Blaine Nelson Russell Sears Anthony saidmachine learning systems suggest unparallel flexibility in dealing with developing input in a multiple applications such as intrusion detection systems and spam e-mail filtering. Malicious opponent always made target on Machine learning algorithms. This paper provides a framework for answering the question, “Can machine learning be secure?” This paper includes taxonomy of different types of attacks on machine learning techniques and systems and multiple defences against those attacks. An analytical model gave a lower bound on attacker’s work function, and a list of open problem [2].

Marco Barreno, Blaine Nelson, Anthony D. Joseph.Saidmachine learning’s ability quickly evolves to changing and a complex situation has helped it to become a elementary tool for computer security. That adaptability is also vulnerability that is attackers can exploit machine learning systems. They present a taxonomy identifying and analyzing attacks against machine learning systems. They show how these classes influence the costs for the attacker and defender, and they give a formal structure defining their interaction. They use their framework to survey and analyse the literature of attacks against machine learning systems. They also explain their taxonomy by presenting how it can guide attacks against SpamBayes, a popular statistical spam filter. Finally, they discuss how their taxonomy suggests new lines of defences [3].

Battista Biggio, Giorgio Fumera, and Fabio Rolisaidin many security applications an adversarial classification problem is face by pattern recognition system, in which an intelligent, adaptive enemy modifies patterns to avoid the classifier. Several strategies have been recently proposed to make a classifier harder to avoid, but they are based only on qualitative and intuitive arguments.They consider a strategy which made of hiding information about the classifier to the enemy through the beginning of some randomness in the decision functionin Adversarial Pattern Classificationwhich use Multiple Classifiers and Randomization, They focus on an implementation of this approach in a multiple classifier system is a classification architecture which is broadly used in security applications. Author suggest support to this strategy, based on an analytical framework for adversarial classification problems which are proposed recently by other authors, and give an experimental evaluation on a spam filtering task to demonstrate their findings [4].

B. Biggio, B. Nelson, and P. Laskovsaid malicious adversaries may manipulate data in adversarial classification tasks such as spam filtering and intrusion detection to prevent the outcome of an automatic analysis. Thus as well achieving high quality classification performances then the machine learning algorithms have to be robust against adversarial data manipulation to successfully operate in these tasks.In classification problems tremendously attractive approach are Support vector machines and their usefulness in adversarial classification tasks has not been broadly investigated yet. In this paper they present a preliminary investigation of the robustness of SVMs against adversarial data manipulation. In particular, they assume that the enemy has control over some training data, and aims to subvert the SVM learning process. Within this assu3mption, they show that this is indeed possible, and propose a strategy to improve the robustness of SVMs to training data manipulation based on a simple kernel matrix correction [6]

P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee said a very effective way to evade signature-based intrusion detection systems (IDS) is to use polymorphic techniques to generate attack instances that do not share a fixed signature. Anomaly-based intrusion detection systems suggestsuperb defence because existing polymorphic techniques can make the attack instances look unlike from each other, but cannot make them same like normal. In this paper a new class of polymorphic attacks is introduce which is called polymorphic blending attacks. It can efficiently avoid byte frequency-based network anomaly IDS by watchfully matching the statistics of the mutated attack instances to the normal profiles. The proposed polymorphic blending attacks can beconsideras a subclass of the mimicry attacks. They take a systematic approach to the problem and formally describe the algorithms and steps required to carry out such attacks. They not only show that such attacks are feasible but also analyse the hardness of evasion under different

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

circumstances. They present complete techniques using PAYL, a byte frequency-based anomaly IDS, as a case study and demonstrate that these attacks are indeed feasible. They also provide some insight into possible countermeasures that can be used as defence [5].

A classifier is ACRE learnable if there is an algorithm that finds a minimum cost instance which avoid detection using just polynomially many queries. Similarly a classifier is also ACRE k-learnable if the cost is not minimum but bounded by k. Then it is proved that linear classifiers with unbroken features are ACRE k-learnable under linear cost functions [9]. Therefore, these classifiers should not be used in adversarial environments. Consequent work by Nelson in [10], [11] generalizes these results to convex-inducing classifiers, viewing that it is normally not required to reverse engineer the decision boundary to construct undetected instances of near minimum cost. In general, some extra works have revisited the task of machine learning in security applications, with exacting prominence on anomaly detection [8], [16], [17], [18].

## III. PROPOSED SYSTEM

Assaults are to aimmense degree proficient, signifying that it is prudently simple for an attacker to recover the key in any of the two settings examined. We belief that such an lack of security reveal that plans like KIDS were just not intended to anticipate key-recovery assaults. Then again, in this paper we have contended that battle against such assaults is key to any classifier that strivesto hinder avoidance by depending on a mystery bit of data. We have given barter on this and other open exploration in the belief of empowering further research around there. The assaults here displayed could be prevented by giving various unplanned counter measures the structure, for example, constricting the most intense length of words and payloads or counting such amounts as order components.Thenthis alterationmay in any case be ineffective against different assaults. We are using Advanced Encryption Standardalgorithm technique for encryption and decryption of file and MD5 algorithm for key generation.Detecting hacker and blocking his profile so that hacker will not affect another user security.

