Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 2, February 2021, pg.82 – 85

Crime Detection System using Data Mining

Jadhav Payal U.; Chikhale Rasika D.; Khokrale Pragati V.; Jadhav S. B.

DOI: 10.47760/ijcsmc.2021.v10i02.013

Abstract – Data mining plays the key role in crime analysis. There are various number of different algorithm in previous research papers like virtual identifier, pruning strategy, support vector machines and apriori algorithms. "VID" (Virtual ID) is to find relationship between record. Then the "Apriori algorithm is used to around six hundred seconds to detect a mail bomb attack. Which is quite fast as we wanted and its very useful to achieve our goal. We used the 'crime mapping analysis based on "KNN" (K-Nearest Neighbor) algorithm to simplify this process and the crime mapping is very essential research area to concentrate on because we can identify the most frequently crime occurring zone with the help of data mining techniques. We use the following steps to reduce the crime rate:

i. Collect crime data.
ii. Group data.
iii. Clustering.
iv. Forecasting the data.

Keywords:- Data Mining, Data Security, System Protection, Shared Location Security, Cyber Security, User Privacy

I. INTRODUCTION

Crimes are happens most and large numbers of times in the world. There are a lots of different types of crimes that happen like robbery, theft of vehicles, jewelleries, etc. As crime increase the investigation process gets longer and more complicated. The used of information mining methods helps in resolving most complicated criminal cases. Then we found the best method for resolving problem is "Crime analysis with crime mapping". It helps in the reduction and decreasing the number of crimes. In day today life securing the computer system/machine using detecting system has been the important task for companies. As we can see there are various types of algorithms. "Decision tree" help in areas like machine learning and pattern reorganization. We are using decision tree algorithm to identify the three most important crimes. With the help of this we are able to detect any internal fraud and crime. For e.g. unwanted sites like social media sites, unauthorized sites, USB ports etc. are tries to use by user or employees, then at that movement of time system will detect the crime and alert the admin.

Many people don't know how to use data mining and where, when it can be used. It providing many benefits, one of it is "Privacy". Now a days each message which is send and received are stored in particular place. In case privacy is most important. Warehouse are used to stored data for years.

II. RELATED WORK

In this digital age, computer and its subsidies have become so handy that all our day to day life is dependent on it. But due to increased chances of attacks we are asked for authentication at each and every step. We need to login into system or any application or any network, we require and need to successfully pass through authentication step. But in order to remember and store password, we have human tendency to keep a simple or mostly a common password or pattern for every authentication purpose. This in turn increases the chances of intrusion. Security till date remains one of the biggest challenges and continuous efforts are taken to improve it. Still we face with 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 call i.e. operating system level.

[1] Crime Analysis Mapping, Intrusion Detection - Using Data Mining paper describes Data Mining plays a key role in Crime Analysis. There are many different algorithms mentioned in previous research papers, among them are the virtual identifier, pruning strategy, support vector machines, and apriori algorithms. VID is to find relation between record and vid. The apriori algorithm helps the fuzzy association rules algorithm and it takes around six hundred seconds to detect a mail bomb attack. In this research paper, we identified Crime mapping analysis based on KNN (K – Nearest Neighbor) and ANN (Artificial Neural Network) algorithms to simplify this process. Crime Mapping is conducted and Funded by the Office of Community Oriented Policing Services (COPS).

[2] Upon an intrusion, security staff must analyze the IT system that has been compromised, in order to determine how the attacker gained access to it, and what he did afterward. Usually, this analysis reveals that the attacker has run an exploit that takes advantage of a system vulnerability. Pinpointing, in a given log file, the execution of one such an exploit, if any, is very valuable for computer security. This is both because it speeds up the process of gathering evidence of the intrusion, and because it helps taking measures to prevent a further intrusion, e.g., by building and applying an appropriate attack signature for intrusion detection system maintenance. This problem, which we call.

[3] Currently, most computer systems use user IDs and passwords as the login patterns to authenticate users. How- ever, many people share their login patterns with coworkers and request these coworkers to assist co-tasks, thereby making the pattern as one of the weakest points of computer security. Insider attackers, the valid users of a system who attack the system internally, are hard to detect since most intrusion detection systems and firewalls identify and isolate malicious behaviors launched from the outside world of the system only. In addition, some studies claimed that analyzing system calls (SCs) generated by commands can identify these commands, with which to accurately detect attacks, and attack patterns are the features of an attack Therefore, in this paper, a security system, named the Internal.

