Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 5, May -2017

KIDS for Key Recovery Attack

Suraj Shinde[1], Pradnya Patil[2], Shweta Yadav[3] , Sayali Yadav[4]
Prof.Sunil Yadav[5]

[1,2,3,4,5]*Computer Engineering, Siddhant College of Engineering, Pune*

Abstract — *With the anomaly detection systems, many techniques and approaches have been developed to track novel attacks on the systems. Anomaly detection systems used many algorithms and predefine rules; it's impossible to define all rules and algorithm and also once algorithm is known to attacker then new attack is created for same. To overcome this issue various machine learning schemes have been developed. One of such scheme is KIDS (Keyed Intrusion Detection System) which is depends on method used to generate KEY and secrecy of the KEY. Problem with KIDS is that attacker easily able to get key after grey box attack or black box attack. Hence improvement in KIDS system is required to provide more security with this attacks .Proposed system provides more security under both this attacks and also protect stored data. Proposed scheme can used to save data of various domains in cloud storage like for healthcare domain user can save the patient data. With the anomaly detection systems, many techniques and approaches have been developed to track novel attacks on the systems. Anomaly detection systems used many algorithms and predefine rules; it's impossible to define all rules and algorithm and also once algorithm is known to attacker then new attack is created for same. To overcome this issue various machine learning schemes have been developed. One of the such scheme is KIDS (Keyed Intrusion Detection System) which is depends on method used to generate KEY and secrecy of the KEY. Problem with KIDS is that attacker easily able to get key after grey box attack or black box attack. Hence improvement in KIDS system is required to provide more security with this attacks .Proposed system provides more security under both this attacks and also protect stored data. Proposed scheme can used to save data of various domains in cloud storage like for healthcare domain user can save the patient data.*

Keywords- *Intrusion Detection System, Anomaly detection system, Network Intrusion Detection system.*

I. INTRODUCTION

Use of internet increased tremendously. Most of the people used internet to transmit their data and used cloud to save it. There is possibility that data may get hacked and get misused. For better protection from such unauthorized Users various Anomaly intrusion detection methods are proposed. Intrusion Detection System used to monitor network activity and inform to the main station about the details. Anomaly detection system classifies the activity and inform about unusual activity. Anomaly detection system includes predefine rules and extract features of behavior of system, uses the same data and compare it with the live data. Provide that result to the main station. Anomaly detection system are having two types Network Intrusion Detection System (NIDS) and Host based Intrusion Detection System .NIDS mainly related to network and it monitor the network activity for multiple machines or servers .HIDS monitor single host or server .Keyed Intrusion Detection System(KIDS) is NIDS type system which is used to provide better security from various attacks. KIDS depends on method used to generate KEY and secrecy of the KEY. With KIDS attacker easily able to get the KEY with interacting with the KIDS system and observing the outcome. Hence improvement in KIDS system is required to provide more security from grey or black box attacks .In this paper proposed system provide more security under this attacks and also protect stored data. Proposed scheme can used to save data of various domains in cloud storage like for healthcare domain user can save the patient data.

Motivation: Now a day's more and more people are getting connected to the Internet to take advantage of internet facility like data storage in cloud and data transfer over to other internet user. Network connectivity has become critical aspect. On one side, the Internet provides potential of reaching easily to end users, at the same time risk, because of the both (harmless, harmful) users of the internet. Attackers or hackers can get access to organizations information for various reasons. Since provide more security for data is one of the important factor in the networking. For better network security Anomaly detection system is used which monitor the network activity and inform to the main station about unusual activity to take action. In case of anomaly detection system once attacker knows the rules or its set of algorithm they create new algorithm to attack on the system so for better improvement KIDS system is required. In KIDS to know behavior of model secret key is needed. Issue with KIDS is that attacker gets to know the key after interaction with the system so improvement is needed. With Improvement KIDS system provides better security from attacks. KIDS system stored data in encrypted format and keys are known only to authorize user to make sure confidentiality of the data. If any attacks happen it prevent attacker and provide information to main station about
the incident.

