IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-12, Dec 2019 E-ISSN: 2347-2693

Survey Report on Cyber Crimes and Cyber Criminals Get Protected from Cyber Crimes: Review Paper

Marripelli Koteshwar[1*], Bipin Bihari Jaya Singh[2]

[1]Dept. of Computer Science, Rayalaseema University, Kurnool, India
[2]Dept. of IT, CVR College of Engineering, JNTU Hyderabad, Telangana, India

**Corresponding Author: koteshwar.marri@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i12.99109 | Available online at: www.ijcseonline.org

Accepted: 19/Dec/2019, Published: 31/Dec/2019

***Abstract*—** Digital Crime is a wrongdoing which includes the utilization of computerized innovations in commission of offense, coordinated to registering and correspondence advances. The cutting edge methods that are multiplying towards the utilization of web movement brings about making misuse, defenselessness making a reasonable path for exchanging secret information to submit an offense through illicit action. The movement includes like assaulting on Information focus Data System, burglary, youngster sex entertainment assembled pictures, online exchange misrepresentation, web deal extortion and furthermore organization in web vindictive exercises, for example, infection, worm and outsider maltreatment like phishing, email tricks and so on. The all-inclusive methodology of system like web at all dimensions of system needs to recoup from perpetrating illicit action in everywhere throughout the world and to stop the criminal nature by ensuring unlawful movement by upholding distinctive dimension of firewall setting inside its disconnected control for each country so as to screen and anticipate violations did in the internet. System security controls are utilized to avoid the entrance of programmers in systems which incorporates firewall, virtual private systems and encryption calculations. Out of these, the virtual private system assumes an indispensable job in keeping programmers from getting to the systems. Virtual Private Network (VPN) furnishes end clients with an approach to secretly get to data on their system over an open system foundation, for example, the web.

***Keywords*—** cyber-crime, cyber criminals, cyber-crime hackers, protectedcateogories, cyber stalking.

I. INTRODUCTION

Digital wrongdoing isn't an old kind of wrongdoing to the world. It is characterized as any crime which happens on or over the vehicle of PCs or web or other innovation perceived by the Information Technology Act. Digital wrongdoing is the most pervasive wrongdoing assuming a staggering job in Modern India. Not just the lawbreakers are making huge misfortunes the general public and the legislature but on the other hand can cover their personality as it were. There are number of illicit exercises which are carried out over the web by actually gifted offenders. Taking a more extensive understanding it very well may be said that, Cyber wrongdoing incorporates any unlawful action where PC or web is either a device or target or both.

The term digital wrongdoing might be judicially deciphered in certain decisions gone by courts in India, anyway it isn't characterized in any demonstration or rule gone by the Indian Legislature. Digital wrongdoing is a wild abhorrent having its base in the abuse of developing reliance on PCs in present day life. Utilization of PC and other partnered innovation in everyday life is developing quickly and has turned into a urge which encourages client accommodation. It is a medium which is limitless and inconceivable. At all the great web does to us, it has its dim sides too.1 Some of the recently developed cybercrimes are digital stalking, digital fear based oppression, email caricaturing, email bombarding, digital erotic entertainment, digital maligning and so forth. Some traditional wrongdoings may likewise gone under the classification of cybercrimes in the event that they are carried out through the vehicle of PC or Internet.

II. HISTORY AND EVOLUTION OF CYBERCRIME

The first recorded cyber-crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modem computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom.

This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and

livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber-crime.

The oxford Dictionary defined the term cybercrime as "Criminal activities carried out by means of computers or the Internet.Cyber-crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime"

"Cyber-crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them

III. CHARACTERISTICS OF CYBER CRIME

The Concept of cyber-crime is very different from the traditional crime. Also due to the growth of Internet Technology, this crime has gained serious and unfettered attention as compared to the traditional crime. So it is necessary to examine the peculiar characteristics of cyber-crime.