[4] The mouse dynamics biometric is a behavioral biometric technology that extracts and analyzes the movement characteristics of the mouse input device when a computer user interacts with a graphical user interface for identification purposes. Most of the existing studies on mouse dynamics analysis have targeted primarily continuous authentication or user re-authentication for which promising results have been achieved. Static authentication (at login time) using mouse dynamics, however, appears to face some challenges due to the limited amount of data that can reasonably be captured during such a process. In this paper, we present a new mouse dynamics analysis framework that uses.

[5] Supervisory Control and Data Acquisition (SCADA) systems, which are widely used in monitoring and controlling critical infrastructure sectors, are highly vulnerable to cyber attacks. Current security solutions can protect SCADA

systems to monitor SCADA system performance, and proactively estimate upcoming attacks for a given system model of a physical infrastructure. We also present the feasibility of intrusion detection.

III. EXITING SYSTEM

In this digital age, computer and its subsidies have become so handy that all our day to day life is dependent on it. But due to increased chances of attacks we are asked for authentication at each and every step. We need to login into system or any application or any network, we require and need to successfully pass through authentication step. But in order to remember and store password, we have human tendency to keep a simple or mostly a common password or pattern for every authentication purpose. This in turn increases the chances of intrusion. Security till date remains one of the biggest challenges and continuous efforts are taken to improve it. Still we face with 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 call i.e. operating system level.

