An Intrusion Detection and Protection System by using Datamining Forensic Technique

Rupali Dokhe[1], Prof.N.G.Pardeshi[2]
[1]*Student,* [2]*Professor,*
[12]*Department of computer Engineering, Sanjeevani College of Engineering Kopargaon, Savitribai Phule Pune University, Pune, Maharashtra, India*

Abstract- Currently, most PC frameworks use client IDs and passwords as the login examples to verify clients. Be that as it may, numerous individuals share their login designs with collaborators and demand these colleagues to help co-assignments, consequently making the example as one of the weakest purposes of PC security. Insider assailants, the legitimate clients of a framework who assault the framework inside, are difficult to recognize since most interruption location frameworks and firewalls distinguish and segregate pernicious practices propelled from the outside universe of the framework as it were. Moreover, a few investigations asserted that breaking down framework calls (SCs) produced by directions can recognize these directions, with which to precisely distinguish assaults, and assault designs are the highlights of an assault.

In this way, a security framework, named the Internal Intrusion Detection and Protection System (IIDPS), is proposed to identify insider assaults at SC level by utilizing information mining and scientific procedures. The IIDPS makes clients' close to home profiles to monitor clients' utilization propensity. As their forensic features and determines whether a valid login user is the account holder or not by comparing his/her current computer usage behaviours with the patterns collected in the account holder's personal profile.

Keywords- Data mining, insider attack, intrusion detection and protection, systemcall (SC), users' behaviours.

I. INTRODUCTION

In the previous decades, PC frameworks have been broadly utilized to furnish clients with less demanding and increasingly helpful lives. Be that as it may, when individuals abuse ground-breaking capacities and preparing intensity of PC frameworks, security has been one of the major issues in the PC area since assailants more often than not attempt to infiltrate PC frameworks and carry on noxiously, e.g., stealing critical data of a company, making the systems out of work or even destroying the systems. Generally, among all outstanding assaults, for example, pharming assault, appropriated disavowal of-benefit (DDoS), listening in assault, and lance phishing assault [1], [2]. we propose a security framework, named Internal Intrusion Detection and Protection System (IIDPS), which distinguishes pernicious practices propelled toward a framework at SC level. The IIDPS utilizes information mining and legal profiling strategies to mine framework call designs (SC-designs) characterized as the longest framework call grouping (SC-succession) that has repeatedly appeared several times in a user's log file for the user. The client's criminological highlights, characterized as a SC-design much of the time showing up in a client's submitted SC-successions yet seldom being utilized by Different clients, are recovered from the user's computer usage history.

II. LITERATURE SURVEY

[1].PriteeShendkar, S. M. Sangv**"New Approach of an Internal Intrusion Detection and Protection System"** International Journal of Innovative Research in Science, Engineering and Technology Vol. 6, Issue 7, July 2017.

In this paper, a security system, called Internal Intrusion Detection and Protection System (IIDPS), is designed to find insiderattacks. The IIDPS creates user's habit profiles to keep track of user's habits anddetermines whether the login user is the account holder or not by comparing thecurrent computer usage behaviours of the user with the patterns collected in theaccount holder's habit profiles.

[2]. Z. B. Hu, J. Su, and V. P. Shirochin**"An intelligent lightweight intrusion detection system with forensics technique,"** in Proc. IEEE Workshop Intell. Data Acquisition Adv. Comput. Syst.: Technol. Appl., Dortmund, Germany, 2007, pp. 647{651.

This paper proposed a security system, named the Internal Intrusion Detection and Protection System (IIDPS) to detect insider attacks at SC level by using data mining and forensic techniques in networked data. The IIDPS creates users' personal profiles to keep track of users' usage habits as their forensic features and determines whether a valid login user is the account holder or not by comparing users current computer usage behaviours with the patterns collected in the account holder's personal profile. The idea behind the inside attacker detection in wire-less sensor network by exploiting the spatial correlation between the packet ratio, which help to detecting dynamic attacking behaviours The routing is performed to identify the shortest path between each source node and their destination address and residual energy is calculated for each node in the network.

[3]. M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, **"Data-stream based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study,"** IEEE Syst. J., vol. 9, no. 1, pp. 1{14, Jan. 2014.

In this paper security System defene s as the Internal Intrusion Detection and Protection System (IIDPS), is help to detect internally attacks by using data mining and forensic technique at SC level. For the track the information of users usages the IIDPS creates users' personal profiles as their forensic features and investigate that the valid login user is account holder can login or not by comparing his/her current computer usage behaviours with the patterns collected in the account holder's personal profile. The experimental results demonstrate that the IIDPS's user identification accuracy is 94.29.