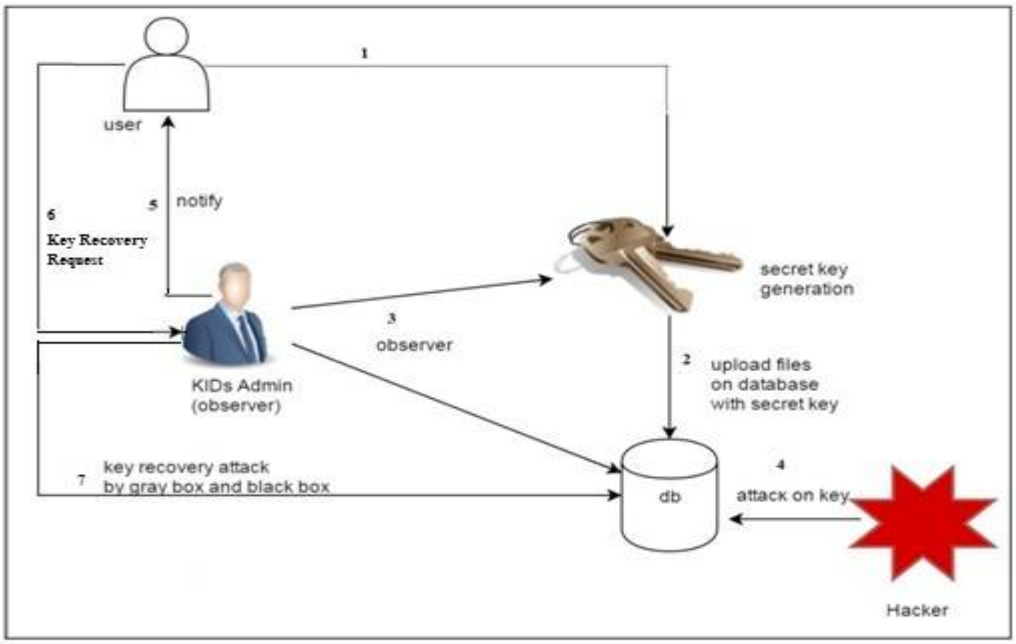


Fig. 1 System Architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

***ALGORITHM:***

***A. AES***

AES is the Advanced Encryption Standard algorithm. This algorithm is used for encryption & decryption of data/files. Given 128 bit plaintext and 256 bit key is used then there are fourteen rounds of following four steps. Following are the steps used in AES algorithm

**1)SubBytes**

The 16 byte as input are substituted by usingS-box

**2) Shiftrows**

Each row of the matrix is shifted to the left.

**3)MixColumns**

Mixing the data within each column of the State array

**4) Adding a Round Key to the State**

128 bits of matrix are XORed with the round key which is 256 bit key.

If this is the final round then the output is the ciphertext.Else the resultant 128 bits areused as 16 bytes and we begin another similar round.

The Cipher transformations can be inverted and then executed in reverse order to produce plaintext byusing the AES algorithm. The individual transformations used in the InverseCipher.

**1)Inverse Sub Bytes**

**2) Inverse Shift Rows**

**3) Inverse Mix Columns**

**4) Add Round Key**

The AES inverse cipher core consists of a key expansion module, a key reversal buffer, an initial permutationmodule, a round permutation module and a final permutation module. The key reversal buffer first accumulate keysfor all rounds and the used them in reverse order to the rounds. The round permutation module will loopmaternally to perform 14 iterations.

***B. MD5***

The MD5 algorithm is a widely used hash function producing a 128-bit hash value.

MD5 algorithm takes input message of arbitrary length and generates 128-bit long output hash. MD5 hash algorithmconsist of 5 steps:

**Step 1.** Append Padding Bits

**Step 2.** Append Length

**Step 3.**InitializeMD Buffer

**Step 4.**Process Message in 16-Word Blocks

**Step 5.** Output

## IV. RESULT AND DISCUSSION

Plotted graph shows that in proposed system time require for key recovery is less than time require for key recovery in existing system. And propose system also provide more security, prevention and confidentiality than existing system.

