ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 10, October 2016**

# A Survey on Hybrid Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques

Roshani Lokhande[1], Susnata Das[2], Sukhada Sabnis[3,] Shital Gawade[4]

Student, Department of Computer Engineering, JSPM's ICOER. Wagholi, Pune, India

**ABSTRACT**: In today's technology, there are new attacks are emerging everyday due to that the system makes the insecure even the system wrapped with number of security measures. To detect the intrusion, an Intrusion Detection System (IDS) is used. To detect the intrusion and respond 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 fails to preserve the evidences against the attack. New security strategy is very much needed to maintain the completeness and reliability 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 administrator followed by invoke the digital forensic tool Once an IDS detects an intrusion. To prove the damage Captured image can be used as evidence in the court of law.

**KEYWORDS**: Intrusion Detection Systems, Digital Forensic, Logs, Cryptography.

## I. INTRODUCTION

Now a day, to safeguard the organization electronic assets, Intrusion Detection System (IDS) is crucial requirement. To determine whether the traffic is malicious or not Intrusion detection is a process of monitor and analyzes the traffic on a device or network. It can be a software or physical appliance that monitors the traffic which violates organization security policies and standard security practices. To detect the intrusion and respond in timely manner as a result risks of intrusions is diminished it continuously watches the traffic. Based on the deployment IDS broadly classified into two types i.e. Host based Intrusion Detection System (HIDS) and Network based Intrusion Detection System (NIDS). Host-based Intrusion Detection System is configured on a particular system/server. It continuously monitors and analyses the activities the system where it is configured. Whenever an intrusion is detected HIDS triggers an alert. For instance, when an attacker tries to create/modify/delete key system files alert will be generated. Major advantages of the HIDS that it analyzes the incoming encrypted traffic which cannot be detected NIDS. To detect the attack like Denial of Service (DoS) attacks, Port Scans, Distributed Denial of Service (DDoS) attack, etc Network Intrusion Detection System (NIDS) continuously monitor and analyze the network traffic. To classify as malicious or non-malicious traffic it examines the incoming network traffic. If any predefined patterns or signatures of malicious behavior are present it re-assembles the packets, examine the headers/payload portion and determine [6].

Recently "Intrusion investigations with data-hiding for computer Log-file Forensics" technique has been proposed [1]. In this approach, log file is stored in two different places as well as in two different forms. On target host the Log file in plain text from is stored and a copy of same log file is stored in another host called log manager and it is hidden in image using steganography. IDS running on target host detects an intrusion and sends an alert message to security administrator about the intrusion when an intruder tries to alter log file on target host. Security administrator use the stego image to extract log file and compares it with log file available in the target host To verify whether the intrusion occurred or not. Intrusion is confirmed If the result of the comparison is unequal else not. Forensic technique is unable to capture the evidence of the attack is the major limitation of this approach. So to preserve the log file damage for forensic analysis, it is not possible and to prove in the court of law, evidence cannot be collected immediately against the attack. In this work automated Digital Forensic Technique with Intrusion Detection System is proposed to overcome this limitation. Because the current IDS are not designed to collect and protect evidence against the attack

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

this new technique is crucial requirement. Digital forensics plays an important role by providing scientifically proven methods to gather, process, interpret and use digital evidence to bring a decisive description of attack.

## II. EXISTING SYSTEM

The proposed approach is as shown in Fig. 1. The functions of each entity are described as follows: Target Host: The target host is a system in which crucial data (i.e. log file) is stored. 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 intrusion; sends an alert message to security centre as well as log server. Further, it invokes the digital forensic tool to capture the state of the system (RAM image and log file image). Newly captured log file image is compared with previous log file image to confirm the intrusion. Comparison result equals to non-zero confirm intrusion else no intrusion. RAM image is analysed to determine the type of the intrusion.

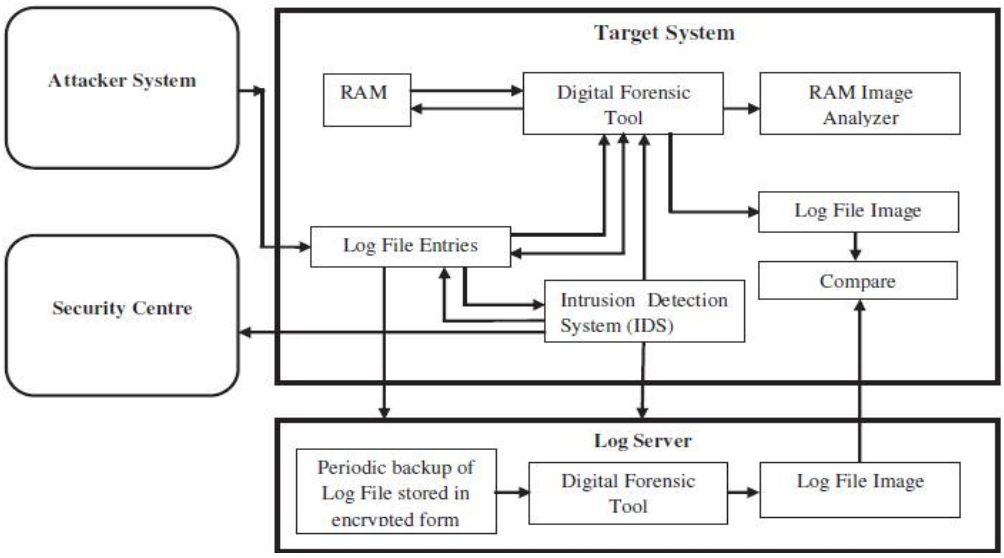


Fig.1 Automated Digital Forensic Technique with Intrusion Detection System Log Server