1**.** ***People with specialized knowledge*** – Cyber-crimes can only be committed through the technology, thus to commit this kind of crime one has to be very skilled in internet and computers and internet to commit such a crime. The people who have committed cyber-crime are well educated and have deep understanding of the usability of internet, and that's made work of police machinery very difficult to tackle the perpetrators of cyber-crime.

2. Geographical challenges **–** In cyberspace the geographicalboundaries reduced to zero. A cyber-criminal in no time sitting in any part of the world commit crime in other corner of world. For example a hacker sitting in India hack in the system placed in United States.

3. Virtual World **–**The act of cyber-crime takes place in the cyberspace and the criminal who is committing this act is physically outside the cyber space. Every activity of the criminal while committing that crime is done over the virtual world.

.4.***Collection of Evidence*** **-**It is very difficult to collect evidence ofcyber-crime and prove them in court of law due to the nature of cyber-crime. The criminal in cyber-crime invoke jurisdiction of several countries while committing the cyber-crime and at the same time he is sitting some place safe where he is not traceable.

5. Magnitude of crime unimaginable- The cyber-crime has thepotential of causing injury and loss of life to an extent which cannot be imagined. The offences like cyber terrorism, cyber pornography etc has wide reach and it can destroy the websites, steal data of the companies in no time.

IV. CYBER CRIME LAW

CYBER law is a typical term which alludes to legitimate locale and different methods for going before administrative perspectives in the web. It is an always conventional procedure. At whatever point a web improvement methodology pursues, various corrections are authorized while it is grown, thus various legitimate issues are additionally gets created by illicit activists. In the Internet, Child Pornography is one of the genuine Cybercrime and online pedophiles track to enjoy youngsters into sex exercises utilizing Internet. The traffic perils, designation in appropriations, spread of foul material, and posting incorporates sex entertainment with all its smudged presentation comprises the most significant known criminal digital offense today. This is one which takes steps to challenge the advancement of innovation of the more youthful creation in cybercrime and furthermore leaving lasting scar and harm on the more youthful age, if can't limited.

V. DIGITAL CRIME

Advanced wrongdoing has numerous synonymies for instance: cybercrime, electronic wrongdoing and PC wrongdoing are alterable words. Right off the bat PC wrongdoing term was utilized to indicate to any crime that done against PCs and systems or utilizing PC as device to do that action. However, over the most recent couple of years these violations stretch out to include other advanced gadgets like PDA, so the term was reach out to computerized wrongdoing. There is nobody definition for computerized wrongdoing as of recently and it's hard to shape standard one, anyway what can be said is that: advanced wrongdoing is centered around violations.

VI. CYBER CRIME CATEOGRIES

Another category of Cybercrime is against administration. Cyber Terrorism is a kind of crime which is distinct in this category. The increase of Internet has shown that the standard of Cyberspace is used by either group or individual to threaten the worldwide governments and to frighten the citizens of the country. This crime manifests when an individual "cracks" a government or military maintained website. The cyber-crime may be broadly classified into three groups. They are

1. Crime against the Individuals Person, Property of an individual.
2. Crime against Organization

Government, Firm, Company and Group of Individuals.

3. Crime against Society.

VII. CYBER STALKING

Stalking all in all methods conduct of bothering or undermining the other individual. Digital Stalking is an expansion of physical type of stalking, which is submitted over the online medium with the utilization of data Technology. In digital stalking the web, email, talk rooms and so on are utilized to stalk someone else.

The Wikipedia characterizes digital stalking, where the Internet or other electronic intends to stalk or badger an individual, a gathering of people, or an association. It incorporate the creation of bogus incriminations or proclamations of reality (as in maligning), checking, making dangers, fraud, harm to information or hardware, the sales of minors for sex, or assembling data that might be utilized to annoy.

