DATA MINING USING – CRIME ANALYSIS MAPPING, INTRUSION DETECTION

G.Pushparani[1], S.Mahalakshmi[2]

[1]*Dept of Computer Science, School of Arts and Science, Vinayaka Mission's Research Foundation, Chennai, India.*
Email : pushparani161098@gmail.com

[2]*Assistant Professor, Dept of Computer Science, School of Arts and Science, Vinayaka Mission's Research Foundation, Chennai, India.*
Email: maha.cs@avit.ac.in

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. 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). Evidence based research helps in analyzing the crimes. We calculate the crime rate based on the previous data using data mining techniques. Crime Analysis uses quantitative and qualitative data in combination with analytic techniques in resolving the cases. For public safety purposes, the crime mapping is an essential research area to concentrate on. We can identity 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 reduction and prevention of crimes and crime disorders.

Keywords: *Data mining, Data Security, User privacy, Supervised learning, Unsupervised learning*

I. INTRODUCTION

Cybercrime involves a mixture of diverse typical crimes with new illegal acts. Individual cybercrime incidents are occurrences of particular criminal offences and, as multiple national crime statistics and surveys demonstrate, are steadily increasing. According to the Federal Bureau of Investigation, the Internet Complaint Center received 269 422 complaints of Internet crime in 2014, which indicates a rise of 1600% in comparison to the 16 838 complains included in the initial report. In a worldwide study released by PricewaterhouseCoopers, the number of reported information security incidents around the world rose 48% in 2014, the equivalent of 117 339 attacks per day. Similarly, the German Crime Statistics indicated a 23.6% increase in the number of cybercrime incident from 2007 to 2008. The various offences of cybercrime pose a serious threat to the global economy, safety, and well-being of the society. In a PricewaterhouseCoopers report, it is highlighted that cyber-security incidents are not only increasing in number but they are also becoming progressively destructive and target a broadening array of information and attack vectors. Cybercrime continues to be on the rise and cybercriminals are launching increasingly sophisticated cyber attacks aimed at disrupting businesses through denial of service attacks and stealing personal information all with serious

economic consequences. Law and policy makers are under increasing pressure to develop timely legislations to address cybercrime issues and provide effective measures to prosecute cybercriminals. We present a comprehensive review of the various laws that are currently available in the Unites States to control cybercrime and support cybersecurity. We also discuss proposed bills in light of how they address cybersecurity challenges in current legislations. Finally, we briefly present recent regulations and proposed bills related to cybersecurity in a few other countries which have set up various government initiatives in this area.

2.Related Works

The idea of Cybercrime is not new, yet there is significant confusion amongst academics, computer security experts and users as to the extent of real Cybercrime. In this paper, we explore the breadth of computer-based crime, providing a definition of the emerging terms "Cybercrime" and "crimeware". We then divide Cybercrime into two distinct categories: Type I Cybercrime, which is mostly technological in nature, and Type II Cybercrime, which has a more pronounced human element. We then use two case studies to illustrate the role of crimeware in different types of Cybercrime, and offer some observations on the role of cognition in the process of Cybercrime. Finally we provide several suggestions for future work in the area of Cybercrime

In recent years, a number of surveys have indicated a significant escalation in reported incidents of computer crime and abuse. This rise is coupled with increasing attention to the issue in the mass media, which has the effect of heightening public perceptions of problems with IT and may represent a barrier to the adoption of technologies such as the Internet and World Wide Web.

3. 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.

3.1DISADVANTAGES

- 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.
- The main problem here is the central problem, where all the data needs to be stored in a single place and required to retrieve this large bulk amount of data would cost a lot.

4. 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). We collect the data from police department and try to get each and every detail, like the person's name, height, age, sex, fingerprint details, and pattern identification number for similar types of cases.

Once we get the information, we start to process the data. We get a lot of unnecessary data along with the required data. But before we start processing the data using data mining techniques and tools, we need to identify unnecessary data and remove those kinds of data to reduce or to avoid the confusion.

4.1Advantages

- We mainly collect the attributes information, like eye color, fingerprint details, characteristics, dimensions, or other features.
- The use of information mining methods helps in resolving 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.