It stores the copy of the log file in an encrypted form. Encryption key maintained only by the log server and it kept secret. Periodically back up of the Target host log file is taken and it is stored on the log server. Upon receiving the log file as a backup, it encrypts the received log file and stores within it. Whenever log server receive a alert message from target host, it decrypts the log file, computes the image of the decrypted log file using digital forensic tool and sends to target host to perform the comparison.
Security Centre: This is the system used by the security administrator to monitor the alerts generated by IDS. It receives alerts from Target Host. Flow of the entire proposed work is shown in figure 2.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 10, October 2016**

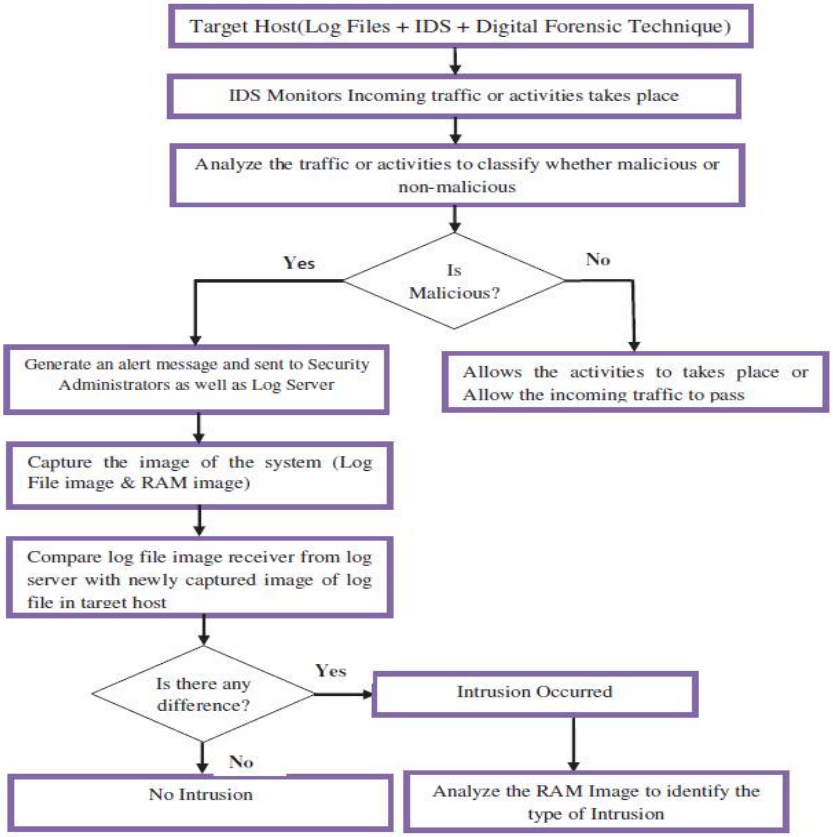


Figure 2. Flow chart of the proposed work

## IV. PROPOSED SYSTEM

In this approach, log file is stored into two different forms as well as in two different places. Log file in plain text from is stored on target host and a copy of same log file is stored in another host called log manager and it is hidden behind an image using steganography. 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.

### *A. TARGET HOST*

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 intrusion; sends an alert message to security centre as well as log server. Further, it invokes the digital forensic tool to capture the state of the system (RAM image and log file image). Newly captured log file image is compared with previous log file image to confirm the 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. LOG SERVER:*

It stores the copy of the log file in an encrypted form. Encryption key maintained only by the log server and it kept secret. Periodically back up of the Target host log file is taken and it is stored on the log server. Upon receiving the log file as a backup, it encrypts the received log file and stores within it. Whenever the log server receives an alert message

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

from target host, it decrypts the log file, computes the image of the decrypted log file using digital forensic tool and sends it to the target host to perform the comparison. The main job of the Log server is encryption and decryption of log files such that the intruder doesn't have access to them. If the intruder gets to know the location and condition of the log files then their safety comes under scrutiny. The most important part will be the key. The key that is used to encrypt and decrypt the log files shall only be available with the owner and nobody else. It shall be provided at the time of delivering the software as a complete product.

### *C. SECURITY CENTRE:*

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.


