(IJIASE) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

EMPLOYBILITY OF DATA MINING TECHNIQUES TO PREDICT CYBER CRIME

Aryan Marwah

NK Bagrodia Public School
Sector 9, Rohini, New Delhi 110085

ABSTRACT

Data mining is the technique in which data is to be extracted from heap of data's which is previously unknown.This paper gives a brief overview of data mining techniques related to cybercrimes and explains how to implement data mining techniques. Cyber security relates with protecting network computer from various attacks like virus, ransomware and Trojans. Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. Data mining can be used to model crime detection problems. Cyber Crimes are a social nuisance and cost our society dearly in several ways. They are IT-based criminal offense. Due to extensive use of Internet and I.T. enabled services new class has been emerged. Here we look how data mining approach helps to detect cybercrime patterns and speed up the process of solving it.

I. INTRODUCTION

With the rapid advancement of information discovery techniques data mining continues to play an important role in cyber security. Cybersecurity is a mind-boggling issue that cuts over different areas and calls for multi-dimensional, multi-layered activities and reactions. It has demonstrated a test for governments in light of the fact that various spaces are regularly controlled through services and divisions. Data mining is the computer-assisted process of digging through and analysing enormous sets of data and then extracting the meaning of the data and it is the process of analysing data from different perspectives and summarizing it into useful information. Data mining plays an important role in terms of prediction and analysis. Data mining and web mining may be used to detect and possibly prevent cyber-attacks and cybercrime. Cybercrime is an illegal act committed using a computer network. It is a subset of computer crime and involves a computer and a network. It is ubiquitous and has become a major security issue. The PC may have been utilized in the commission of a wrongdoing, or it might be the objective [1]. They are offenses that are carried out against people or gatherings of people with a criminal thought process to purposefully hurt the notoriety of the person in question or cause physical or mental damage, or misfortune, to the unfortunate casualty straightforwardly or in a roundabout way, utilizing present day media transmission systems, for example, Internet (Chat rooms, messages, see sheets and gatherings) and cell phones (SMS/MMS)" [2].

(IJIASE) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

II. CYBER CRIME IN INDIA

Cybercrime is one of the dangerous factors for any country. It is impossible to find a country which has a crime- free society. In the Indian scenario with e commerce becoming popular in the last few years' cybercrimes are a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attack. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

A key finding of the Economic Crime Survey 2006 was that a typical perpetrator of economic crime in India was male (almost100%), a graduate or undergraduate and 31-50 years of age. Further, one third of the frauds were from insiders and over 37% of them were in senior managerial positions [3]. The present society is filled with various kinds of cybercrimes. this paper has a brief overview of cybercrimes and its existence, types and brief study, major steps to prevent and combat working department This paper is organized as follows. Section 1 gives the introduction about data mining, cybercrime and cyber security. Section 2 describes cybercrime in India. Section 3 explains the role of data mining in cyber security in India. Concluding remarks are given in Section 4.

With expanding web infiltration, cybercrimes have additionally expanded over the most recent couple of years. Somewhere in the range of 2011 and 2015, the quantity of cybercrimes enrolled in the nation has gone up multiple times. With expanding portable and web entrance in the nation, cybercrimes have additionally expanded proportionately. Somewhere in the range of 2011 and 2015, in excess of 32000 cybercrimes were accounted for the nation over. More than 24000 of these cases are enlisted under the IT Act and the staying under the different areas of IPC and other State Level Legislations (SLL). Fig no 1 demonstrates the cases enlisted under IT Act and IPC Act. Digital Crimes in India are enrolled under two distinct acts, the IT Act and the Indian Penal Code (IPC).

- The cases registered under the IT Act include:
- Tampering computer source documents (Section 65 IT Act)
- Loss /damage to computer resource/utility (Section 66 (1) IT Act)
- Hacking (Section 66 (2) IT Act.
- Obscene publication/transmission in electronic form (Section 67 IT Act)
- Failure of compliance/orders of Certifying Authority (Section 68 IT Act) Fig no 2 shows Cyber Crime in India and the number of cases registered under IT Act.

cases also registered under IPC section that includes:

- Offences by/against Public Servant (Section 167, 172, 173, 175 IPC)
- False electronic evidence (Section 193 IPC)
- Destruction of electronic evidence (Section 204, 477 IPC)
- Forgery (Section 463, 465, 466, 468, 469, 471, 474, 476, 477A IPC)
- Criminal Breach of Trust (Section 405, 406, 408, 409 IPC)
- Counterfeiting Property Mark (Section 482, 183, 483, 484, 485 IPC).