Stalking is a consistent procedure, comprising of a progression of activities, every one of which might be totally lawful in itself. The meaning of Cyber stalking isn't all around satisfactory as it fluctuates spot to put. As indicated by Professor LimberRoyakkers -
"Digital stalking is the over and over badgering or compromising of an individual through the web or other electronic methods for correspondence. A digital stalker is somebody with affectionate as well as sexual thought processes who continually badgers another person electronically: through the announcement board, talks box, email, spam, fax, signal or phone message. Stalking by and large includes the consistent badgering or undermining of another person: following an individual, showing up at somebody's home or working environment, making irritating telephone calls, leaving composed messages or questions, or vandalizing somebody's property.
There are three ways in which cyber stalking is conducted i.e

1. stalking by E-mail - where the offender directly sends e-mail to thevictim to threaten her or to harass her. It is the most common form of stalking in the modern world. The most common is sending hate, obscene, pornographic material and threatening mail to the victim.

2. Stalking through Internet –this is global form of cyber stalking. Inthis the offender doesn't invade the private space of the victim but harasses her through the global medium publically. The offender through the internet medium post the phone numbers and email address of the victim on porn sites and put morphed photos of the victim on cyber space and threaten them. This is the serious nature of cyber stalking where the stalker chases all the activity of victim on the net and posted false information about her on the websites.

3. Stalking through Computer - In this form the offender is technocrat and he can take control of the computer of the victim as soon as the computer starts operating. In this the stalker gets control of the victims computer address and gets control over it. This form of cyber stalking requires high degree of computer knowledge to get access to the targets computer and the option available to the victim is to disconnect the computer and abandon the current internet address.

VII. DIGITAL CRIME SCENE INVESTIGATION:

After an investigator reach the crime scene the real investigation process is began, the important part of investigation process and next steps are depended on it. An investigator should recognize significant evidences

in the crime scene; he/she also has to identify these evidences and their sources.
As done in traditional -physical-crime scene evidences must be preserved and documented. The thing that should be kept in mind is the importance of integration between physical and digital crime scenes, the scene of the crime has physical part and digital part and they cannot be separated.

VIII. ISSUES WITH THE PRESENT ATTACKS DETECTION SYSTEM

The following issues have been identified in the presently available Intrusion Detection System:

1. High False Alarm Rate (FAR)
2. Not completely adaptable
3. Low detection rate of u2r type of attacks
4. Low detection rate of r2l type of attacks

IX. LEGAL RECOGNITION AND POSITION IN INDIA

Though the behavior widely identified as stalking has existed for centuries, the legal system has only codified its presence in the statues in the recent decades. Cyber stalking only gather importance after the evolution of the internet in the nineties. The rise in crimes related to cyber stalking through the online medium is an extension of traditional stalking that utilizes a high tech *modus operandi*.In each jurisdiction the statute is different as far as cyber stalking is concerned. In The United States, California is the first state to pass the anti-stalking law in 1990. But as far as the stalking through computers is concerned there are few states or countries that passed laws related to cyber stalking.

X. CYBER CRIMINALS

Cyber-crime has become a profession and the demography of the cyber-criminal is changing rapidly with the type of organized gangsters who are more traditionally associated

with drug-trafficking, extortion and money laundering. The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill. The probable marketplace for this transaction is a hidden IRC (Internet Relay Chat) chat room. Gaining control of a bank account is increasingly accomplished through phishing. All of the following phishing tools can be acquired very cheaply.

The cyber criminals works in the following ways:

- **Coders,**
- **kids,**
- **drops,**
- **Mob.etc.**

Criminals are defined in above line for all types are given below.