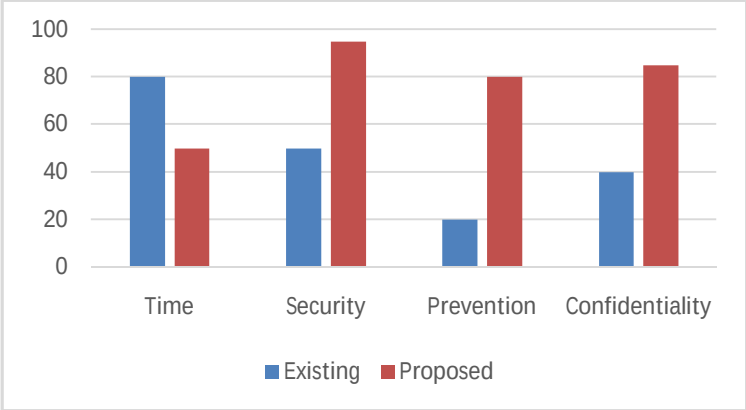


Fig. 2: Result analysis

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Following table shows comparison between existing system and propose system in terms of time, security, prevention and Confidentiality.

| | Existing | Proposed |
|---|---|---|
| **Time** | 80 | 50 |
| **Security** | 50 | 95 |
| **Prevention** | 20 | 80 |
| **Confidentiality** | 40 | 85 |

Table-1: Experimental Result

## V. CONCLUSION

Privacy in data is most important because of sensitive information may have harm full effect on someone's life, so it is most important to provide security and privacy to our sensitive information. The system will improve the security and confidentiality of stored data over cloud and Intranet. The new propose technique offers a better KIDS System which works against the grey/black box attacks. Also to increase Security complexity system saves user data in encrypted format and takes the prevention steps against unauthorized user.

## REFERENCES

[1] Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos, "Key-Recovery Attacks on KIDS, a Keyed Anomaly Detection System,"IEEETransactionsOn Dependable And Secure Computing, Vol. 12, No. 3, May/June 2015
[2] 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 '06 ), pp. 16-25, 2006.
[3] M. Barreno, B. Nelson, A.D. Joseph, and J.D. Tygar, "The Security of Machine Learning," Machine Learning, Vol. 81, no. 2, pp. 121- 148, 2010.
[4] B. Biggio,G. Fumera, and F. Roli, "Adversarial Pattern Classification Using Multiple Classifiers and Randomisation," Proc. IAPR Int'l Workshop Structural, Syntactic, and Statistical Pattern Recognition, Lecture Notes in Computer Science, Vol 5342., pp. 500-509, 2008.
[5] B. Biggio, B. Nelson, and P. Laskov, "Support Vector Machines Under Adversarial Label Noise," J. Machine Learning Research, Vol. 20, pp. 97-112, 2011.
[6] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee, "Polymorphic Blending Attacks," Proc. 15th Conf. USENIX Security Symp., Vol. 15, 2006.
[7] SasaMrdovic, BranislavaDrazenovic" KIDS – Keyed Intrusion Detection System" Proc. Seventh Int'l Conf. Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA '10), Lecture Notes in Computer Science, Vol 6201, pp. 173-182, 2010.
[8] C. Gates and C. Taylo, "Challenging the Anomaly Detection Paradigm: A Provocative Discussion," Proc. New Security Paradigms Workshop (NSPW), pp. 21-29, 2006.
[9] D. Lowd and C. Meek, "Adversarial Learning," Proc. 11th ACM SIGKDD Int'l Conf. Knowledge Discovery in Data Mining (KDD '05), pp. 641-647, 2005.
[10] B. Nelson, A.D. Joseph, S.J. Lee, and S. Rao, "Near-Optimal Evasion of Convex-Inducing Classifiers,"J. Machine Learning Research, Vol. 9, pp. 549-556, 2010.
[11] B. Nelson, B.I.P. Rubinstein, L. Huang, A.D. Joseph, S.J. Lee, S. Rao, and J.D. Tygar, "Query Strategies for Evading Convex-Inducing Classifiers," J. Machine Learning Research, Vol. 13, pp. 1293-1332, May 2012.
[12] Y. Zhou, Z. Jorgensen, and M. Inge, "Combating Good Word Attacks on Statistical Spam Filters with Multiple Instance Learning," Proc. 19th IEEE Int'l Conf. Tools with Artificial Intelligence (ICTAI '07), pp. 298-305, 2007.
[13] A. Kolcz and C.H. Teo, "Feature Weighting for Improved Classifier Robustness," Proc. Sixth Conf. Email and Anti-Spam (CEAS '09), 2009.
[14] O. Kolesnikov, D. Dagon, and W. Lee, "Advanced Polymorphic Worms: Evading IDS by Blending in with Normal Traffic," Proc. USENIX Security Symp., 2005.
[15] K. Wang, J. Parekh, and S. Stolfo, "Anagram: A Content Anomaly Detector Resistant to Mimicry Attack," Proc. Ninth Int'l Conf. Recent Advances in Intrusion Detection (RAID '06), pp. 226-248, 2006.
[16] K. Rieck, "Computer Security and Machine Learning: Worst Enemies or Best Friends?" Proc. DIMVA Workshop Systems Security (SYSSEC), 2011.
[17] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," Proc. IEEE Symp. Security and Privacy, pp. 305-316, 2010.
[18] Y. Song, M. Locasto, A. Stavrou, A.D. Keromytis, and S.J. Stolfo, "On the Infeasibility of Modeling Polymorphic Shellcode: Re-Thinking the Role of Learning in Intrusion Detection Systems," Machine Learning, Vol. 81, no. 2, pp. 179-205, 2010.