II. RELATED WORK

The Machine learning has been used in large area of security related tasks like network intrusion detection and spam filtering ,malware and , to identify between malicious and justify samples is serious problem, N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D.Verma. explorer the same problem in [3] so bypassing can be classified. However, these problems are specifically challenging for machine learning rules and algorithms because of the existence of intelligent and adaptive adversaries who can carefully handle the input data to demote the performance of the detection system, breaching the underlying consideration of data stationary, so that meaning is that training data or test data follow the same distribution (although typically unknown). Adversarial learning research not only been direct the problem of analyse security of commom learning Algorithms to intentionally-targeted attacks, but also that of formulate learning algorithms with upgrade security. To deal with evasion attacks, clear knowledge of different types of adversarial data handling has been included into learning algorithms, e.g., using game-theoretical. An implicit assumption at the back of traditional machine learning and pattern recognition algorithms is that training data or test data are produce from the same, possibly not known, distribution. This assumption is however similar to the violated in adversarial settings, since malicious user may intentionally manipulate the input set data to downgrade the systems performance. D. Lowd and C. Meek[4] notice that the attacker not required model the classifier explicitly ,but only observe lowest attacker instance as in the N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D.Verma setting . They develop a concept of reverse engineering the adversarial classifier reverse engineering (ACER) problem .Given an malicious user cost function ,they observe the complexity of finding a lowest attacker cost that the classifier the labels as negative. They consider no general information of the training data, though the attacker may know the property space and also must include one positive and one negative example each. A classifier is ACRE-learnable of their presence a polynomial query algorithm that detect a lowest attacker cost for negative instance. They conclude that linear classifier is learnable ACRE with linear attacker cost functions and some other Minor limitation. The ACER-learning problem gives a means of teach how challenging it is to use queries in to the reverse engineer classifier from specially hypothesis class using a special feature space.

III. PROPOSED SYSTEM

Our aim is to provide great degree expert, that it is the sensibly easy for an attacker to recoup the key in any of the settings. It is consider that the such an absence of security not protect from anticipate like children from key-recovery assaults. Here claimed the resistance against such assaults is key to any classifier that attempt to hinder avoidance by depending on a mystery bit of data. We have given exchange on this and other open enquiries in the trust of empowering further research around there. The assaults here exhibited could be the forestalled by presenting various impromptu the counter measures of the frameworks, for example, constraining the most large length of words , or including such amounts as order components. Then again, that these variations may in any case be the powerless against some individual assaults. In this manner, our suggestion for future plans is to construct choices in light of hearty standards as opposed to specific fixes. Our aim is enhance the KIDS and try to meet maximum security properties so that it can able to secure stored data in clouds for various healthcare domains. Architecture of proposed system and proposed system module Details: Node Creation & Routing: In this module, authenticated node is created for each user. KIDS system gets all details about user and stored the same for creating the rules. After node creation when user saved files, each files get saved in encrypted format. For each file user get secret Key. Key- Recovery Attacks On Kids: At this point assault can able to attack and get the knowledge about the secret key. Assault able to get user data files and used same information for various reasons . Assault changes the Key and modified the same so it will not available further more to any authenticated user. Implicitly here grey box or black box attacks happened in which secret Key partially or fully modified and then make available to end nodes. Keyed Anomaly Detection and Adversarial Models: Revisited After secret key modification KIDS system alerts to the main station and check the authentication list. If unauthenticated node found then it get blocked by KIDS system. Modified key then recoup and provided to the intended node. Performance Analysis: For performance evaluation following graph can be used Delay, Packet delivery ratio

IV. SYSTEM ARCHITECTURE

1. Node Creation and Routing:
In this module, a remote system is made. Every one of the hubs are haphazardly sent in the system region. Our system is a portable system, hubs are doled out with versatility (movement).Source and destination hubs are characterized. Information exchanged from source hub to destination hub. Since we are working in versatile system, hubs portability is set i.e., hub move starting with one position then onto the next.

2. Key- Recovery Attacks On Kids:
At the point when surveying the security of frameworks, for example, KIDS, one noteworthy issue originates from the nonappearance of broadly acknowledged antagonistic models giving an exact portrayal of the aggressor's objectives and his abilities one such model for secure machine learning and talked about different general assault classes. Our work does not fit well inside in light of the fact that our principle objective is not to assault the learning calculation itself, but rather to recoup one bit of mystery data that, in this way, may be vital to successfully dispatch an avoidance assault.

