

Implementation of “An Intelligent Intrusion Detection and Protection System Using Log Analysis And System Calls”

¹Deepali Bhingardive, ²Ranmalkar Vrushali S

Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra

ABSTRACT

Now days, most computer systems use user Ids and passwords as the login patterns to authenticate users. However, many people share their login patterns with co-workers and request these co-workers to assist co-tasks, thereby making the pattern as one of the weakest points of computer security. To detect the intrusion, an Intrusion Detection System (IDS) is used. To detect respond and the intrusion in timely manner is its prime function. In other words, IDS function is limited to detection as well as response. The IDS is unable to capture the state of the system when an intrusion is detected. So that in original form it fail to preserve the evidences against the attack. New security strategy is very much needed to maintain their liability and completeness of evidence for later examination. In this research work, there proposed an automated Digital Forensic Technique with Intrusion Detection System. It sends an alert message to capture the state of the system, to the administrator followed by invoke the digital forensic tool Once an IDS detects an intrusion. To prove the damage Captured image and picture can be used as evidence in the court of law.

KEYWORDS :- *Intrusion Detection Systems, Digital Forensic, Logs, Cryptography, Data mining, insider attack.*

1. INTRODUCTION

In the past decades, people exploit powerful capabilities and processing power of computer system, security has been one of the very serious problems in the computer domain. In today's scenario, to safeguard the organization electronic assets, Intrusion Detection System is crucial requirement. To find whether the traffic is malicious or not Intrusion detection is a process of analyzes and monitor the traffic on a device or network. It can be a physical appliance or software that monitors the traffic which violates organization security policies and standard security practices. To catch the respond and intrusion in timely manner as a result risks of intrusions is diminished it continuously watches the traffic. Based on the deployment IDS (Intrusion Detection System) broadly divided into two types such that Host based Intrusion Detection System (HIDS) and the second is Network based Intrusion Detection System (NIDS). Host-based Intrusion Detection System (HIDS) is configured on a particular server/ system. It continuously analyses and monitor the activities the system where it is set up or configured. Whenever an intrusion is detected Host based Intrusion Detection System triggers an alert notification. For instance, when an attacker tries to modify or create or delete key system files alert will be generated. Wide advantages of the HIDS that it analyses the incoming encrypted traffic which can't be detected NIDS. To catch the attack like Port Scans, Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attack, etc. Network Intrusion Detection System continuously analyses and monitors the network traffic. To classify as non-malicious or malicious traffic it inspect the incoming network traffic. If any predefined signatures or patterns of malicious behavior are present it re-assembles the packets, examine the payload/ headers portion and determine. Recently "Intrusion investigations with data-hiding for computer Log-file Forensics" system has been designed. In this approach, log file is stored in two different area as well as in two different forms. On target host the Log file in plain text form is stored and a copy of same log file is stored in another host called log manager and it is covered in image using steganography. Intrusion

Detection System running on target host detects an intrusion and sends an alert message notification to the security administrator about the intrusion when an intruder tries struggling to alter log file on target host. Security administrator uses the stego image to extract log file and compares it with log file available in the target host. To justify whether the intrusion occurred or not. Intrusion is confirmed If the result of the comparison is not equal else not.

Forensic technique system is unable to capture the proof of the attack is the major limitation of this approach. So to secure the log file damage for forensic analysis, it is not possible and to show in the court of law, proof cannot be collected immediately against the attack. In this work automated Digital Forensic Technique with Intrusion Detection System IDS is proposed to overcome this limitation. Because the current IDS are not designed to protect and collect evidence against the attack this new technique is crucial requirement. Digital forensics plays very important role by providing scientifically proven methods to process, gather, interpret and use digital evidence to bring a decisive description of attack.

