Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 8, Issue 4, April-2021

CRIME DETECTION SYSTEM USING DATA MINING AND FORENSIC TECHNIQUES

Vishakha More[1], Vivek Varpe[2], Jayan Raut[3], Gauri Baraskar[4]

vishakhamore252@gmail.com[1], vivekvarpe7@gmail.com[2], jayanraut@gmail.com[3], gauribaraskar1898@gmail.com[4],

Information Technology, Dr D Y Patil Institute of Engineering and Technology, Ambi, Pune[1]
Information Technology, Dr D Y Patil Institute of Engineering and Technology, Ambi, Pune [2]
Information Technology, Dr D Y Patil Institute of Engineering and Technology, Ambi, Pune [3]
Information Technology, Dr D Y Patil Institute of Engineering and Technology, Ambi, Pune [4]

Abstract ***—The system proposes a security system, named the Crime Detection System using Data Mining and Forensic Techniques (CDSDM) at system call (SC) level, which creates personal profiles for users to keep track of their usage habits as the forensic features. The CDSDM uses a local computational grid to detect malicious behaviors in a real-time manner the proposed work is regarded with Digital forensics technique and crime detection mechanism. The number of hacking and crime incidents is increasing each year. The system designed Crime Detection System (CDS) that implements predefined algorithms for identifying the attacks over a network. Therefore, in this project, a security system, named the Crime Detection System using Data Mining (CDSDM), is proposed to detect insider attacks at SC level by using data mining and forensic techniques. By analyzing the corresponding system calls the system can identify the user forensic features to improve the accuracy of crime detection and will able to port the CDSDM to a parallel system to shorten detection response time.***

INTRODUCTION

In this digital era, the computer and its subsidies have become so handy that all our day-to-day life is dependent on it. But due to the increase in harmful activities, we are asked for authentication at each and every step. We need to login into the system or any application or any network, we require and need to successfully pass through the authentication step. But in order to remember and store passwords, we have a human tendency to keep a simple or mostly a common password or pattern for every authentication purpose. This increases the chances of intrusion. Security to date remains one of the biggest challenges and continuous efforts are taken to improve it. Still, we face a large number of attacks such as DOS attack, phishing attack, eves dropping attack, spa email attack, Trojan horse attack, etc. All these attacks are easy to be detected at system calls i.e. operating system level.