3. Keyed Anomaly Detection And Adversarial Models Revisited:

Firmly identified with the focuses talked about above is the need to set up plainly characterized and persuaded ill-disposed models for secure machine learning calculations. The suspicions made about the assailant's abilities are basic to legitimately break down the security of any plan, yet some of them may well be unlikely for some applications. One disputable issue is whether the assailant can truly get criticism from the framework for examples he picks. This bears a few analogies with Chosen-Plaintext Attacks (CPA) in cryptography. This supposition has been made by numerous works in secure mama chine learning, including our own

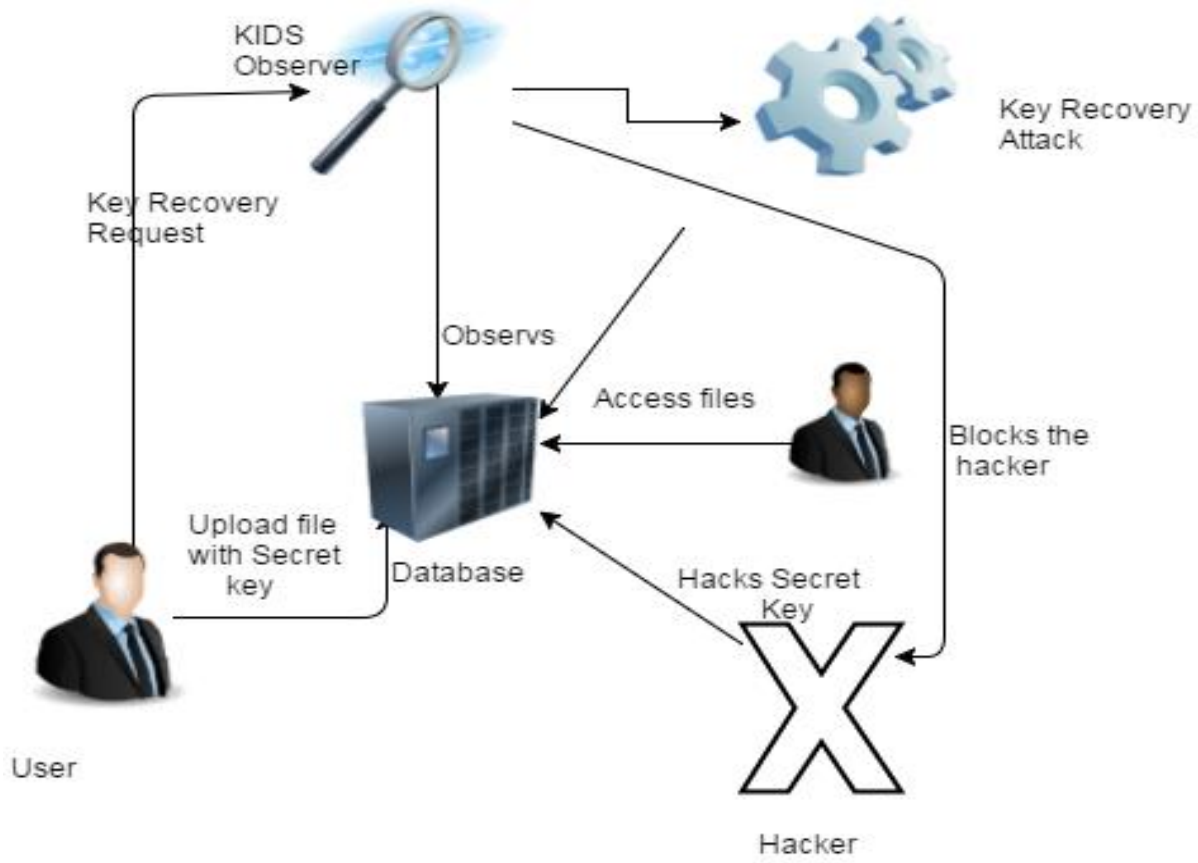


Fig.1 System Architecture

V. RELEVANT MATHEMATICS ASSOCIATED WITH THE PROJECT

Let S is the Whole System Consists:

S = U,NC,KD,KA,PA .

1. U is the set of number users. U=U1,U2Un.
2. NC is the set node created by admin. NC=NC1,NC2,..NCn.
3. KD is set of key recovery attack. KD=KD1,KD2.KDn.
4. KA is set of keyed anomaly detection. KA=KA1,KA2..KAn.
5. PA is set of performance analysis PA=PA1,PA2..PAn

Step 1: user or hacker request for data and get important information U=U1,U2Un.

