CRIMINAL BEHAVIOUR ASSESSMENT MAPPING INTRUSION IDENTIFICATION USING PATTERN RECOGNITION

[1] Mrs.K.VIJAYALAKSHMI,[2] K. PREETHIKA,[3] J. JYOTHISHWAR,[4] K. MANIKANTH,[5] K. GEETHA

[1] Assistant Professor,[2345] B.Tech Students

Department Of Computer Science & Engineering

Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

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. 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. Evidence-based research helps in analyzing crimes. We calculate the crime rate based on the previous data using datamining techniques. For public safety purposes, crime mapping is an essential research area to concentrate on.

We can identify the most frequently crime-occurring zones with the help of data mining techniques. In Crime Analysis Mapping, we follow the following steps in order to reduce the crime rate: 1) Collect crime data 2) Group data 3) Clustering 4) Forecasting the data. Crime Analysis with crime mapping helps in understanding the concepts and practice of Crime Analysis in assisting police and helps in the reduction and prevention of crimes and crime disorders.

I. INTRODUCTION

Crimes are one of the most predominant problems that is happening in most of the urban areas in the world. There are a lot of different types of crimes that happen, including robbery, theft of vehicles, etc. As crime increases, the investigation process gets longer and more complicated. The use of information mining methods helps in resolving the most complicated criminal cases. One of the best methods is crime analysis with crime mapping. Crime analysis with crime mapping helps in understanding the concepts and practices of crime analysis in assisting police and helps in the reduction and prevention of crimes and

crime disorders. Evidence-based research helps in analyzing crimes. We calculate the crime rate based on the previous data using data mining techniques. Crime analysis uses quantitative and qualitative data and analytic techniques in resolving cases. For public safety purposes, crime mapping is an essential research area to concentrate on. We can identify the highest-risk crime zones with the help of data mining techniques .

Involves analyzing and identifying patterns in various forms of data to detect and prevent criminal activities, particularly in the context of cybersecurity. This approach leverages advanced algorithms and machine learning techniques to recognize anomalies or patterns indicative of malicious behavior within digital systems.. Pattern recognition algorithms then scrutinize this data, seeking irregularities or trends that may signify potential security threats or unauthorized access. The goal is to create a comprehensive map of potential criminal behavior, enabling proactive measures to thwart cyber threats. By integrating pattern recognition into intrusion identification, this methodology enhances the ability to identify subtle deviations from normal system behavior, allowing for more accurate and timely threat

detection. This approach is crucial in today's interconnected digital landscape, where cybercriminals continually evolve their tactics, making traditional security measures less effective.

II. II LITERATURE SURVEY

Intrusion detection using data mining techniques.

As the network dramatically extended, security considered as major issue in networks. Internet attacks are increasing, and there have been various attack methods, consequently. Intrusion detection systems have been used along with the data mining techniques to detect intrusions. In this work we aim to use data mining techniques including classification tree and support vector machines for intrusion detection.

In recent years, internet and computers have been utilized by many people all over the world in several fields. In order to come up with efficiency and up to date issues, most organizations rest their applications and service items on internet. On the other hand, network intrusion and information safety problems are ramifications of using internet. In other words, network intrusion is considered as new weapon of world war. Therefore, it has become the general concern of the computer society to detect and to prevent intrusions efficiently. There are many methods to strengthen the network security at the moment, such as encryption, VPN, firewall, etc., but all of these are too static to give an effective protection. However, intrusion detection is a dynamic one, which can give dynamic protection to the network security in monitoring, attack and counter-attack. Thus, Intrusion Detection System (IDS) has been applied to detect intrusion network. Intrusion Detection technology can be defined as a system that identifies and deals with the malicious use of computer and network resources. In the case of detecting data target, intrusion detecting system can be classified as host-based and network-based.

Developing custom intrusion detection filters using data mining

One aspect of constructing secure networks is identifying unauthorized use of those networks. Intrusion detection systems look for unusual or suspicious activity, such as patterns of network traffic that are likely indicators of unauthorized activity. However, normal operation often produces traffic that matches likely "attack signatures", resulting in false alarms.