5. ARCHITECTURE

The structural design of the proposed system is shown in the figure-1

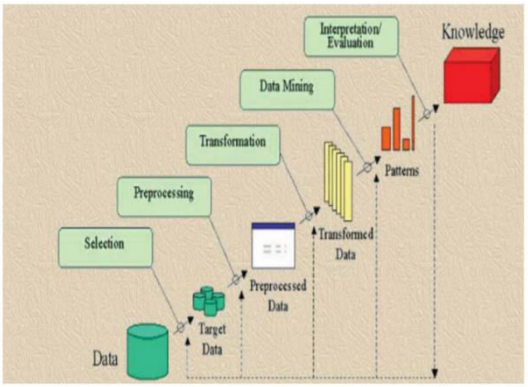

Fig-1 Architecture

6. MODULE DESCRIPTION

6.1 Crime analysis

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 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.

6.2 Community oriented policing services:

Crime mapping is conducted and funded by the Office of Community Oriented Policing Services (COPS). Evidence based research helps in analyzing the 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 the cases. For public safety purposes, the crime mapping is an essential research area to concentrate on. We can identity the highest risk crime zones with the help of data mining techniques.

6.3 Distributed denial of service attack:

Distributed denial of service attacks is one of the most common attacks on internet sites. Intrusion detection helps in identifying the network related activity and using this we can provide security against DOS attacks. There are two types of intrusion detection methods available here: misuse detection which is based on exact pattern match, and anomaly detection which requires more training related to artificial intelligence. Fuzzy intrusion recognition engine is an anomaly IDS

which identifies malicious sites which are not trustworthy using fuzzy systems. Here, 3-D packet count with a 15-minute interval is used to find the regular network connections and try to indicate the intrusions, if any, at that point of time .

6.4Clustering technique:

In this, they used clustering techniques to identify crime patterns. In a geographical area, the need to identify the crime at a point in time is known as clustering. We can use a map to identify the plot. The largest challenge is with free text fields. It is difficult to convert the free text fields into data, but the K means technique is used for this purpose in this paper. Operational data can be extracted and transformed to another form using this technique. By doing this, it is much easier to find out the crime patterns for the detectives to identify the frauds