Step 2: To recover information or key. We create node and use routing on it. NC=NC1,NC2,..NCn.

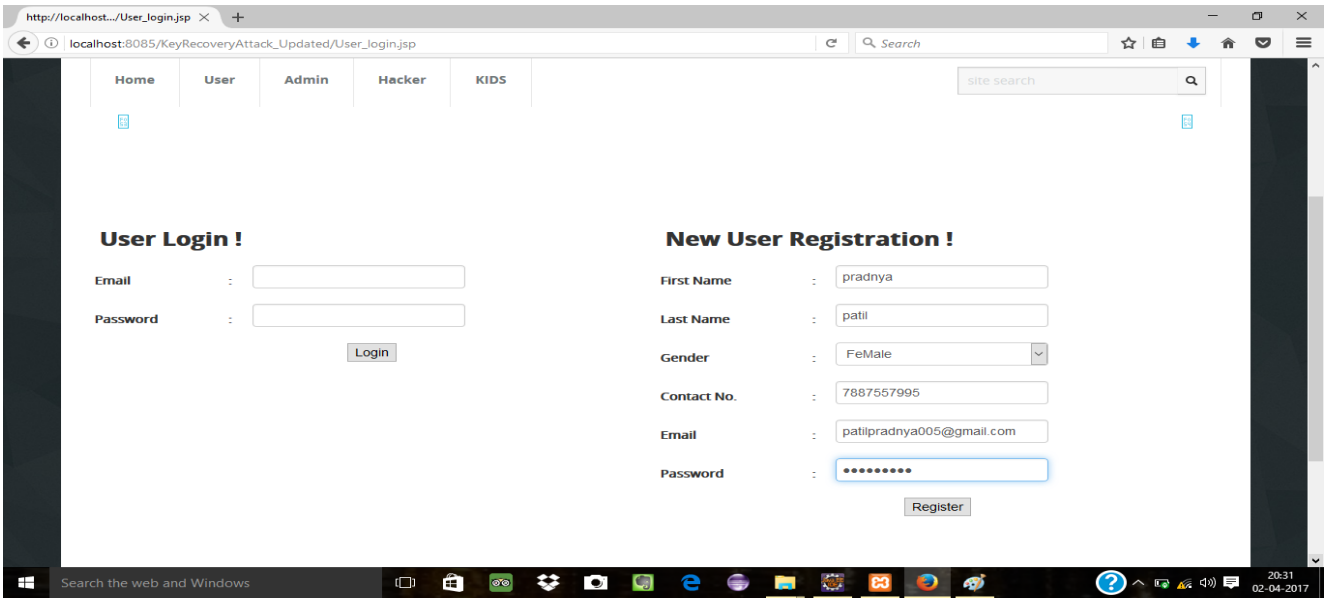
Step 3:Then key recovery attack apply on KIDS. KD=KD1,KD2.KDn.

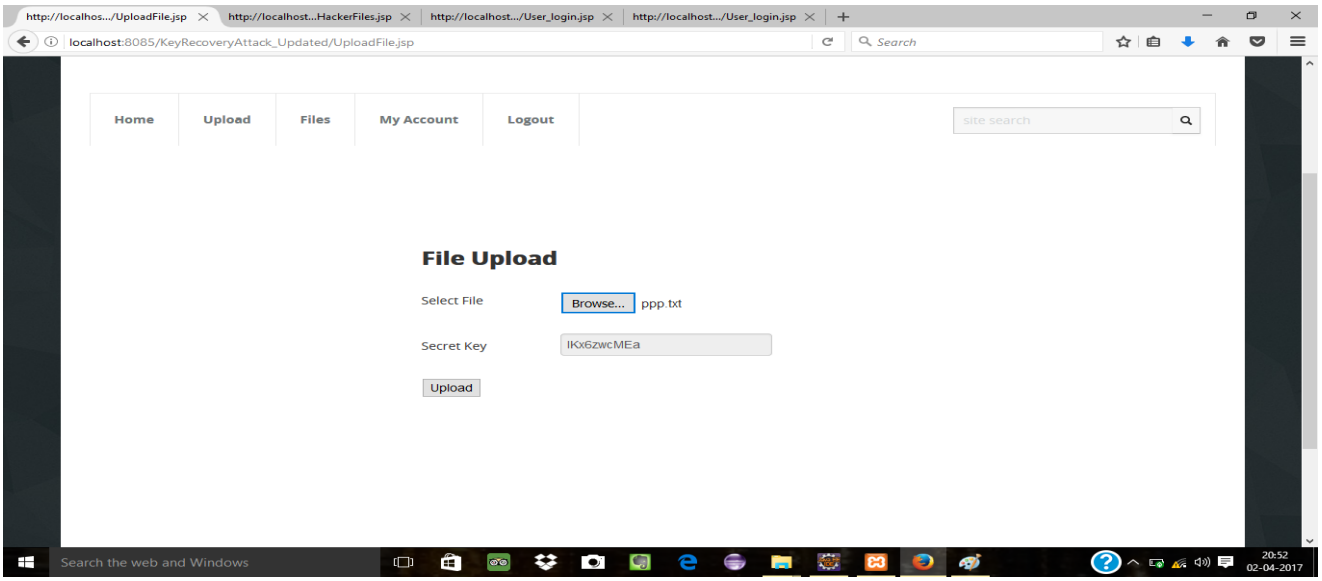
Step 4:After that key anomaly detection and adversarial model revisited KD=KD1,KD2.KDn.