Fuzzy network profiling for intrusion detection

The Fuzzy Intrusion Recognition Engine (FIRE) is an anomaly-based intrusion detection system that uses fuzzy logic to assess whether malicious activity is taking place on a network. It uses simple data mining techniques to process the network input data and help expose metrics that are particularly significant to anomaly detection. These metrics are then evaluated as fuzzy sets. FIRE uses a fuzzy analysis engine to evaluate the fuzzy inputs and trigger alert levels for the security administrator. This paper describes the components in the FIRE architecture and explains their roles. Particular attention is given to explaining the benefits of data mining and how this can improve the meaningfulness of the fuzzy sets. Fuzzy rules are developed for some common intrusion detection scenarios. The results of tests with actual network data and actual malicious attacks are described. The FIRE IDS can detect a wide-range of common attack types.

Fuzzy cognitive maps for decision support in an intelligent intrusion detection system

The health of a computer network needs to be assessed and protected in much the same manner as the health of a person. The task of an intrusion detection system is to protect a

computer system by detecting and diagnosing attempted breaches of the integrity of the system. A robust intrusion detection system for a computer network will necessarily use multiple sensors, each providing different types of information about some aspect of the monitored system. In addition, the sensor data will often be analyzed in several different ways. We describe a decision engine for an intelligent intrusion detection system that fuses information from different intrusion detection modules using a causal knowledge based inference technique. Fuzzy cognitive maps (FCMs) and fuzzy rule-bases are used for the causal knowledge acquisition and to support the causal knowledge reasoning process.

Crime pattern detection using data mining

Data mining can be used to model crime detection problems. Crimes are a social nuisance and cost our society dearly in several ways. Any research that can help in solving crimes faster will pay for itself. About 10% of the criminals commit about 50% of the crimes.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

Crime has been increasing day by day and everyone in the world is trying to figure out how to manage the crime rate and to work on certain cases, most of the people are trying to store the data for future reference. Human errors can occur at any point of time. There are different types of crimes law enforcement levels, such as traffic violations, sex crime, theft, violent crime, arson, gang/drug offenses, cybercrime. Different crime data mining techniques are proposed among each of them including entity extraction, clustering techniques, Association rule mining. Crime zones can be identified by occurrence of crime, by using hotspots. Patrol is needed at these hotspot areas.

The data mining tool helps in reducing the crime rate drastically.

Disadvantages

1. Security is considered to be a major issue in networks.
2. Analyzing huge amount of data becomes difficult.

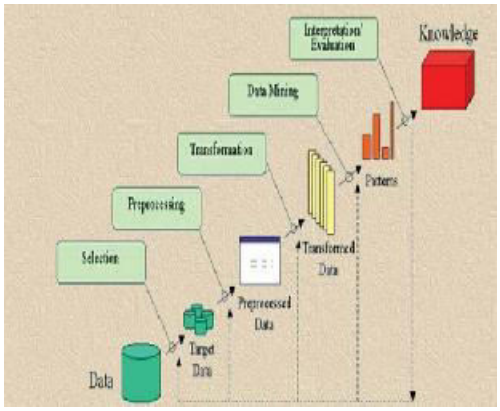
PROPOSED SYSTEM

Crime Mapping helps in understanding the concepts and practice of Crime Analysis in assisting police and helps in reduction and prevention of crimes and crime disorders using data mining tools. We can use data mining tools involved using ANN (Artificial Neural Networks) and KDD (Knowledge Discovery in Databases).

Advantages

1. To process huge amounts of data.
2. It is suitable to detect the ignored and hidden information at any point of time.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

MODULES

Admin Detector

MODULE DESCRIPTION

Admin

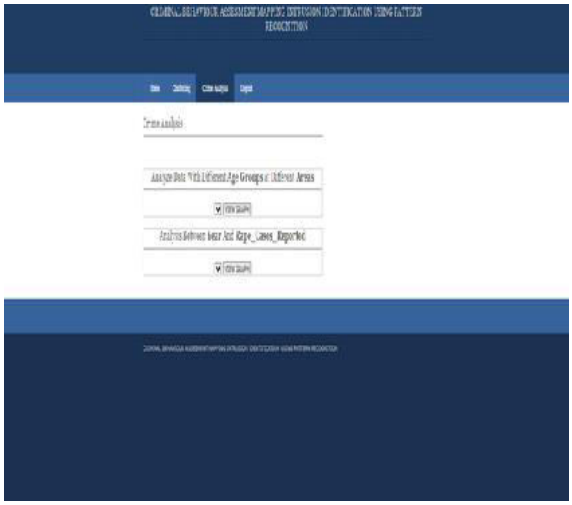
In this application admin is a module, here admin can login directly with username and password, after admin login he can upload dataset which is related to crime and can view dataset, these are some operations which are going to done by the admin.