2. LITERATURE SURVEY

Computer forensics science, which views computer systems as crime scenes, goal to preserve, identify, analyze, recover and present opinions and facts on information collected for a security event [1]. It investigate what attackers have done like as spreading computer malwares, viruses, and malicious codes and conducting Distributed Denial of Service attacks [2]. Most intrusion catching techniques focus on how to detect malicious network behaviors [3] and acquire the characteristics of attack packets, such that attack patterns, based on the histories recorded in log files [4]. Qadeer et al [5] used self-developed packet sniffer to gather network packets with which to discriminate network attacks with the help of packet distribution and network states. O Shaughnessy and Gray [6] obtained attack patterns and network intrusion from system log files. These files keep traces of computer misuse. It means, from synthetically produced log files, these patterns or traces of misuse can be more correctly reproduced. Wu and Banzhaf [7] acquired research progress of assigning methods of computational intelligence, including fuzzy systems, artificial neural networks, evolutionary computation, swarm intelligence and artificial immune systems to catch malicious behaviours. The authors systematically compared and summarized different intrusion detection methods, thus allowing us to clearly view those existing research challenges. These aforementioned applications and techniques truly contribute to network security. However, they cannot simply authenticate remote-login users and detect specific types of intrusions, example, when an undefined user logs in to a system with a valid password and user ID. In our previous work, a security system, which includes forensic quality for users at command level rather than at SC level, by invoking forensic techniques and data mining, was developed. Moreover, if attackers use more sessions to issue attacks, e.g., launch DDoS attacks or multistage attacks, then it is not easily for that system to determine attack patterns. Hu et al [8] presented an intelligent lightweight Intrusion Detection System that utilizes a forensic technique to profile user behaviors and a data mining technique to carry out the cooperative attacks. The authors claimed that the system could catch intrusions efficiently and effectively in real time. However, they did not define the SC filter. Giffin et al. [9] provided another e.g., of integrating computer forensics with a knowledge based system. The system choose a predefined model, which, grant SC-sequences to be simply executed, is employed by a detection system to bound program execution to ensure the security of the protected system. This is helpful in catching applications that issue a series of malicious SCs and identifying attack sequences having been stored in knowledge bases. When an undetected attack is presented, the system frequently finds the attack sequence in 2s as its computation overhead. Fiore t al. [10] explored the effectiveness of a detection approach which is based on machine learning using the Discriminative Restricted Boltzmann Machine technique to combine the expressive power of generative models with better classification accuracy capabilities to infer part of its knowledge from incomplete training data so that the network anomaly finding scheme can provide an adequate degree of protection from both external and internal menaces. Faisal et al [11] examine the possibility of using data stream mining to improve the security of advanced metering infrastructure through an Intrusion Detection System. The advanced metering infrastructure, which is one of the most important components of smart card, serves as a bridge for providing bidirectional information flow between the utility domain and user domain. The authors treat an Intrusion Detection System (IDS) as a second-line security measure after the first-line of primary advanced metering infrastructure security system techniques such as authorization, authentication and encryption.

A. Intrusion Investigations with Data-hiding for Computer Log-file Forensics:

In most of companies or organizations, logs play important role in information security. However, the common security mechanism only backup logs, it is not able to detect traces of intruders because the hacker who is able to intrudes the security mechanism of organization would try to alter logs or destroy important intrusion evidences

making it impossible to keep evidence using traditional log security strategies. Thus, logs are not considered as evidence to prove the damage. In that case, digital prove lacks in terms of completeness which makes it difficult to perform computer forensics operations. In order to maintain the completeness and reliability of evidence for later forensic procedures and intrusion detection, the study applies idea of steganography to logs forensics, for which even intrusion altered records will be kept as well. Comparing to traditional security strategies, this study proposes a better logging system to ensure the completeness of logs. Furthermore, the study will assist in intrusion detection through alteration behavior, and help in forensic operations.

B. A log correlation model to support the evidence search process in a forensic investigation:

Computer forensics searches for evidence to reassemble the actions that led the system from a secure state to the moment an intrusion was detected. The main source of data for a forensic investigation is the information provided by log files. Log files are produced by applications to keep a register of the actions occurred on the system. However, the massive amount of recorded events complicates the forensic investigation. A model composed by a set of agents in order to filter, collect, normalize, and to correlate events coming from diverse log files is proposed in this paper. The purpose of the model is to assist the analyst in the evidence search process of a forensic investigation.

C. Intrusion detection and identification system using data mining and forensic techniques:

Presently, most computers authenticate a password and user's ID before the user can log in. However, if the two items are known to hackers, there is a risk of security breach. In this paper, we propose a system, named the Identification System (IDIS) and Intrusion Detection, which builds a profile for each user in an intranet to keep track of his/her usage habits as forensic features. In this way the IDIS can identify who the underlying user in the intranet is by comparing the user's current inputs with the features collected in the profiles established for all users. User habits are extracted from their usage histories by using data mining techniques. When an attack is detected, the IDIS switches the user's inputs to a honey pot not only to isolate the user from the underlying system, but also to collect more attack features by using the honey pot to enrich attack patterns which will improve performance of future detection. Our experimental results show that the recognition accuracy of students in the computer science department of our university is nearly 99.16% since they are sophisticated users. The recognition accuracy of those other than computer science students is 94.43%.