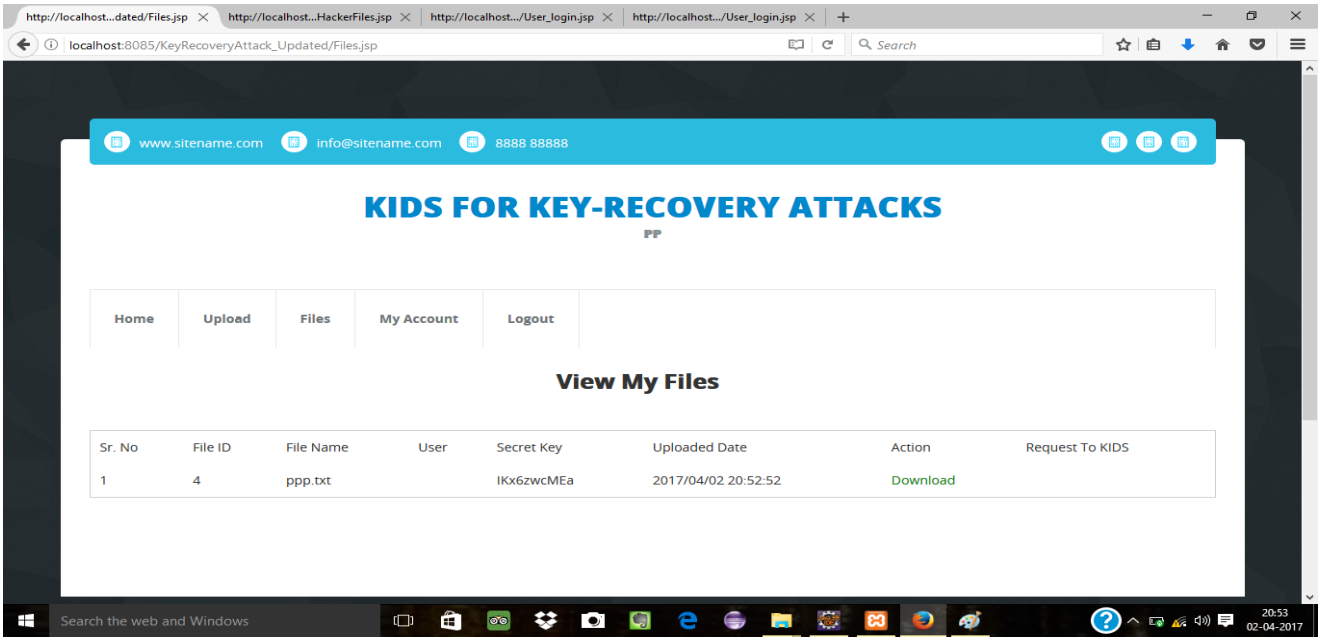
Step 5:Them performance analysis and result comparing is done. PA=PA1,PA2..PAn