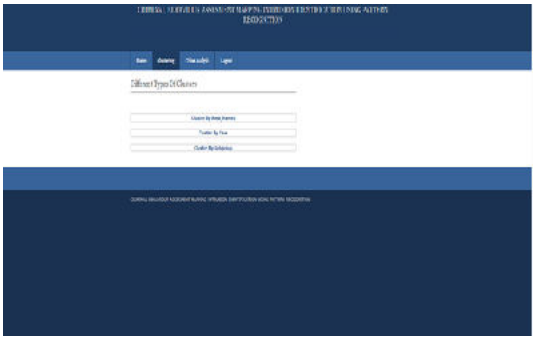
Detector

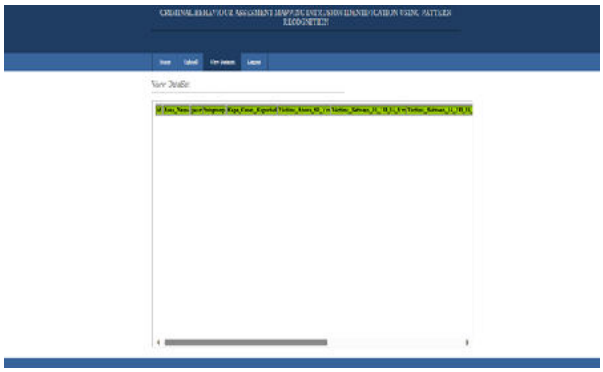
Here detector is a module, he can directly login with username and password after successful

login he can perform some operations such as can view data and make clusters based some selected features and analyze data to detect intrusions and view graphical analysis of intrusions.

V. SCREENSHOTS







VI. CONCLUSION

With the assistance of these devices, the wrongdoing information will be nourished to the information-digging device for

investigation and afterward comes about for two unique models will be recorded. With the assistance of the SAM instrument/tools, we will maintain a strategic distance from the distinction in the outcome and after that the subsequent information will be utilized for the finding the relations amongst those et cetera. Along these lines we will lessen false positives and false negatives in the field of the interruption identification framework utilizing the information mining in the field of wrongdoing information examination.

FUTURE WORK

The information concerning the illegal activity will be sent to the device that digs up some information for further investigation with the help of these devices, and the results of the investigation will afterwards be recorded for two different models. We will keep a deliberate distance from the distinction in the accomplishment with the assistance of the SAM instrument/tools, and after that, the resulting knowledge will be utilised for the discovering of the connections between those. In this manner, we will lower the number of false positives and false negatives in the area of the interruption recognition framework by applying data extraction in the field of criminal activity data examination.

REFERENCES

1. Chen, Hsinchun, et al. "Crime data mining: a general framework and some examples." computer 37.4 (2004): 50-56.
2. Ektefa, Mohammadreza, et al. "Intrusion detection using data mining techniques." Information Retrieval & Knowledge Management,(CAMP), 2010 International Conference on. IEEE, 2010.
3. Clifton, Chris, and Gary Gengo. "Developing custom intrusion detection filters using data mining." MILCOM 2000. 21st Century Military Communications Conference Proceedings. Vol.IEEE, 2000.
4. Dickerson, John E., and Julie A. Dickerson. "Fuzzy network profiling for intrusion detection." Fuzzy Information Processing Society, 2000. NAFIPS. 19th International Conference of the North American. IEEE, 2000.
5. Siraj, Ambareen, Susan M. Bridges, and Rayford B. Vaughn. "Fuzzy cognitive maps for decision support in an intelligent intrusion detection system." IFSA World Congress and 20th NAFIPS International Conference, 2001. Joint 9th. Vol. 4. IEEE, 2001.
6. Nath, Shyam Varan. "Crime pattern detection using data mining." Web intelligence and intelligent agent technology workshops, 2006. wi-iat 2006 workshops. 2006 ieee/wic/acm international conference on. IEEE, 2006.
7. Florez, German, S. A. Bridges, and Rayford B. Vaughn. "An improved algorithm for fuzzy data mining for intrusion detection." Fuzzy Information Processing Society, 2002. Proceedings. NAFIPS. 2002 Annual Meeting of the North American. IEEE, 2002.
8. Panda, Mrutyunjaya, and Manas Ranjan Patra. "A comparative study of data mining algorithms for network intrusion detection." Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on. IEEE, 2008.
9. Vaidya, Jaideep, and Chris Clifton. "Privacy-preserving data mining: Why, how, and when." IEEE Security & Privacy 2.6 (2004): 19-27.