[4]. J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, **“Detecting web-based DDoS attack using MapReduce operations in cloud computing environment,"** J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 28{37, Nov. 2013. This paper proposes a method of integration between HTTP GET flooding among DDOS attacks and MapReduce processing for a fast attack detection in cloud computing environment. This method is possible to ensure the availability of the target system for accurate and reliable detection based on HTTP GET flooding. In experiments, the processing time for performance evaluation compares a pattern detection of attack features with the Snort detection. The proposed method is better than Snort detection method in experiment results because processing time of proposed method is shorter with increasing congestion.

III. PROPOSED SYSTEM

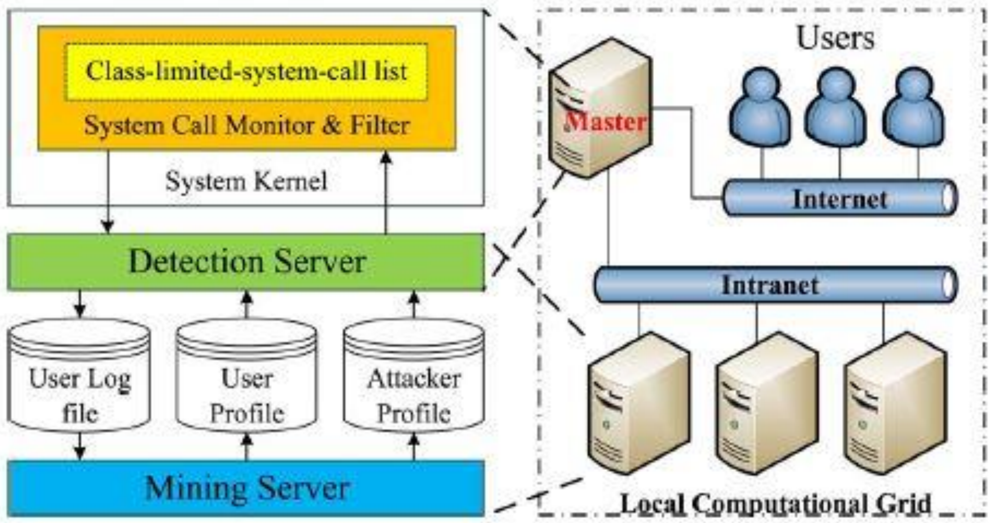


Fig.1: Proposed System Architecture

Explanation: The IIDPS, as appeared in Fig., comprises of a SC screen and channel, a mining server, a location server, a nearby computational matrix, and three storehouses, including client log records, client profiles, and an assailant profile. The SC screen and channel, as a loadable module inserted in the part of the framework being considered, gathers those SCs submitted to the bit and stores these SCs in the configuration of uid, pid, SC in the secured framework where uid, pid, and SC individually speak to the client ID, the procedure ID, and the SC c put together by the fundamental client. It likewise stores the client contributions to the client's log record, which is a document keeping the SCs put together by the client following their submitted arrangement. The mining server investigations the log information with information mining methods to distinguish the client's PC use propensities as his/her personal conduct standards, which are then recorded in the user's profile.

Advantages of Proposed System:

1. Can distinguish a client's measurable highlights by dissecting the comparing SCs to upgrade the precision of assault recognition;
2. Able to port the IIDPS to a parallel framework to additionally abbreviate its identification reaction time; and
3. Effectively oppose insider assault.

IV. ALGORITHM IMPLEMENTATION

1. Algorithm

1: The algorithm for generating user habit file

Input: u’s log file where u is the user f underlying structure Output: u’s habit file 1. G =log file – sliding window /* sliding window = L-window = C-window */

2. For (i = 0 ; I ¡ G-1 ; i++)

3. For(j = i + 1 ; j ¡= G ; j++)

4. For (each of (—Sliding window— k + 1) k-grams in current L-window.

5. For (each of (—Sliding window— k’+ 1) k’-grams in Cwindow.

```
6. Compare the k-grams and k'-grams with the longest common subsequence algorithm

 7. if the identified SC-pattern already exist in the habit file

 8. increase the count of SC-pattern by one.

9. else

10. insert the SC-pattern into habit file with count=1;
```

2. Algorithm: Detecting an internal intruder or attacker

```
1. NCS$\mu$ = ø;
2. while(receiving u's input SC, denoted by h){
3. NCS$\mu$= NCS$\mu$ U {h};
4. if( | NCS$\mu$ | > |Sliding window| ){
 5. L-window = right NCS$\mu$ |sliding window|); /* right(x,y) retrieves the last L window of y from x */
6. for(j = |NCS$\mu$|-| sliding window| ; j>0 ; j-- ){
7. C-window = mid(NCS$\mu$,j,|sliding window|); /* mid(x,y,z) retrieves sliding window of size z begining at the position of y from x */
8. Compare k-grams and k'-grams using comparison logic employed in algorithm 1 to generate habit file
 9. for(each user g, 1<= g<=N)
 10. calculate similarity score sim(u,j) between NCS$\mu$ and g's user profile by invoking eq.8
11. if((NCS$\mu$ mod paragraph size) == 0) /* paragraph size=30 meaning we judge wheather u
12. Sort similarity score for all users.
13. if((the decisive rate of every u's user profile < threshold1) or (the decisive rate of attacker profile > threshold2)) /* threshold1 is predefined lower bound of average decisive rate of users u's
profile, while threshold2 is the predefined upper bound of average rate of attacker profile*/is attacker or account holder for every 30 input SC's*/
14. alert system manager that u is a suspected attacker, rather than u himself/herself ;
```