IV. PROPOSED SYSTEM

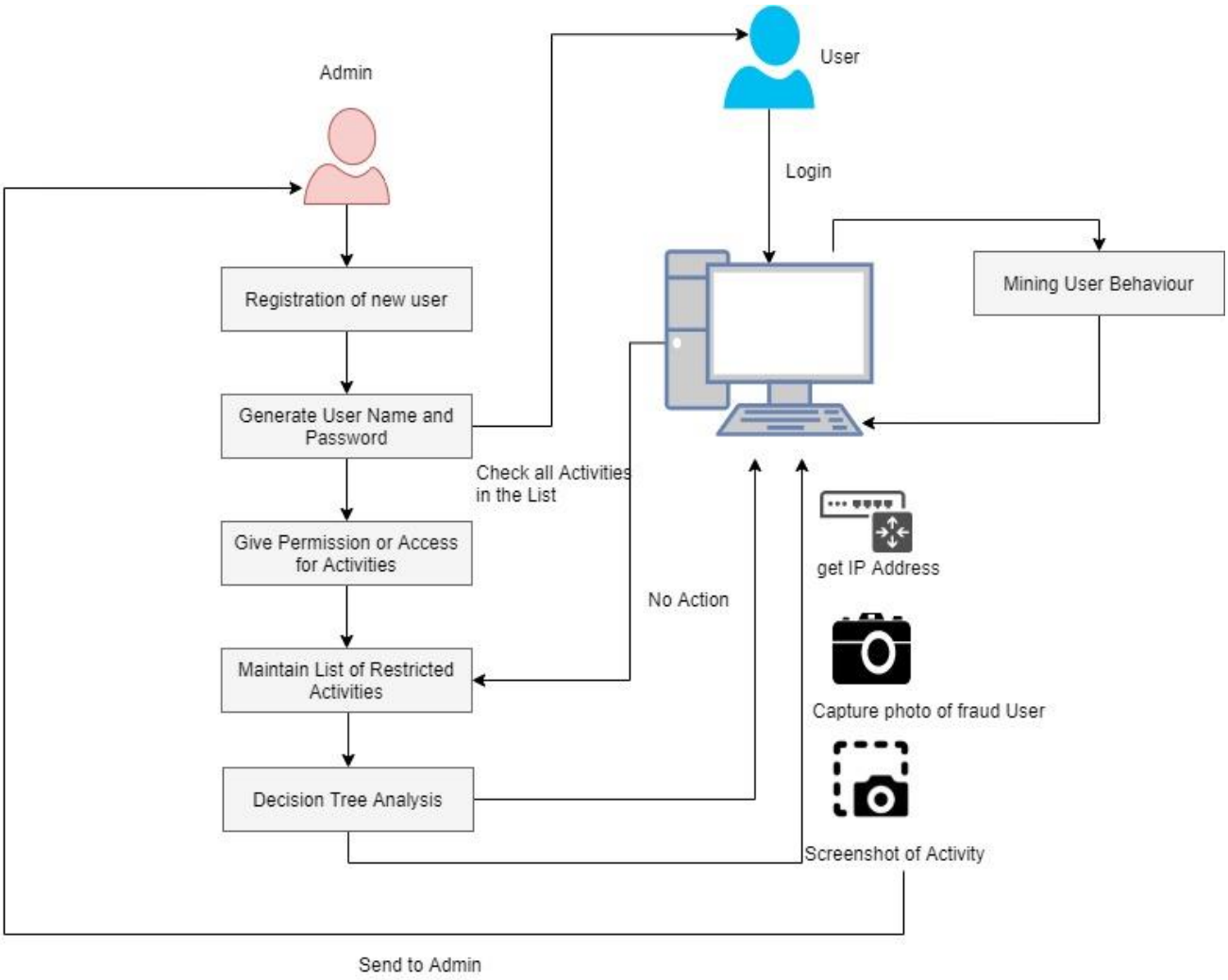

Figure 1: Architecture diagram

Admin plays the important role in our Crime detection system. Admin gives the all details to new user which are required for the new user. Crime mapping helps in understanding using concepts and practice of crime analysis in assisting police and helps in decreasing the number of crimes and literally stopping crime disordering using “Data Mining”. We are used

data mining tools involved using KNN (K-Nearest Neighbor). We are using a java language. In java random access classes are used to generate a series of random numbers. The generatorOTP(int) method use in length of OTP as parameter. We have created an array of characters which will store to desired OTP. Each execution of the program generates unique OTP.

We start from the root of the decision trees for predicting a class label for a record. We compare the values of the root attribute on the basis of comparisons, we follow the branch corresponding to that value and jump to the next node. Then we used to take a or capture snap of the unauthorized employees or users we load the OpenCV native library while writing java code using OpenCV library, the first step you need to do is to load the native library of OpenCV using the loadLibrary(). Then loading this OpenCV native library we also read frames from the camera using the read() method of the photo capture class. With that we are also going to take screenshot of the main screen for that we are using create ScrrenCapture () method from the Robotclass. We also used tools to set a dimension of snapshot image by using the parameters we give the format like we using the .bmp format but with that other are available .png, .jpg, etc.

V. CONCLUSION

The crime detection system using data mining employs data mining and forensic techniques to identify the user behavioral patterns for a user. The time that a habitual behaviour pattern appears in the users log file is counted, the most commonly used patterns are filtered out, and then a users profile is established. By identifying a users behaviour patterns as his/her computer usage habits from the users current input, the system resists suspected attackers. The future work of insider attack detection research will be about collecting the real data in order to study general solutions and models. It is hard to collect data from normal users in many different environments. It is especially hard to acquire real data from a masquerader or traitor while performing their malicious actions. when data were available it is more easily controlled and reach under the set of regulation rather than effective and valuable data for research.

REFERENCES

[1] C. Yue Int. Technol., vol. 10, no. 2, pp. 131, May 2010.

[2] Q. Chen, S. Abdelwahed, and A. Erradi, A model-based approach to self-protection in computing system, in Proc. ACM Cloud Autonomic Comput. Conf., Miami, FL, USA, 2013, pp. 110.

[3] H. Lu, B. Zhao, X. Wang, and J. Su, DifiSig: Resource dier- entiation based malware behavioral concise signature generation, Inf. Commun. Technol., vol. 7804, pp. 271284, 2013.

[4] Z. Shan, X.Wang, T. Chiueh, and X. Meng, Safe side eects commit- ment for OS-level virtualization, in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111120.

[5] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, Detecting web based DDoS attack using MapReduce operations in cloud computing environ- ment, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 2837, Nov. 2013.

[6] 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. 15.

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