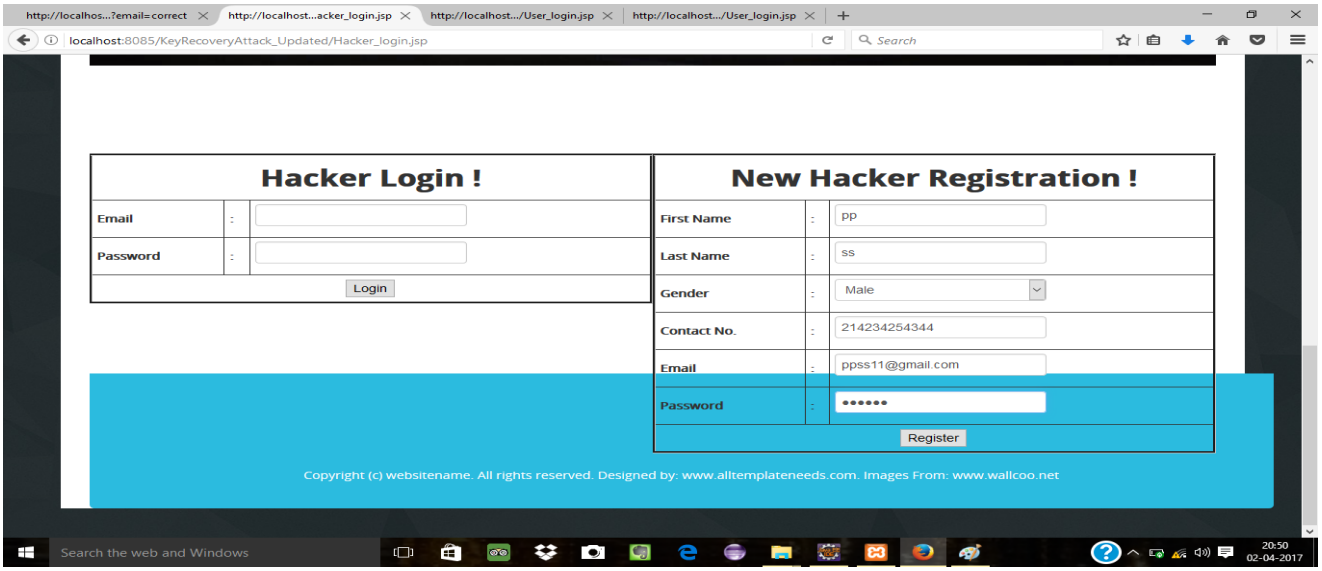
Output: we recover our key.