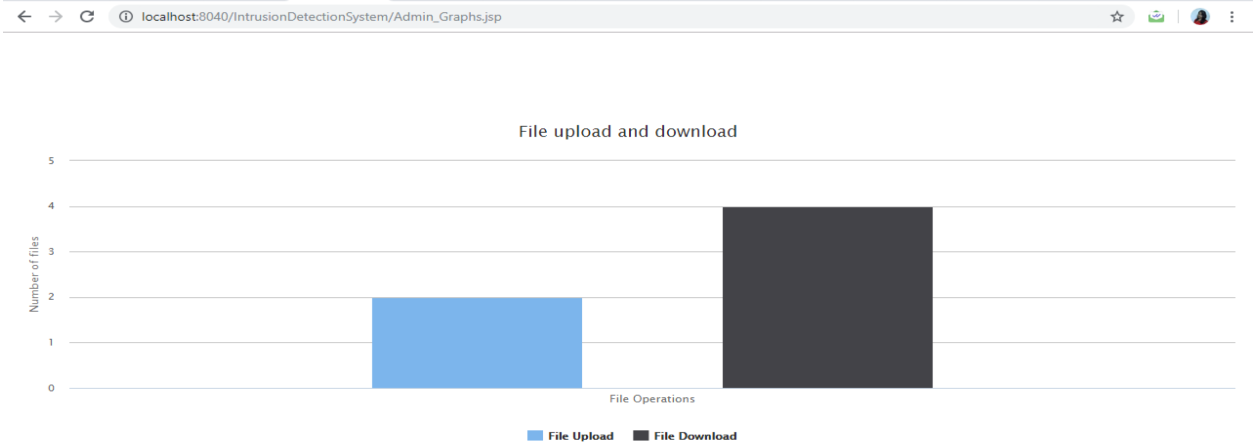
V. RESULTS AND DISSCUSION

The configuration of the experimental testbed, which consists of 12 users;one protected computer, Logical configuration of the testbed employed.Named Alpha; and another two members of the computational grid, namedBeta with 48 processing cores and Gamma with 12 processing cores.All the computers operate with Linux operating system, and the memorysize for each computer is at least 25 GB. The measured bandwidths andnetwork types between two arbitrary nodes of the computational grid Inthe IIDPS testbed, the SC monitor and filter is first installed into theAlpha computer to obtain each user's log _le The SCs from 12 differentcategories of users are collected as the experimental data, including thesystem (root), oracle, message queue (mq), reservation, ticketing, financial,operating strategy (os), backup, configuration management (cm), webapplication, business rule, and audit users.A total of 193 613 SCs have been collected from 12 log _les, in which thelength of a sliding window is 10.

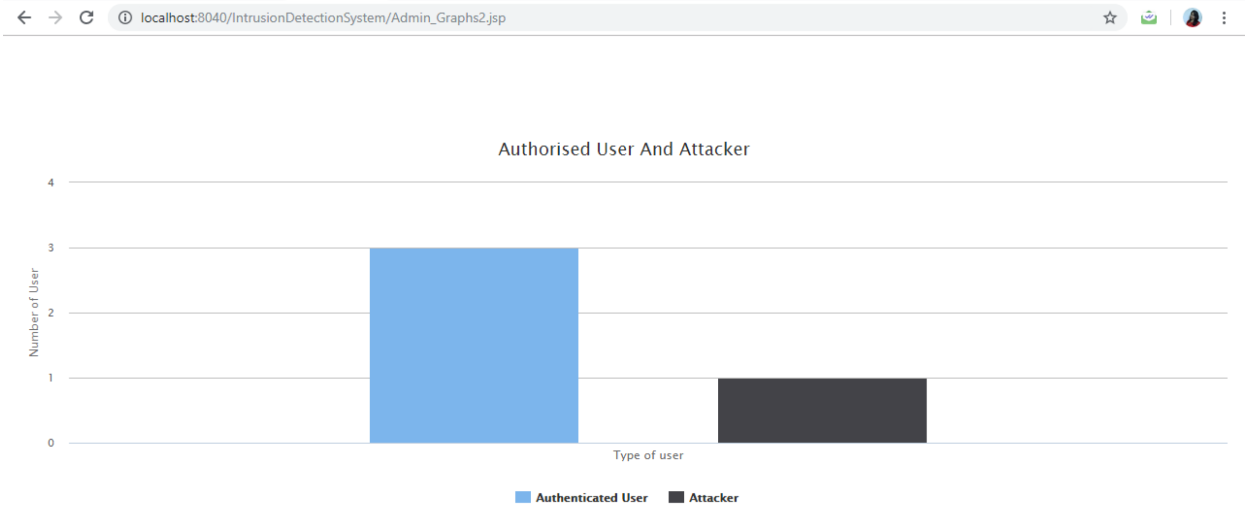
In the second experiment, we again randomly chose 75users computerusage history as the training data for creating 12 user profiles, and theremaining 25simulate user u's online inputs. The purpose is to gain thesimilarity scores between u and all the users so that the IIDPS can judgewho the user u is in the intranet. The statistical information for 12 userprofiles generated by the mining server is listed in Table V, in which the\Account ID" shows the user's ID, |Training data| is the number ofSCs in the training data, |Habit _le| is the number of SC-patterns(rather than SCs) collected in a habit _le, and User profile is the numberof SC-patterns gathered in the user's user profile. About 40their similarityweights are less than the pre-defined threshold 0.001.The IIDPS is a typical HIDS that monitors internal events of a system. AHIDS often gathers and analyzes information issuedby users within a system to identify possible threats. To investigatethe system's intrusion detection capability, in the thirdexperiment, the IIDPS is compared with four HIDS and Symantec CSP.The OSSEC analyzes log data, checks _le integrity, moni- tors set policies,detects rootkits, alerts suspected attacks in realtime, and responds actively.