Figure 3. File Integrity

The second activity performed by user is key log. In key log, if any user typed any key on keyboard that keys will stored in text file in project folder. Also that typed keys are send to the server. So that server will know which keys are pressed on client machine by user. After that server send keys to the client mail id. So that client will easily know which keys are pressed on his machine.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 10, October 2016**

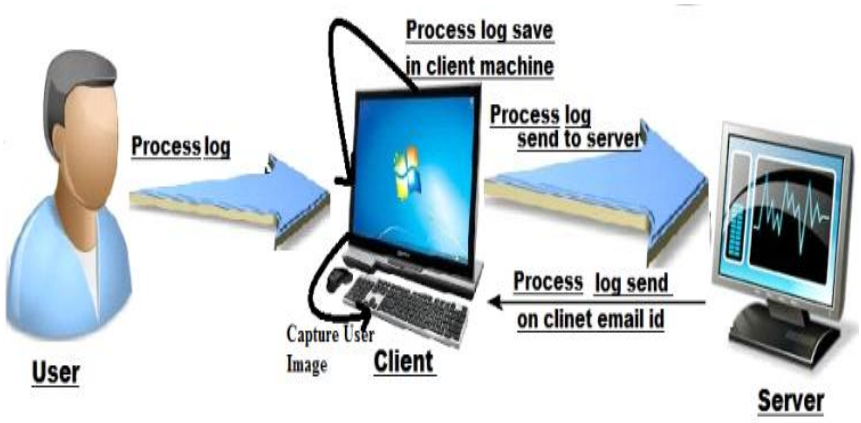


Figure4. Process log

As well as these activities, one main action performed by our project is, if any user perform any activity on client machine, then system will take picture of that user by web cam and send his image to the clients email id. So that client will easily know which user was performing activities on his machine.

## V. APPLICATIONS

1. System can be used in college.
2. System also used in organizations.
3. System also useful in the cyber cafes.
4. System also used for the personal use.

## VI. FUTURE WORK

This system can be used to detect the host intrusion detection where host machine comprises the confidential files. Attackers can attack on host machine that attacks would be detect by the system and updated files can be recovered by system. This system can detect the files modification and also prevent the file modification. If files deleted from the host machine permanently then system can recovered the files.

## VII. CONCLUSION

In this work, intrusion detection system is proposed. IDS are used to determine the intrusion. We can easily detect which activities are performed by user. So that we can recover that all modified file. By using web cam system take pictures of user which performs malicious activities and save that activity in folder and send that activity log and image of user on clients email id so that we know this particular user. So that our system is very effective and efficient for detecting intrusion of system.

## REFERENCES

1. Fang-YieLeu,Kun-Lin Tsai " A Internal Intrusion Detection and Protection System by Using data Mining andForensic Techniques"
2. Ya-Ting Fan1 and Shiuh-Jeng Wang, "Intrusion Investigations with Data-hiding for Computer Log-file Forensics", IEEE 2010.
3. R. Araeteh, M. Debbabi, A. Sakha, and M. Saleh, "Analyzing multiple logs for forensic evidence," Digital Investigation 4S, pp, 82- 91, 2007.
4. J. Herrerias and R. Gomez, "A log correlation model to support the evidence search process in a forensic investigation," Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07), pp. 31-42, 2007.
5. Bhagyashree Deokar, Ambarish Hazarnis, " Intrusion Detection System using log files and reinforcement learning", International Journal of Computer Applications (0975 – 8887) ,May 2012
6. Karen Scarfone& Peter Mell, National Institute of Standards and Technology (NIST) Special Publication 800-94 , " Guide to Intrusion Detection and Prevention Systems", Feb 2007.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 10, October 2016**

7. Karen Kent, Tim Grance, Hung Dang, NIST Special Publication 800- 86 , "Guide to Integrating Forensic Techniques into Incident Response" , Aug 2006.
8. D. Zhu and J. Xiao, "R-tfidf, a Variety of tf-idf Term Weighting Strategy in Document Categorization," in *Proc. Int. Conf. Semantics, Knowledge Grids*, Beijing, China, Oct. 2011, pp. 83–90. S. E. Robertson, S. Walker, M. M. Beaulieu, M. Gatford, and A. Payne, "Okapi at TREC-4," in *Proc. 4th text Retrieval Conf.*, 1996, pp. 73–96.
9. S. Yu, K. Sood, and Y. Xiang, "An effective and feasible traceback scheme in mobile internet environment," *IEEE Commun. Lett.*, vol. 18, no. 11,pp. 1911–1914, Nov. 2014.
10. B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," *IEEE Syst. J.*, vol. 7, no. 2,pp. 262–274, Jun. 2013.
11. S. C. Arseni, E. C. Popovici, L. A. Stancu, O. G. Guta, and S. V. Halunga, "Securing an alerting subsystem for a keystroke-based user identification system," in *Proc. Int. Conf. Communication*., Bucharest, Romania, 2014, pp. 1–4.
12. G. M. Amdahl, "Validity of the single processor approach to achieving large scale computing capabilities," in *Proc. AFIPS Spring Joint Computer*., New Brunswick, NJ, USA, 1967, pp. 1–4.
13. M. Minsky, "Form and content in computer science," *J. ACM*, vol. 17, no. 2, pp. 197–215, Apr. 1970.