Fig no 1 shows Cyber Crime in India and the number of cases registered under IT Act.

Year	IT Act		IPC Act	
	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
2011	1791	1184	422	446
2012	2876	1522	601	549
2013	4356	2098	1337	1203
2014	7201	4246	2272	1224
2015	8045	5102	3422	2867
Total	24269	14152	8054	6289

Fig 1 Number of cases registered and persons arrested under IT Act and IPC Act

In recent years, cases registered under IT ACT and IPC Act has been very high, cases registered under these acts has grown by 300% between 2011 and 2015.There was almost increase of 70% in cybercrime between 2013 and 2015.Many criminals also arrested during this time.The Government also confesses the rise in crime and detailed that the uses of smart phones and advance applications helps in rising of cybercrime.

Maharashtra and Uttar Pradesh on the top The rundown of states with the most elevated rate of cybercrime for the period 2011 to 2015 tosses no curve balls. Maharashtra best the rundown with in excess of 5900 cases in the 5 years pursued by Uttar Pradesh with near 5000. Karnataka is third with in excess of 3500 cases. The top states in this rundown are the ones with a more prominent web supporter base. The last 10 are moderately littler states with lower populace and lower web infiltration [4].

Mumbai: Cybercrimes have steadily increased in Maharashtra in the last three years, doubling in 2014 over the previous year. Most of the 9,322 cases registered under the IT Act and IPC Act during 2014 were registered in Maharashtra. New Delhi: Cyber Crime cases in the country registered under IT Act surged nearly 300 percent between 2011 and 2014. The study revealed that in the past, the attacks have been mostly initiated from countries like US, Turkey, China, Brazil, Pakistan, Algeria,

(IJIASE) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

Europe and UAE, with growing adoption of internet and smartphones India has emerged one of the primary targets among criminals. Hyderabad: An email allegedly from India's central bank, asking to secure their bank account details with the RBI is fake, and an attempt by new-age fraudsters to con people into giving away bank account details and lose hard-earned money, security experts said. The email says RBI has launched a new security system, asking users to click on a link to open a page with list of banks in place. Once anyone chooses a particular bank, it asks for all net banking details, including card numbers and the secret three digit CVV number, among others. The incidence of Cyber Crime cases during 2014 is shown in Fig no 5. Also Fig no 6.1 and 6.2 shows the state wise analysis of Cyber Crime in India.

Considering the increasing trends of the crimes the Bureau has collected a comprehensive data on cybercrimes in 2014 using revised Performa of 'Cybercrime in India'. The IT Act, 2000, specifies the acts which are punishable.

III. ROLE OF DATA MINING IN CYBER SECURITY

Datamining has played major role in security application which are mentioned below:

- Anomaly Detection
- Profiling Network Traffic Using Clustering
- Methodology
- Scan Detection
- Cyber-terrorism, Insider Threats, and External Attacks
- Credit Card Fraud and Identity Theft
- Attacks on Critical Infrastructures

IV. CONCLUSION

Data mining has numerous applications in security incorporating into national security just as in digital security. The dangers to national security incorporate assaulting structures and annihilating basic foundations, for example, control networks and media transmission frameworks. Information mining methods are being utilized to distinguish suspicious people and gatherings, and to find which people and gatherings are fit for completing fear based oppressor exercises. Cybercrime is about the wrongdoings where correspondence channel and specialized gadget has been utilized legitimately or in a roundabout way as a medium whether it is a Laptop, Desktop, PDA, Mobile telephones, Watches, Vehicles. It is more diligently to recognize and hardest to stop once happened causing a long haul negative effect on unfortunate casualties. Digital security is worried about shielding PC and system frameworks from debasement because of malevolent programming including Trojan ponies and infections. In this paper we focused mainly on data mining for cyber security applications in India. We also concluded role of data mining to observe confidential data to preserve cyber security. For cyber security and national security data mining is a very wide & active area to research. Data mining helps users to make all kinds of correlations and leads to privacy concerns.