It has a collaboration learning agent that analyzes log _les to identifysimple Type-III attacks. AIDE (Tripwire) checks _le and directors' integrity for a predefined time interval given by the system administrator.SAMHAIN provides _le integrity checking and log file monitoring andanalysis. It also detects rootkits, monitors ports, identifies rogue root privilege executable, and figures out hidden processes that issue Type-Iand Type-II attacks.Symantec CSP as a superset of the Symantec host IDS can detect part ofthe Type-III attacks and DDoS attacks launched by a system. It identifies DDoS attacks issued by a system by monitoring the system's outbound traffic. However, this may also trigger false-positive alarms, particularlywhen users or normal programs upload data to the Internet.

The experimental results demonstrate that the IIDPS's user identificationaccuracy is 94.29the response time is less than 0.45 s, implying that it canprevent a protected system from insider attacks effectively and efficiently.

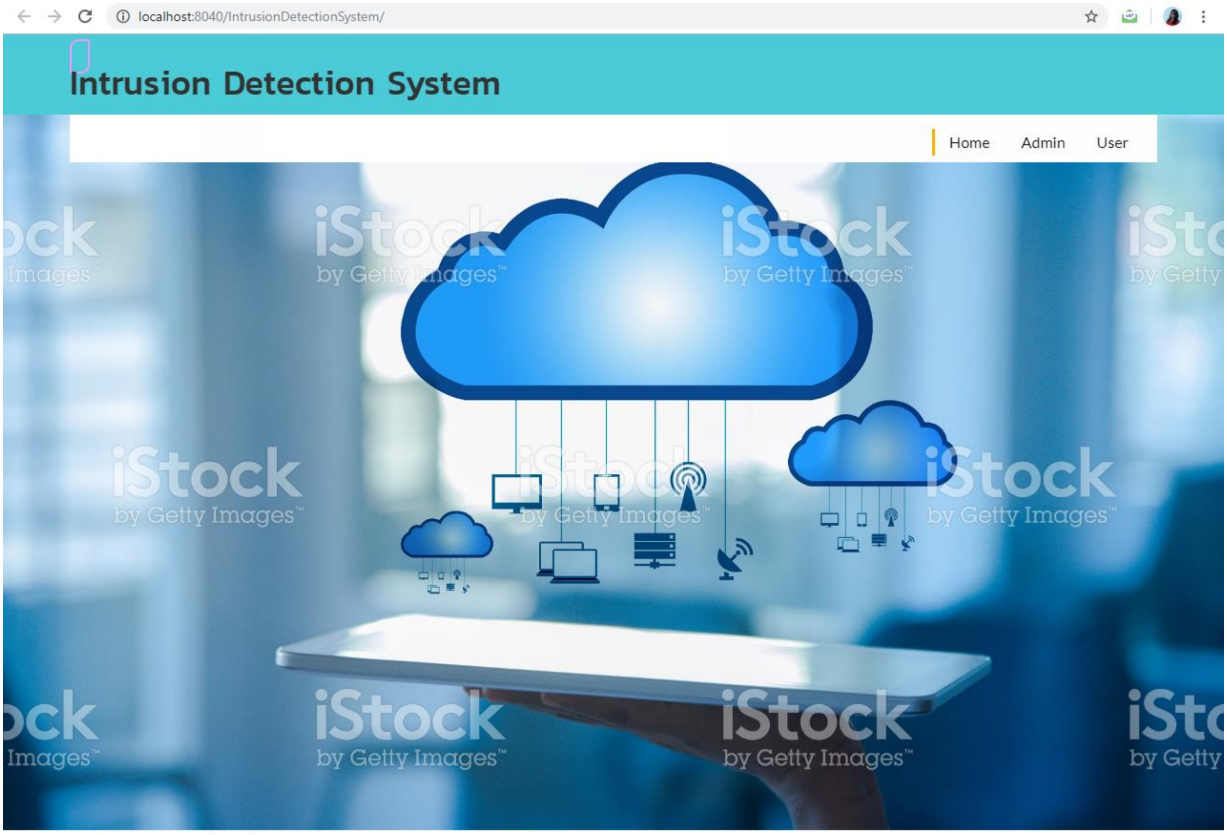


Graph.1: File upload and download graph

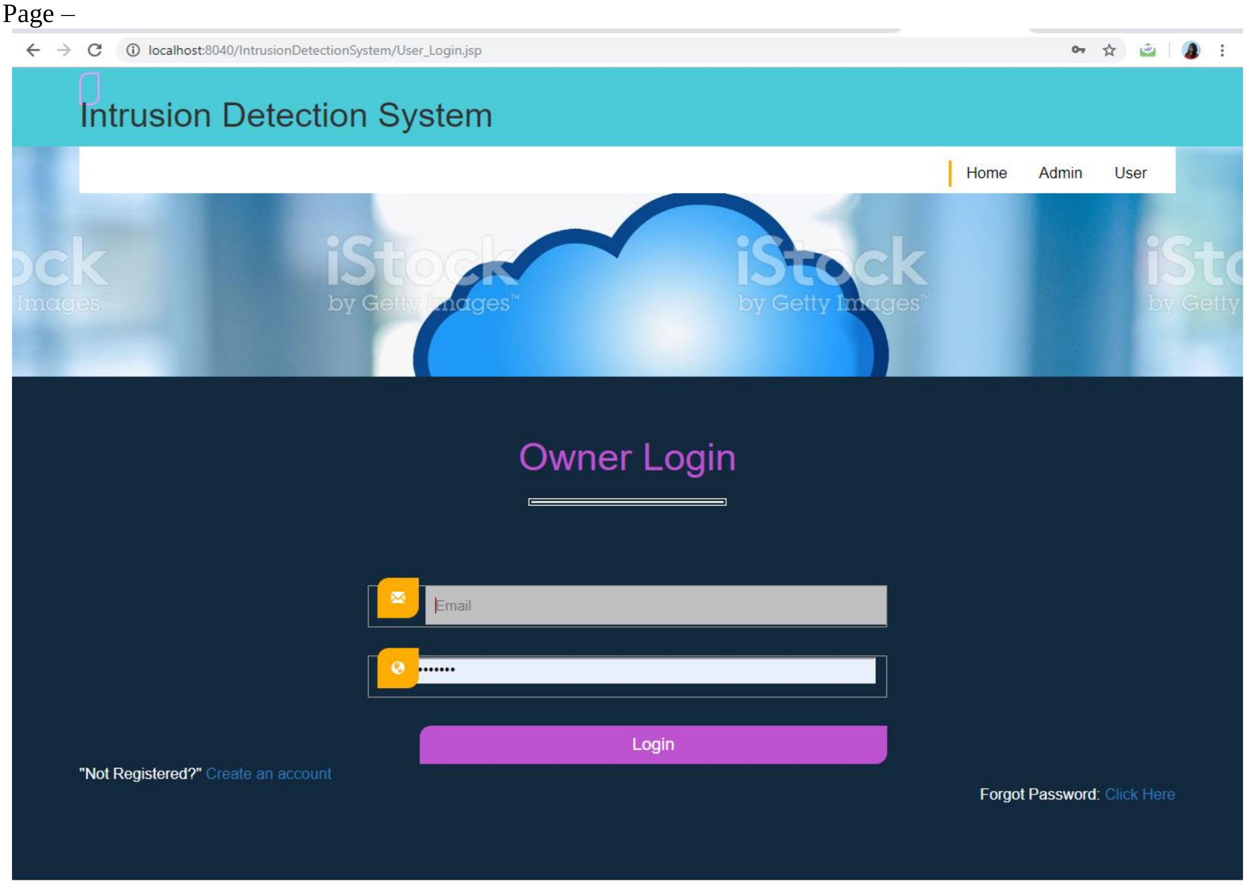


Graph 1: Authorized user and attacker graph

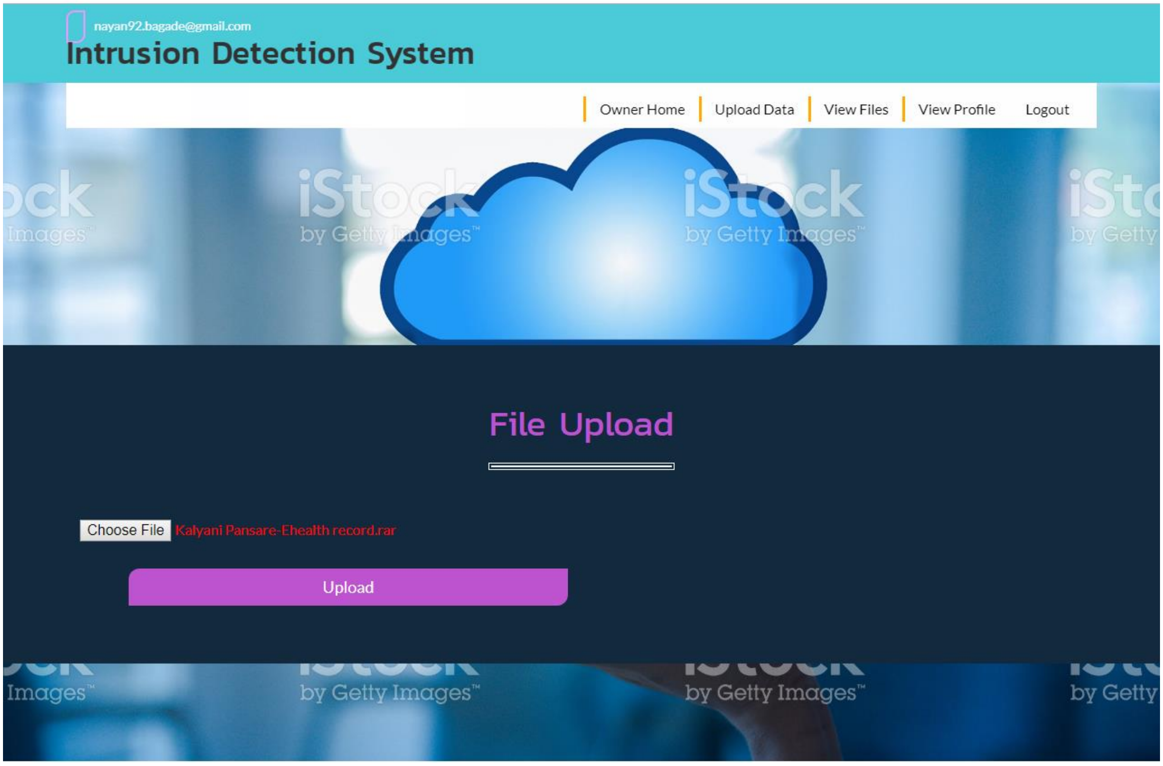
Home page –


localhost:8040/IntrusionDetectionSystem/
Intrusion Detection System
Home
Admin
User

Login Page –


localhost:8040/IntrusionDetectionSystem/User_Login.jsp
Intrusion Detection System
Home
Admin
User
Owner Login
Email
•••••••
Login
"Not Registered?" Create an account
Forgot Password: Click Here