3. PROPOSED SYSTEM

In this approach, log file is stored into two different forms as well as in two different places. Log file plain text from is stored on target host and a copy of same log file is stored in another host called log manager. When an intruder tries to alter log file on target host, IDS running on the target host detects an intrusion and sends an alert message to the security administrator about the intrusion which in turn takes the required steps to mitigate it.

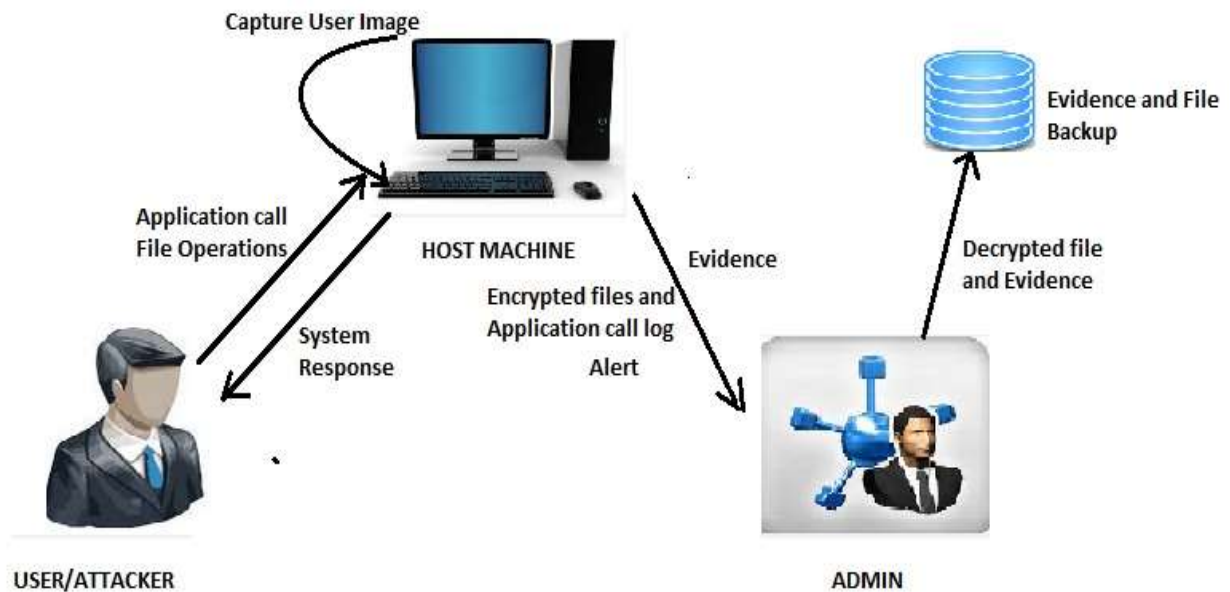


Figure -1: Proposed Architecture

A. Target Host

The target machine is one on which different user can access the different application. We are going to develop intrusion detection system for college. For example students are having access for only software which are required for their academic needs. If some students doing malicious activities on the host machine then our system will detect the intrusion. The Crucial data (i.e. log files) is stored in the Target Host. Continuous monitor of log file is prime requirement to preserve the integrity and confidentiality of the data stored in it. To achieve this, IDS is deployed on target host and it is a continuous process round the clock. Whenever an attacker tries to intrude the target host, IDS running on target host detects the log server. Further, it invokes the digital forensic technique to capture the state of the system (RAM image and log file image) and t. Newly captured log file image is compared with previous log file image to confirm he intrusion. Our Target Host is nothing but our Operating System as it is a Host based System. The intruder shall be able to access the system but if he tries to alter any of the system properties and manipulate the records then the IDS comes into picture.

B. User/ Attacker:

It is the user which can do the normal operations on the host machine. It may be attacker or normal user. Attacker have to login to the system. User needs to enter the credentials such as email id, password contact details at the time of registration. At the tie of login if user fails to enter correct information such as user id and password then system should automatically get close. If user did operations other than normal operations then system will detect the intrusion. If user play with secure file in particular folder then original file and updated file will send to the server.