7. RESULTS

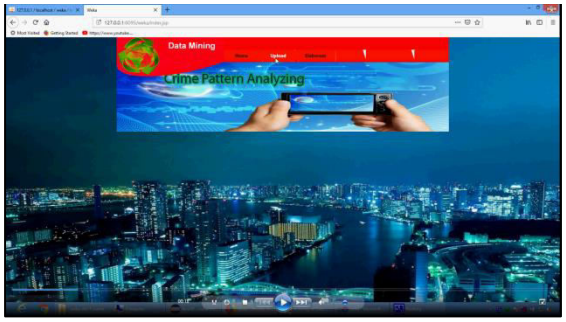

Fig-1 Home Page

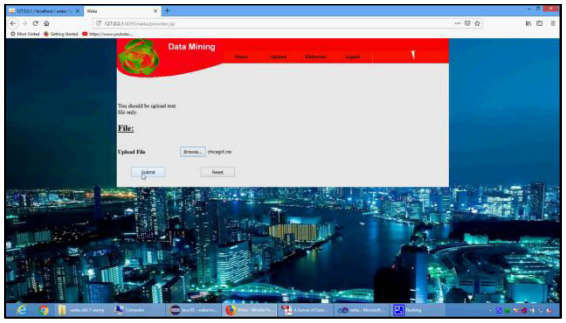

Fig-2 Data set upload

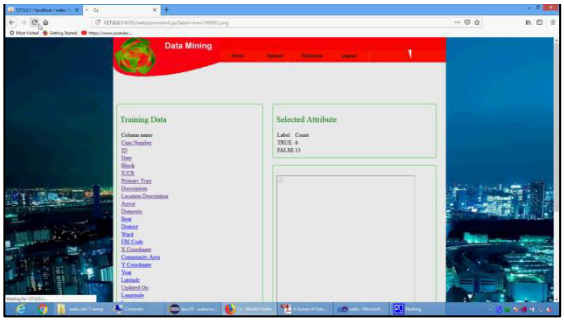

Fig-3 Training Data Set With attribute

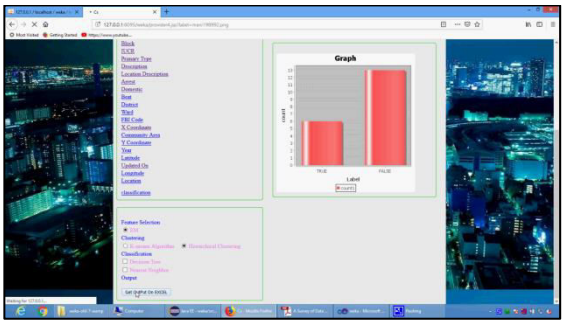

Fig-4 Attribute true or false level

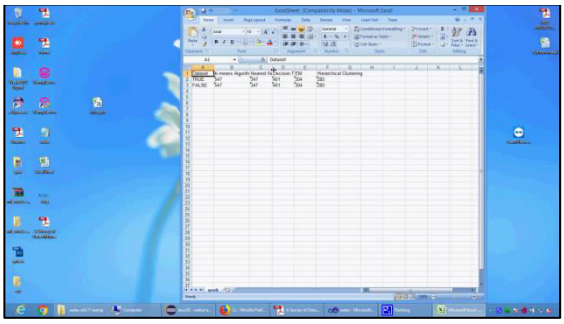

Fig-5 Out Put view

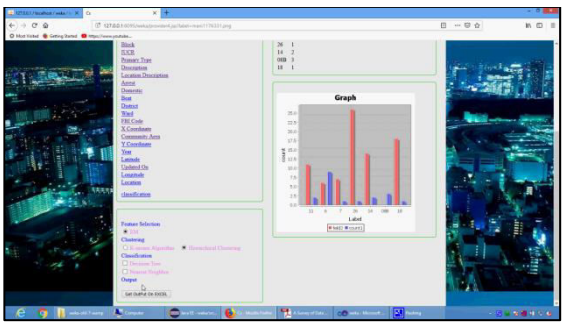

Fig-6 Analysis view

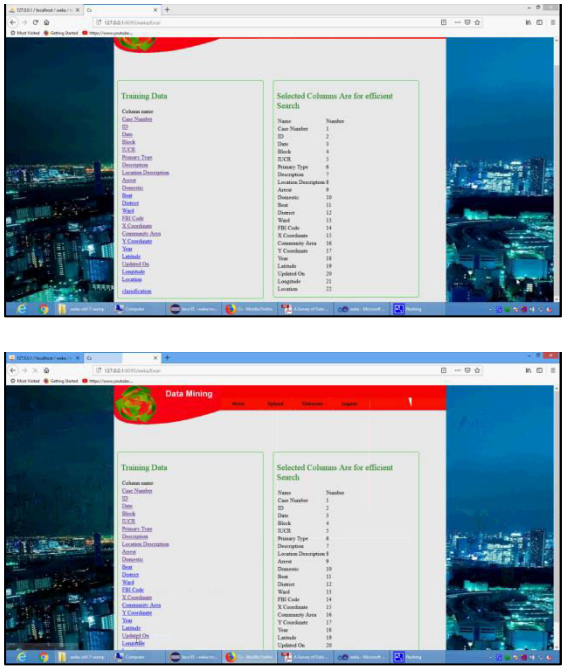

Fig-7 Crime data view

8. CONCLUSION

The authors identified and presented the features of cybercrime incidents, a classification system for related offences and a schema that binds together the various elements and examines their interrelations to better suggest corresponding actions, measures and policies. The process involved revision of reports conducted by authorities, academia and agencies related to information security. The identification of cybercrime features allows for a more comprehensive description of individual incidents that leads to better understanding, handling and management of their occurrences.

The modular feature-based approach toward description of incidents allows for additional features to be included in the future. Also the expansion or consolidation of their respective elements can also be achieved depending on specific perspectives. This paper also proposed a comprehensive two-level classification system of cybercrime offences based on European Union's initial typology and further analysis taking account of the present status and recent forms of cybercrime. The system encompasses the most common forms of computer related offences and can prove useful for law enforcement agencies. Furthermore, the proposed system is included as part of the feature-based description to classify a cybercrime incident under a corresponding criminal offence.

9. Future Work

The authors are currently working in automating the proposed approach using the XML-based Structured Threat Information Expression; a structured language for describing cyber threat information so it can be shared, stored, and further analyzed. A future extension could take into account the frequency of occurrences in order to propose custom actions, measures and policies, and finally incorporate the produced schema in an automated incident management system with standard operating procedures and protocols. The operational efficiency of such system would provide automated identification of incidents and emergency response protocols. Furthermore, all information handled by the system would be recorded in the form of an aggregator to produce analytics, statistics and visualizations for gaining insights and future planning, leading to optimization of handling cybercrime incidents by the relevant agencies.

10. 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. 1. 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