Data upload by user –



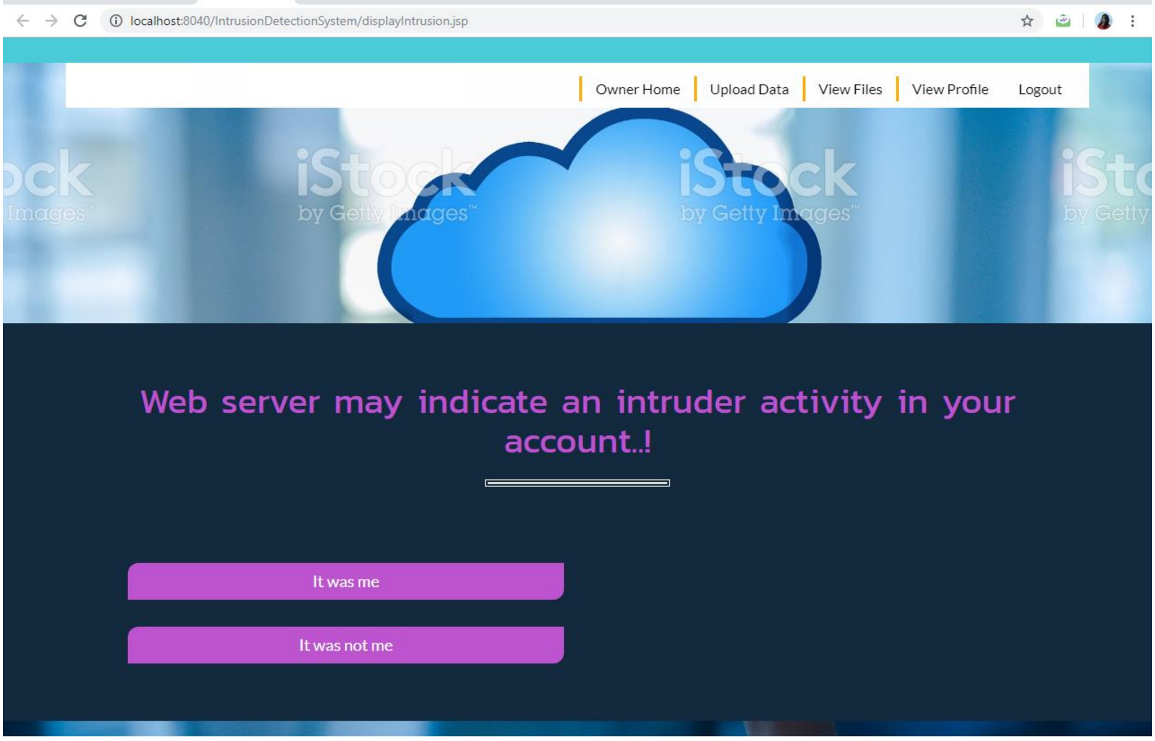
nayan92.bagade@gmail.com

Intrusion Detection System

File Upload

Choose File Kalyani Pansare-Ehealth record.rar

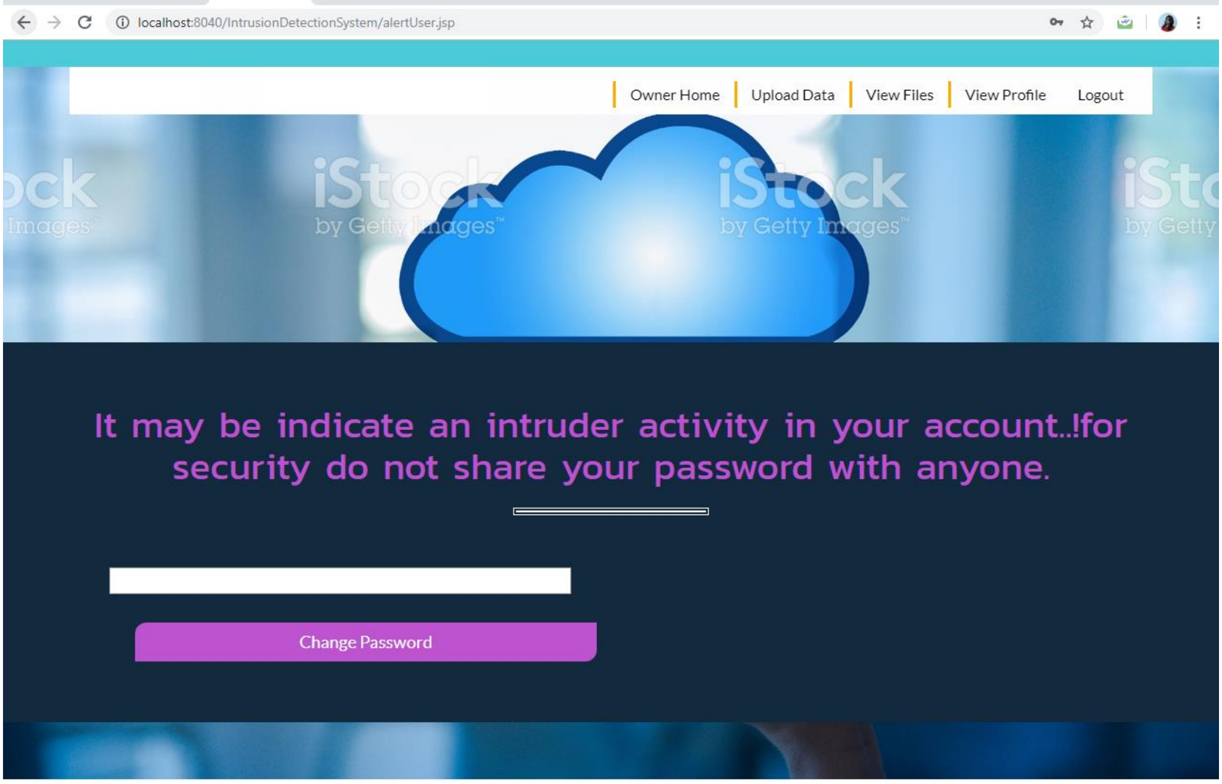
Confirming activity by user –



localhost:8040/IntrusionDetectionSystem/displayIntrusion.jsp

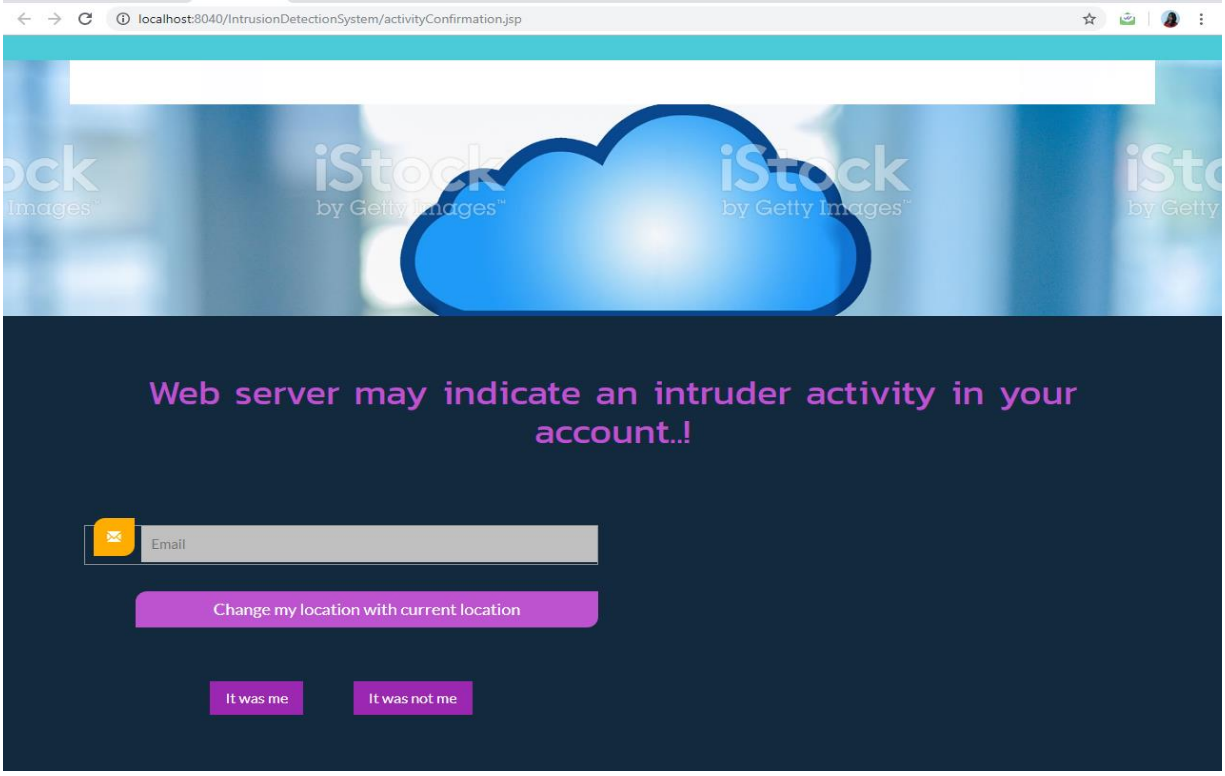
Web server may indicate an intruder activity in your account..!

Password change for security –



It may be indicate an intruder activity in your account..!for security do not share your password with anyone.

Activity confirmation after login from different location –



localhost:8040/IntrusionDetectionSystem/activityConfirmation.jsp
Email
Change my location with current location
It was me
It was not me

Web server may indicate an intruder activity in your account..!

VI. CONCLUSION AND FUTURE WORK