C. Security Centre/ Admin:

This is the system used by the security administrator to monitor the alerts generated by IDS. It receives alerts from Target Host. Once the target host has sent the alert to the Security Centre, the job of the Security Centre starts. The attack is hence detected and looked into at the Security Centre. The Security centre is the most essential component of the IDS. Its job is to track the intrusion in such a way that as soon as he/she tries to access the system, an alert should be sent to the real owner. This shall be accompanied by the webcam image capturing activity in order to prove the offence in the court of law. If the intruder tries to access the files without the net connection, the system shall shut down by itself within 10 seconds, and if he has the net connection intact, then we shall also be able to inform the true owner about the intrusion with the help of an e-mail. In proposed system we are detecting the intrusion through many thing like integrity, checking currently running processes, by key log, etc. These all

activities are performed by user. The first activity is file integrity. We are detecting intrusion through file integrity. In file integrity concept if any user delete the file or modify file or insert file into specific directory then by using our system we can detect it. If any file delete or modify of insert into specific folder then that file will save in folder which is specified by client. Then file integrity log send to server. Server send the integrity of that file to the clients email id. So that client will easily know which file is modified. So that that we can recover that modified file from specified backup folder.

4. MATHEMATICAL MODEL

A. User:

- Set (U) = fu0, u1, u2, u3g
- U0- insert files
- U1- delete files
- U2- update files
- U3- install new process

B. Client Module:

- Set (C) = fc0, c1, c2, c3, c4, c5, c6g
- C0- capture user image
- C1- generate file log
- C2- generate process log
- C3- encrypt all logs using AES algorithm
- C4- send encrypted files log to server
- C5- send encrypted processes log to server
- C6- send user image to client emailed

C. Server:

- Set (S) = fc4, c5, s0, s1, s2, s3g
- S0- decrypt all encrypted logs
- S1- send files log to client email id
- S2- send process log to client email id
- S3- maintain history of client's pc

D. Union and Intersection of project:-

- Set (C) = fc0, c1, c2, c3, c4, c5, c6g
- Set (S) = fc4, c5, s0, s1, s2, s3g
- C union S= fc0, c1, c2, c3, c4, c5, c6, s0, s1, s2, s3g
- C intersection S = c4, c5

Vein Diagram:

Following figure shows the interaction of the project module with each other . we have shown this interaction by using set theory.