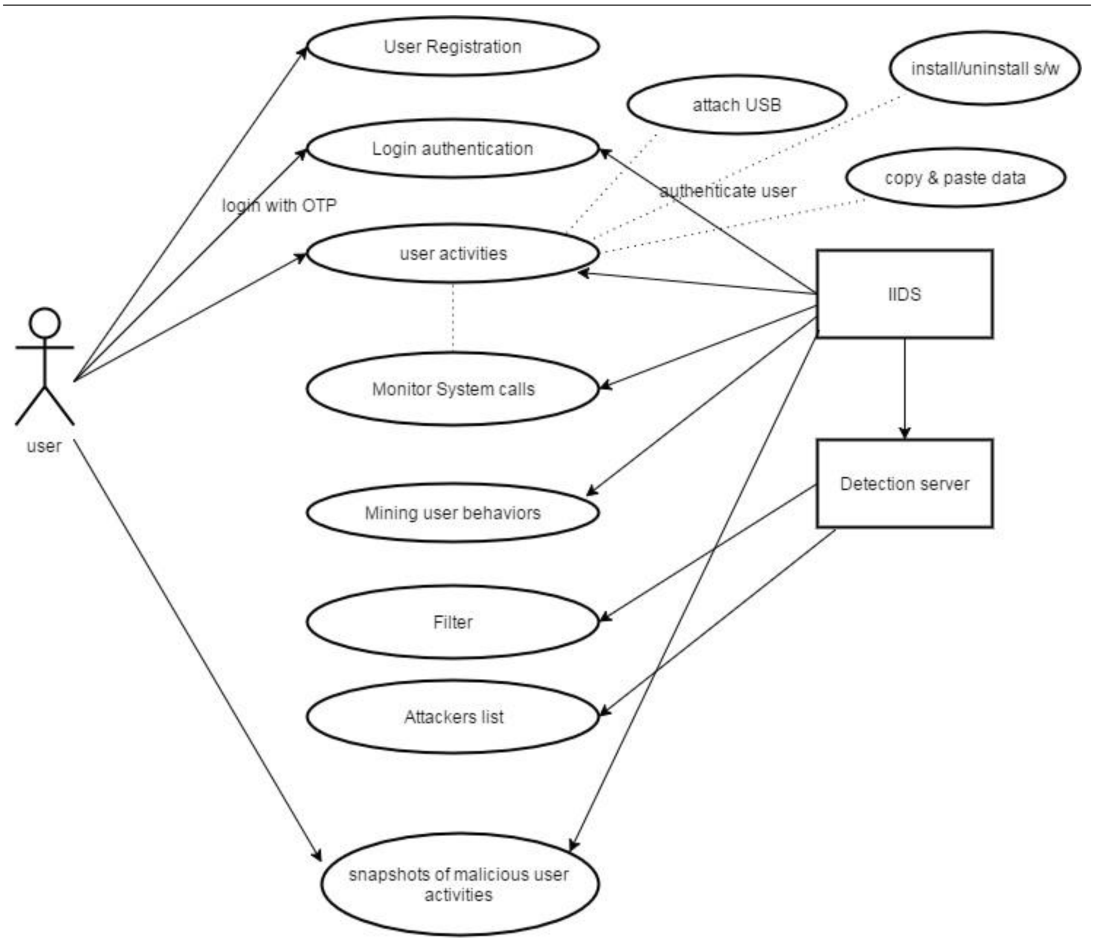
PROBLEM STATEMENT

Today, small and medium-sized enterprises (SME) can be considered as the new big target for cyber attacks, while cybercrime prevention is often neglected within their environment. We can many small-scale firms, where no advanced security measures are taken to protect any confidentiality of the data stored on the system, so we are proposing the system for crime detection and analysis.

PROPOSED SYSTEM

This System presents data mining techniques to detect the crime and analysis. We are using the Decision tree algorithm to identify the various possible ways of crime. At the initial product, our system will identify the 3 most important crimes. The system will continuously keep on monitoring the activity of the system user and keep track of all the activities it has been permitted while creating the profile by the admin of the system. So with the help of a decision tree algorithm, we will able to detect any internal fraud and crime. So if the user does not has permission to use the USB port of the system, but still, if he tries to attach the USB, then at that moment of time system will detect the crime and alert the admin.

Every organization, they have some share path/location where all the confidential documents are stored and preserved. It is a store at a centralized location so that the intended user can access and use it if required. If the registered user of the system tries to modify the files available on share location when users modify rights are disables by admin, then the system will detect this activity and will generate the alert to admin. The system will also monitor the user activities like if he/she tries to change the system-related changes in the control panel. And if found any suspicious then it will take the screenshot of the user through the webcam and will send the email to the admin of the system.



CONCLUSION

We are going to develop a system that prevents and alerts intrusion attacks and our system. We have various modules that store and keep track of all the users in the system. All the user's activities will be monitored and get recorded in a log file. If the system finds abnormal activities i.e. the activity which matches with the activity is restricted for the user, then the system will generate an alert message to the admin. The system has a self monitoring function that means it continuously keeps on monitoring the user activities.

REFERENCES

[1] 1]Chen, S. Abdelwahed, and A.Erradi "shielding systems by using the module-based approach." ACM Cloud Autonomic Comput. Miami, FL, USA, 2013, pp. 1–10.

[2] Q. Wang, L. Vu, K. Nahrstedt, & H. Khurana " illegal nodes identification system in network coding based stream," in Proc. IEEE INFOCOM, San Diego, CA, USA.

[3] H. S. Kang and S. R. Kim, A new logging-based IPtraceback approach using data mining techniques, J.Internet Serv. Inf. Security, vol. 3, no. 3/4, pp.7280, Nov. 2013.

[4] C. Yue and H. Wang, Bogusbiter " To stop unofficial & illegal strikes and activities by using A explicit protection," ACM Trans. Int. Technol., vol. 10, no. 2, pp. 1–31, May 2010.