We have proposed an approach that employsdata mining and forensic techniques to identify the representative SC-patterns for a user. The time that a habitual SC pattern appears in the user’s log file is counted, the most commonly used SC-patterns are filtered out, and then a user’s profile is established. By identifying a user’s SC-patterns as his/her computer usage habits from the user's current input SCs, the IIDPS resists suspected attackers.

VII. REFERENCES

[1]. S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsersOr how to thwart a phisher with trusted computing," in Proc. IEEE Int. Conf. Avail., Rel. Security, Vienna, Austria, Apr. 2007, pp. 120–127.

[2]. C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," ACM Trans. Int. Technol., vol. 10, no. 2, pp. 1–31, May 2010.

[3]. Q. Chen, S. Abdelwahed, and A. Erradi, "A model-based approach to self-protection in computing system," in Proc. ACM Cloud AutonomicComput. Conf., Miami, FL, USA, 2013, pp. 1–10.

[4]. F. Y. Leu, M. C. Li, J. C. Lin, and C. T. Yang, "Detection workload in a dynamic grid-based intrusion detection environment," J. Parallel Distrib.Comput., vol. 68, no. 4, pp. 427–442, Apr. 2008.

[5]. H. Lu, B. Zhao, X. Wang, and J. Su, "DiffSig: Resource differentiation-based malware behavioral concise signature generation," Inf. Commun Technol., vol. 7804, pp. 271–284, 2013.

[6]. Z. Shan, X. Wang, T. Chiueh, and X. Meng, "Safe side effects commitment for OS-level virtualization," in Proc. ACM Int. Conf. AutonomicComput., Karlsruhe, Germany, 2011, pp. 111–120.

[7]. M. K. Rogers and K. Seigfried, "The future of computer forensics: A needs analysis survey," Comput. Security, vol. 23, no. 1, pp.12–16, Feb. 2004.

[8]. J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting web-based DDoS attack using MapReduce operations in cloud computing environment," J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 28–37, Nov. 2013.