XI.CYBER HACKERS

White hat hacker
A white hat hacker is an ethical hacker who ethically oppose to the abuse of computer systems. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) would like to break into them. The term white hat hacker is also often used to describe those who attempt to break into systems or networks in order to help the owners of the system by making them aware of security flaws, or to perform some other altruistic activity. Many such people are employed by computer

Black hat hackers:
A black hat is a person who compromises the security of a computer system without the permission of authorized party, typically with malicious intent. The somewhat similar activity of defeating copy prevention devices in software which may or may not be legal in a country's laws is actually software cracking. The primary difference between white and black hat hackers is that a white hat hacker claims to observe ethical principles. Like black hats, white hats are often intimately familiar with the internal details of security systems, and can delve into obscure machine code when needed to find a solution to a tricky problem. Some use the term grey hat and fewer use brown hat to describe someone's activities that crosses between black and white.

Grey Hat Hackers:
A Grey Hat in the computer security community, refers to a skilled hacker who sometimes acts legally, sometimes in good will, and sometimes not. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or for malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits.

Internet Crime Hackers:
Internet crime hackers commit crime on the internet, using the Internet and by means of the Internet. Internet crime is a general term that includes crimes such as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitate crimes.

Blackmail Hackers:
Blackmail is a long-established illegal act that has been given a new twist in the modern age. The blackmailer may threaten to release embarrassing or other harmful information via the Internet or a private network if the victim does not comply with the demands of the criminal. A cybercrime of this type may go as far as having the victim transfer funds to an untraceable bank account using some type of online payment program, thus making full use of modern technology to commit the crime Blackmail Hackers.

XII. PROTECTED FORM CYBER CRIME

Terminate Online Session Completely:
Closing the browser window or typing in a new website address without logging out may give others a chance of gaining access to your account information. Always terminate your online session by clicking on the "Log out or Sign Out" button. Avoid using the option of "remember" your username and password information.

Create Backup of Important Data:
Backup of all the important files whether personal or professional should be created. Getting used to back up your files regularly is the first step towards security of your personal computer.

Protect Your Password:
Try creating a password that consists of a combination of letters (both upper case and lower case), numbers and special characters. Password should be changed regularly. Do not share your password with other people.

Participation in Social Networking:
While participating in most social networking sites do not expose the personal information to others and all of these sites have a certain intensity of control over security issues. Use privacy settings to prevent personal information being broadcast.

Use Your Own Computer:
It's generally safer to access your financial accounts from your own computer only. If you use some others computer, always delete all the "Temporary Internet Files", and clear all your "History" after logging off your account.

Update Your Software Package Regularly:
Frequent online updates are needed for all the Internet security software installed on your computer system.

Using Email:
A simple rule in using this communication tool is not to open any links in emails from people you do not know. Hackers do use E-mail as the main target seeking to steal personal information, financial data, security codes and other. Do not use the link sent to you. If you need access to any website, visit the website by typing the address in your menu bar. Cyber-crime, being a burning issue around the world, many countries is beginning to implement laws and other regulatory mechanisms in an attempt to minimize the incidence of cybercrime. The laws in many countries on effectiveness of the punishment and prevention of computer crime requires a robust number and scope of the regulations, and even the proceedings, which lags far behind the reality of demand for computer crime in judicial practice.

XIII. REVIEW OF WORK

In this related work I would explained for various algorithms worked on cyber-attacks detection on the basis of data mining techniques and forensic principles and legal action reviews also included. This is review of various concept and methods are used for detection and prevention of cybercrime and cyber-crime attacks detection process on the basis of various methods are determined.

Association Rules: In Data mining approaches for cyber-attacks detection include association rules and frequent episodes, which are based on building classifiers by discovering relevant patterns of program and user behavior. Association rules and frequent episodes are used and the features can be defined in the form of packet and connection details. However, mining of features is limited to entry level of the packet and requires the number of records to be large and sparsely populated; otherwise, they tend to produce a large number of rules that increase the complexity of the system.

Data Clustering Methods: In Methods such as the k-means and the fuzzy c-means have also been applied extensively for cyber-attacks detection. One of the main drawbacks of the clustering technique is that it is based on calculating numeric distance between the observations, and hence, the observations must be numeric. Observations with symbolic features cannot be easily used for clustering, resulting in inaccuracy. In addition, the clustering methods consider the features independently and are unable to capture the relationship between different features of a single record, which further degrades attack detection accuracy.