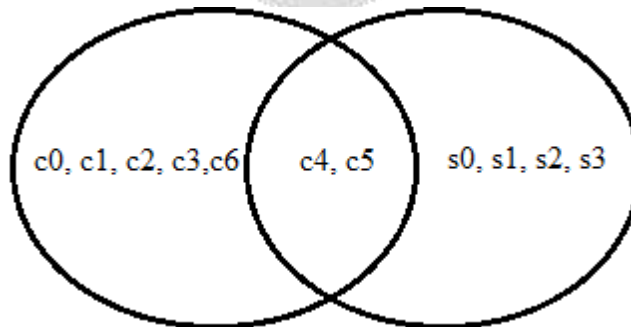


Figure 2

5. RESULT



Figure -3: Server Screen

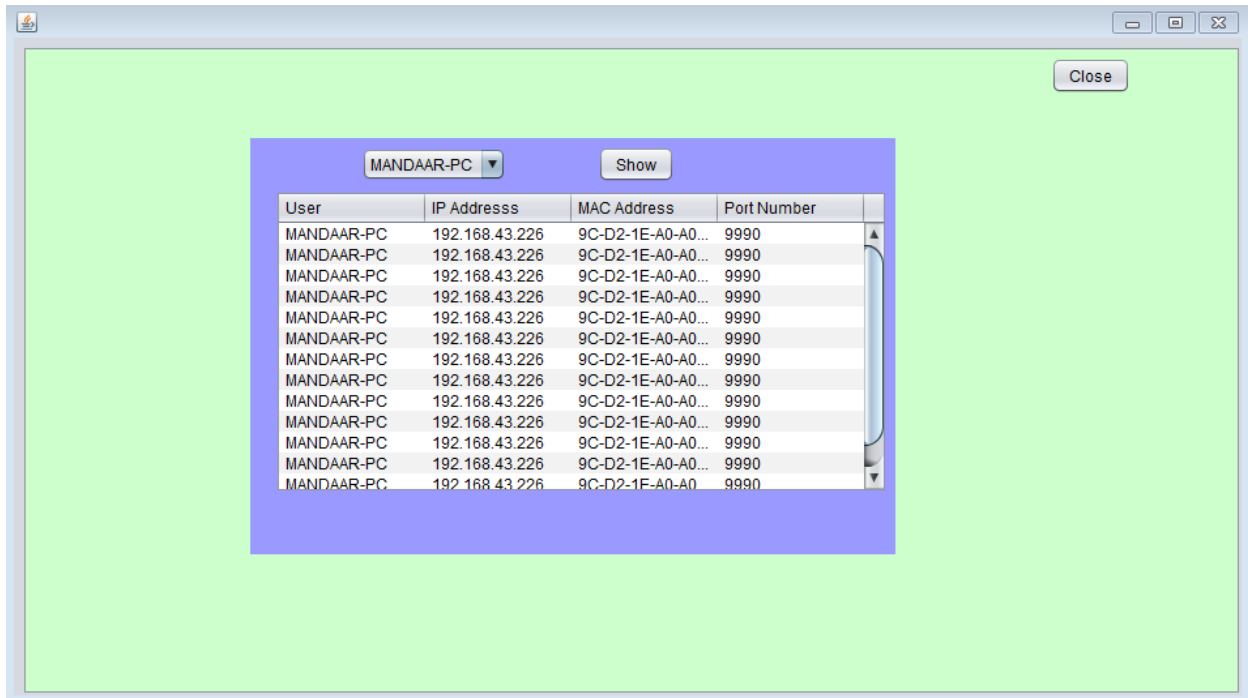
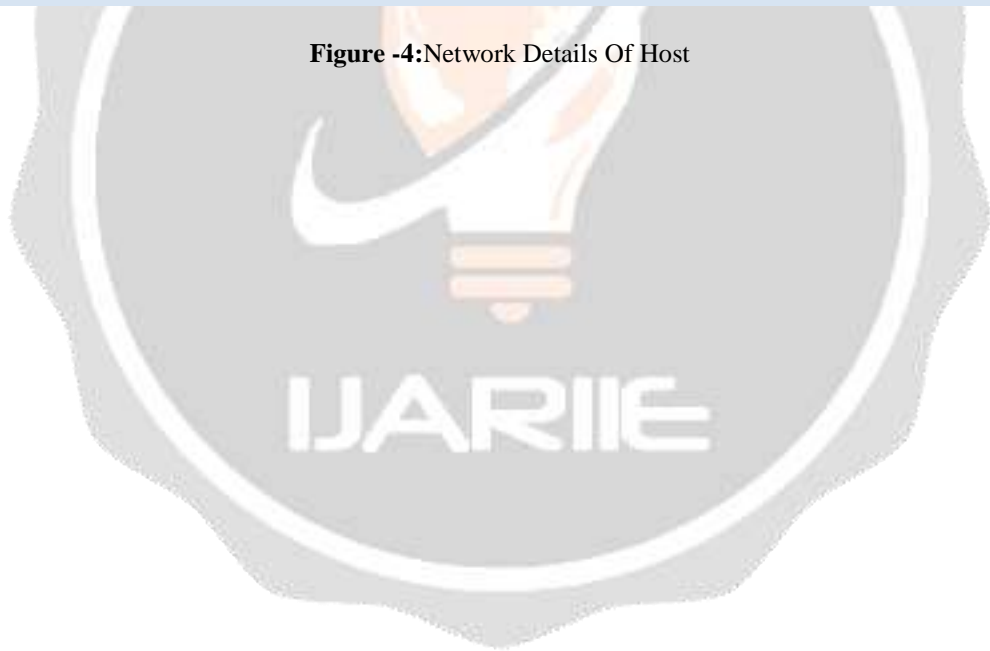


Figure -4:Network Details Of Host



19/06/2017

Alert Search Option:

From: Jun 1, 2014 To: Jun 19, 2017

Real Time Monitoring

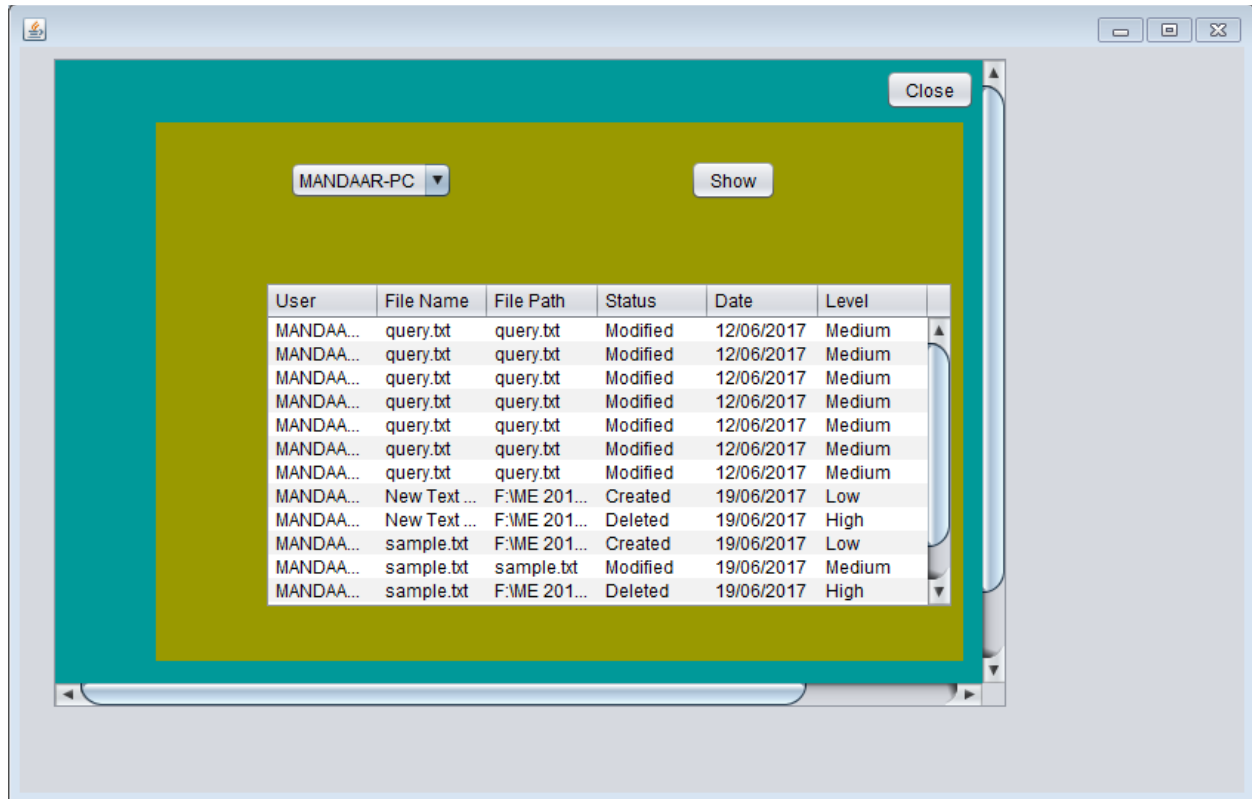
Minimum Level: Low

Max Alerts: 5 User: MANDA...

Search

File Id	File Name	File Location	Status	Date	User Name
449	New Text Docum...	F	Created	19/06/2017	MANDAAR-PC
451	sample.txt	F	Created	19/06/2017	MANDAAR-PC
454	samples.txt	F	Created	19/06/2017	MANDAAR-PC

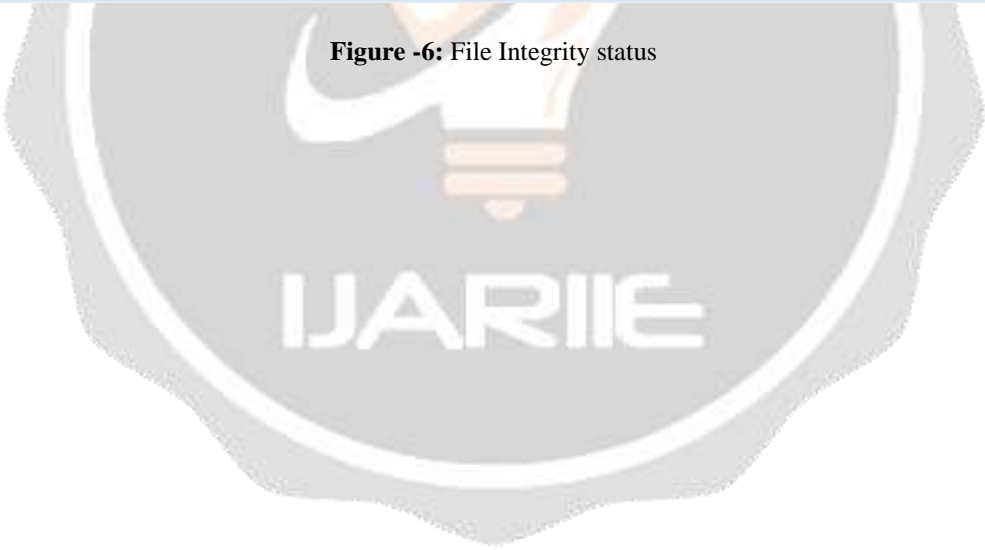
Figure- 5: File Directory Status



The screenshot shows a window titled 'MANDAAR-PC' with a 'Show' button and a 'Close' button. Below these is a table with the following data:

User	File Name	File Path	Status	Date	Level
MANDAA...	query.bt	query.bt	Modified	12/06/2017	Medium
MANDAA...	query.bt	query.bt	Modified	12/06/2017	Medium
MANDAA...	query.bt	query.bt	Modified	12/06/2017	Medium
MANDAA...	query.bt	query.bt	Modified	12/06/2017	Medium
MANDAA...	query.bt	query.bt	Modified	12/06/2017	Medium
MANDAA...	query.bt	query.bt	Modified	12/06/2017	Medium
MANDAA...	query.bt	query.bt	Modified	12/06/2017	Medium
MANDAA...	New Text ...	F:\ME 201...	Created	19/06/2017	Low
MANDAA...	New Text ...	F:\ME 201...	Deleted	19/06/2017	High
MANDAA...	sample.bt	F:\ME 201...	Created	19/06/2017	Low
MANDAA...	sample.bt	sample.bt	Modified	19/06/2017	Medium
MANDAA...	sample.bt	F:\ME 201...	Deleted	19/06/2017	High

Figure -6: File Integrity status



User	IP Addresss	MAC Address	Port Number	Date	Time	Processes
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	10:37:08	TeamViewer...
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	11:12:01	TeamViewer...
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	11:27:22	
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	11:27:22	
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	11:29:41	
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	11:30:58	
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	11:43:02	TeamViewer...
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	11:50:47	TeamViewer...
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	11:56:54	TeamViewer...
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	12:00:56	TeamViewer...
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	12:00:56	TeamViewer...
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	12:01:50	TeamViewer...
ACE2-PC	192.168.1.109	00-21-97-8F...	9990	11/04/2015	12:07:44	TeamViewer...