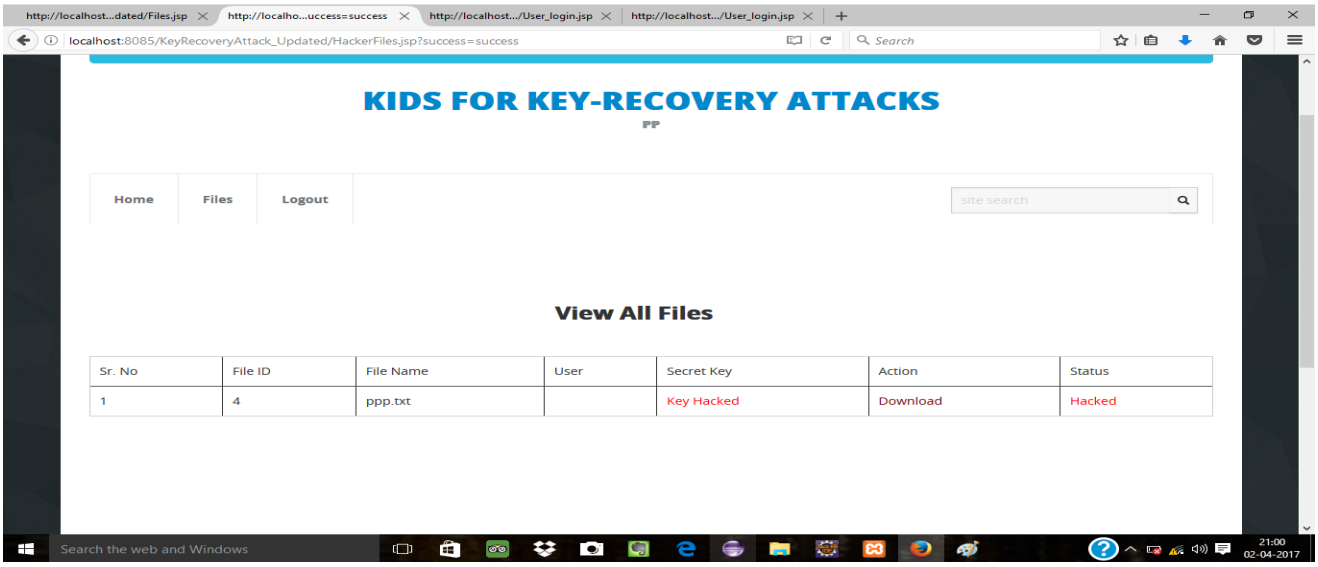
VI. Snapshots

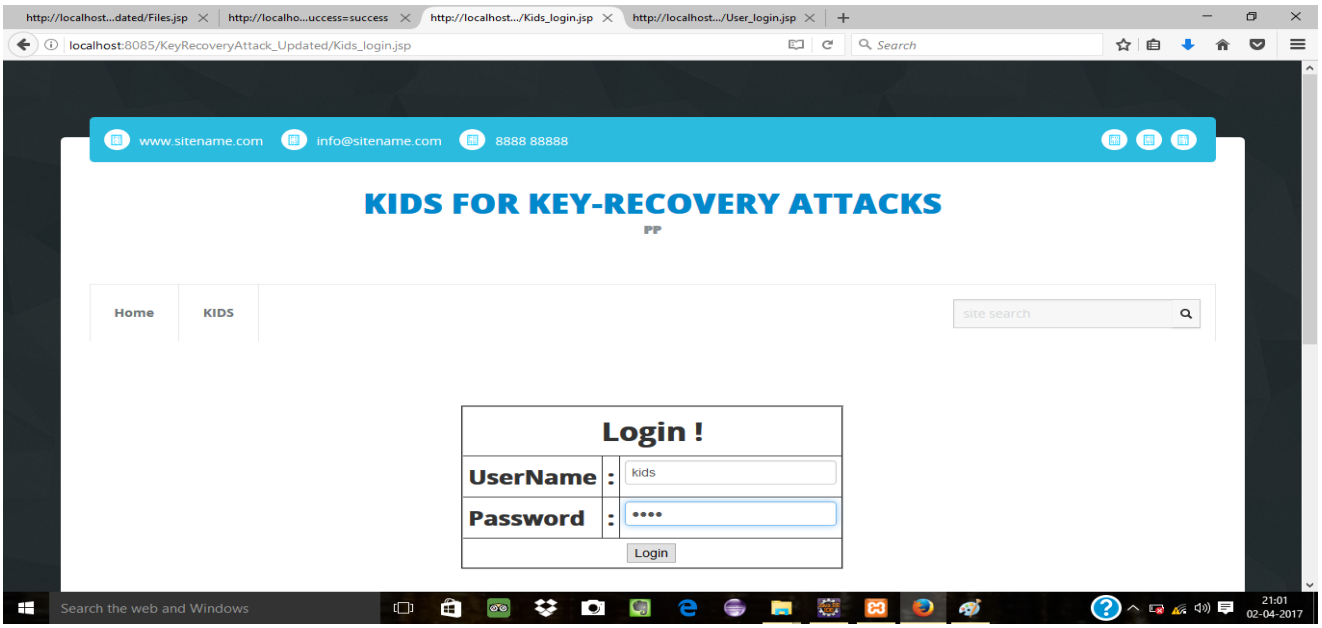


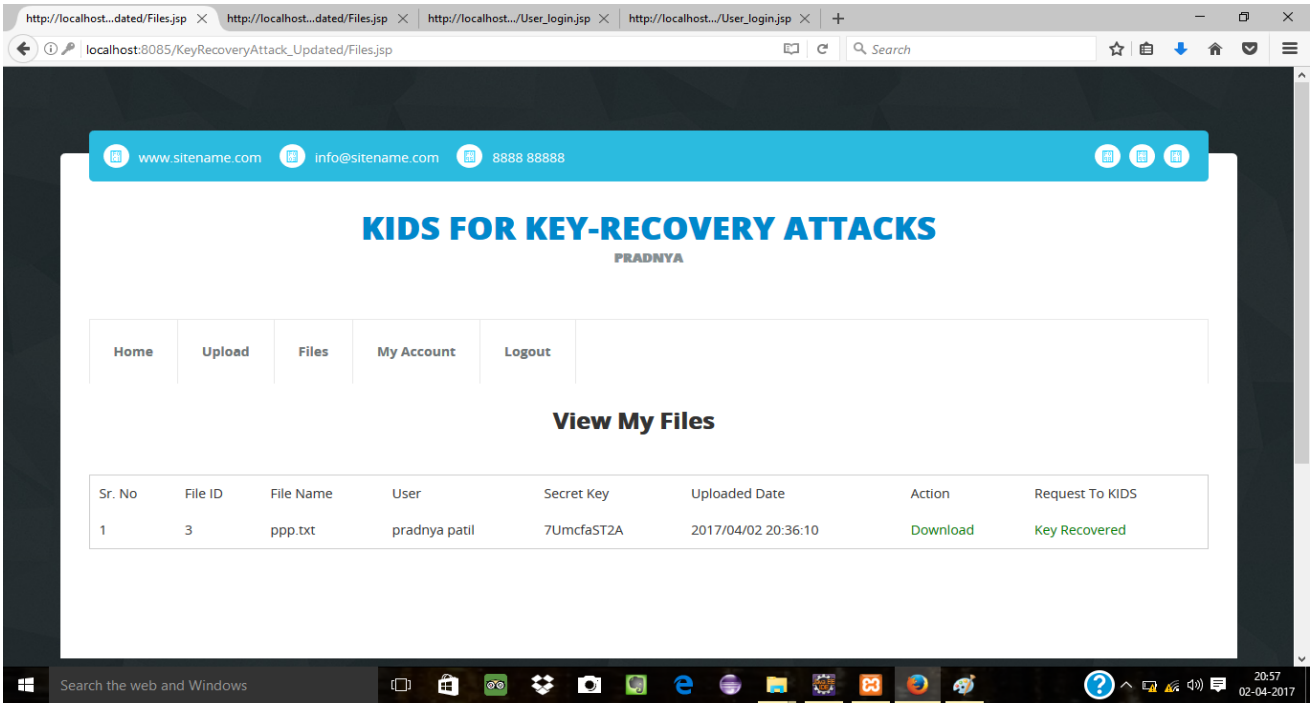












VII. Conclusion and Future Work

In this project we have examined the quality of KIDS against key-recovery assaults. In doing as such, we have adjusted to the irregularity recognition setting an ill-disposed model obtained from the related field of ill-disposed learning.
To the best of our insight, our work is the first to exhibit key-recovery assaults on a keyed classifier. Shockingly, our assaults are to a great degree proficient, demonstrating that it is sensibly simple for an aggressor to recoup the key in any of the two settings examined. Such an absence of security may uncover that plans like KIDS were just not intended to avert key-recovery assaults. However, we have argued that resistance against such attacks is essential to any classifier that attempts to impede evasion by relying on a secret piece of information.
Our future design is to base decisions on robust principles rather than particular fixes. Going beyond KIDS, it remains to be seen whether similar schemes are secure against key recovery attacks. Our attacks (or variants of them) are focused on keyed classifiers, and we believe that they will not carry over randomized classifiers. We note that, in its present form, KIDS cannot be easily randomized, as choosing a new key implies training the classifier again, which is clearly impractical in real-world scenarios.

VIII. References

[1] 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.
[2] 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.
[3] B. Biggio, G. Fumera, and F. Roli, Adversarial Pattern Classification Using Multiple Classifiers and Randomization, Proc. IAPRIntl Workshop Structural, Syntactic,and Statistical Pattern Recognition, pp. 500-509, 2008.
[4] B. Biggio, B. Nelson, and P. Laskov, Support Vector Machines Under Adversarial Label Noise, J. Machine Learning Research, vol. 20, pp. 97-112, 2011.
[5] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, Adversarial Classification, Proc. 10th ACM SIGKDD Intl Conf. Knowledge Discovery and Data Mining (KDD 04), pp. 99-108, 2004.
[6] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee, Polymorphic Blending Attacks, Proc. 15th Conf. USENIX SecuritySymp., 2006.
[7] C. Gates and C. Taylo, Challenging the Anomaly Detection Paradigm: A Provocative Discussion, Proc. New Security ParadigmsWorkshop (NSPW), pp. 21-29, 2006.
[8] A. Kolcz and C.H. Teo, Feature Weighting for Improved Classifier Robustness, Proc. Sixth Conf. Email and Anti-Spam (CEAS 09), 2009