Figure -7: Process Log On Host Machine



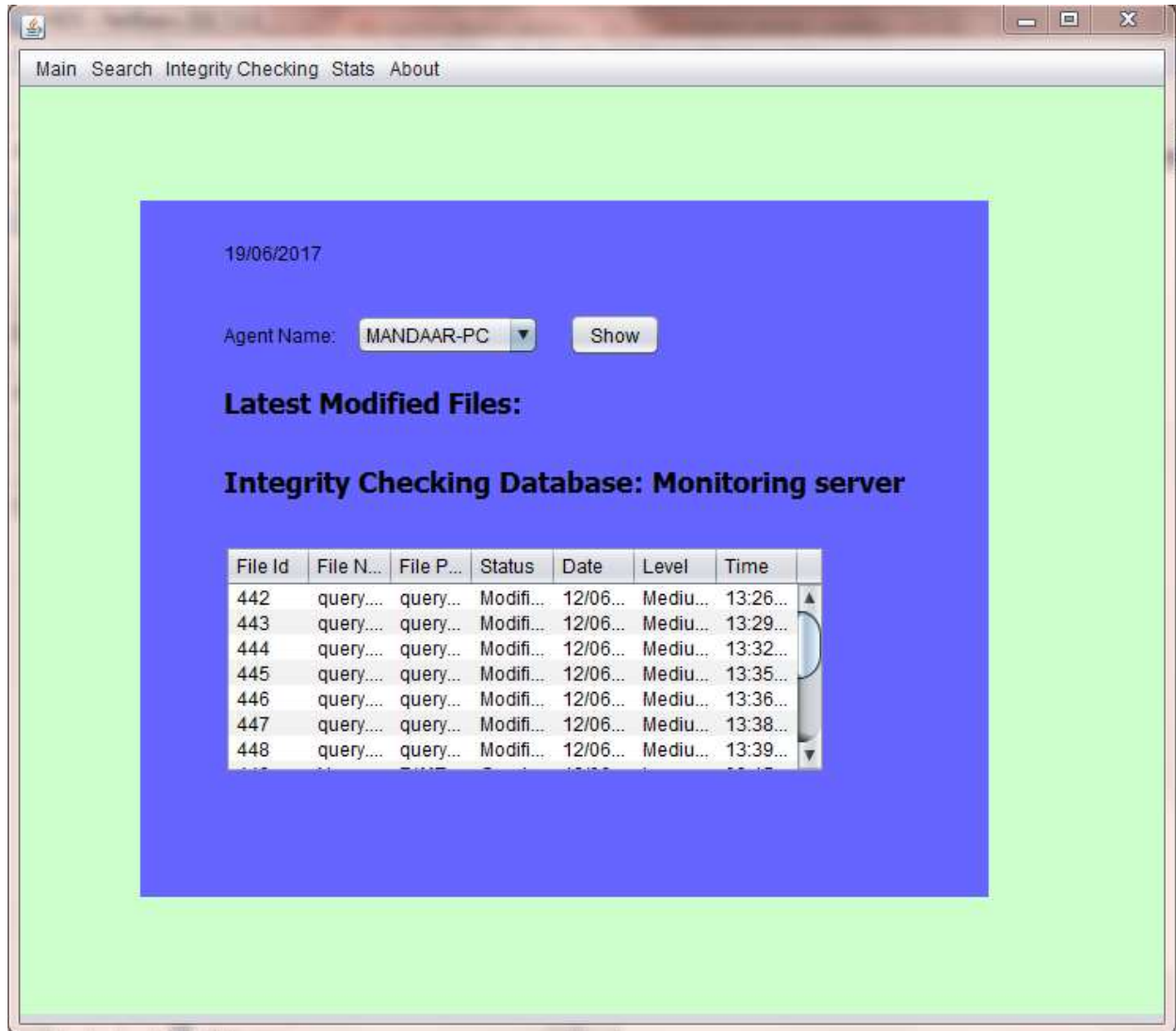


Figure- 8 : Modified Files From Host Machine



Figure -9 : Intruder Image Captured And Sent On Mail

6. RESULT ANALYSIS

Result Description	Expected Output	Actual Output
As per the proposed system working, if any malicious insider is trying to do the black listed operations or unethical activities as per admin's norms, his/her details should be logged and sent to admin for review.	The proposed Internal Intrusion Detection and Prevention system must emphasize on tracking user actions on any files or system calls made on host machines in order to determine the internal intrusion	In proposed system, the user when performs any un allowed operation such as deleting a file or calling system call processes which are black listed or not in white list of allowed processes, the users identity such as Captured image, IP address, mac address and the operation done (intrusion done) is sent to admin via mail id and also is simultaneously stored in server database for further log analysis

7. PARAMETER EVALUATION

Features	Image Capture	MAC Tracking	File Tracking	System Call Logs	RealTime Update	Key Logging
Existing Systems	✗	✗	✓	✗	✓	✓
Proposed System	✓	✓	✓	✓	✓	✓

8. CONCLUSION

The proposed system has employed an approach that makes use of data mining and analysis techniques to identify the various system call patterns for a user. The frequency of the SC calls is logged into files is computed, the most commonly used SC-patterns are filtered out, and then a user's profile is created to generate the black list and the white list of SC. By comparing the patterns with the previous patterns in the database, the IIDPS system identifies the attackers and resists them from doing the un-allowed System Calls. The experimental results depict the efficiency of the system to be 94% which indicates the IIDPS can assist system administrators to point out an insider or an attacker in a closed environment. The future scope of the system is far more wider as it can be deployed over LANS, WANS MANs in order to cover larger area under supervision and the distributed parallel computing can be done to compute realtime investigations.

9. ACKNOWLEDGEMENT

All faith and honor to the GOD for his grace and inspiration. I would like to thank all my Friends and Family members they were always been there to support me. I sincerely thanks to my Department Head, PG coordinator and all other staff members to give me the guidelines for this paper.

10. REFERENCES

- [1] 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.
- [2] 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.
- [3] Q.Wang, L.Vu, K.Nahrstedt, and H. Khurana, "MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1-5.
- [4] A.Garcia, R.Monroy, L.A.Trejo, and C.Mex-Perera, "Analyzing log files for postmortem intrusion detection," *IEEE Trans. Syst., Man, Cybern., Part C: Appl. Rev.* vol.42, no. 6, pp. 1690-1704, Nov.2012.
- [5] M.A.Qadeer, M.Zahid, A.Iqbal, and M.R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in *Proc. Int. Conf. Commun. Softw. Netw. Singapore*. 2010, pp. 313-317.
- [6] S.O'Shaughnessy and G.Gray, "Development and evaluation of a data

set generator tool for generating synthetic log files containing computer attack signatures," *Int. J. Ambient Comput. Intell.* , vol. 3, no. 2, pp. 64-76, Apr. 2011.

[7] S.X.Wu and W.Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Appl. Soft Comput.* , vol. 10,

[8] 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.

[9] J.T. Giffin, S.Jha, and B.P.Miller, "Automated discovery of mimicry attacks," *Recent Adv. Intrusion Detection* , vol. 4219, pp. 41-60, Sep. 2006.

[10] U.Fiore, F.Palmieri, A.Castiglione, and A. D.Santis, "Network anomaly detection with the restricted Boltzmann machine," *Neurocomputing* , vol. 122, pp. 13-23, Dec. 2013.

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