Bayesian Network: In] Bayesian Network is a graphical representation of the joint probability distribution function over a set of variable. The network structure can be represented in Bayesian Network as a Directed Acyclic Graph where each node represents a random variable and each edge between nodes shows the relation between nodes. Individuals invents whichoccurs during attack are represented as nodes in the graph and relationship between those events are represented as edges of the graph is then used to detect the cyber-attacks. Bayesian network can also be used for cyber-attacks detection. However they tend to be attack specific and build a decision network based on special characteristics of individual attacks. Thus, the size of a Bayesian network increases rapidly as the number of features and the type of attacks modeled by a Bayesian network increases.

Hidden Markov Model: To detect anomalous traces of system calls in privileged processes Hidden Markov Model are applied. However, modeling the system alone may not always provide accurate classification as in such cases various connection level features are ignored. Further, HMMs are generative systems and fail to model long-range dependencies between the observations.

Decision Tree:]The decision trees select the best features for each decision node during the construction of the tree based on some well-defined criteria. One such criterion is to use the information gain ratio. Decision trees generally have very high speed of operation and high attack detection accuracy even if dealing with a large amount of data.

Support Vector machine (SVMs): In Though the neural networks can work efficiently with noisy data, they require large amount of data for training and it is often hard to select the best possible architecture for a neural network. Support vector machines have also been used for detecting cyber attackss. Support vector machine map real valued input feature vector to a higher dimensional feature space through nonlinear mapping and can provide real time detection capability, deal with large dimensionality of data, and can be used binary class as well as multiclass classification.

Genetic Algorithms (GAs): In Genetic algorithms mimic the natural reproduction system in nature where only the fittest individual in a generation will be reproduced in subsequent generations, after undergoing recombination and random change.

Fuzzy Logic: In A set of rules can be created to describe a relationship between the input variables and the output variables, which may indicate whether an cyber-attacks occurred.

XIV. CONCLUSION

The motivation of this investigation is that, there are many bothering things happening in the web. Cybercrime suggests

all of the activities completed with criminal point in the web. These could either be the wrongdoings in the common sense or could be works out, as of late progressed with the advancement of the new medium. By virtue of the obscure thought of the Internet, it is possible to attract into a variety of criminal

Activities with no potential repercussions and people with knowledge, have been appallingly manhandling this piece of the Internet to continue wrongdoings in the web. In any case, any activities which basically pester human sensibilities can moreover be joined into its ambit. The objective of this examination is the revolution of computerized bad behavior using advanced laws and advanced security strategies. The advanced security methodologies bunches correctly and beneficially distinguishes suspicious URLS, perceives malware tests and phishing locales using grouping techniques, the time of security.

XIV. LIRETATURE REVIEW

N. Kumari and A. K. Mohapatra, "[1]Crimes committed within electronic or digital domains, particularly within cyberspace, have become
Common. Criminals are using technology to commit their offenses and create new challenges for law enforcement agents, attorneys, judges, military, and security professionals. Digital forensics has become an important instrument in identifying and solving computer-based and computer-assisted crime. This paper provides a brief introduction to
Digital forensics.

M. Reith, C. Carr, and G. Gush,[2]. This model attempts to address some of the shortcomings of previous methodologies, and provides the following advantages: a consistent and standardized framework for digital forensic tool development; a mechanism for applying the framework to future digital technologies; a generalized methodology that judicial members can use to relate technology to non-technical observers; and, the potential for incorporating non-digital electronic technologies **within the abstraction.**

E. Casey,[3]. With this integration or eversion of cyberspace comes an increase in the realness of virtual events. Bullying in high schools and hate crimes in universities have moved into cyberspace, amplifying these harmful behaviors by delivering virtual blows anytime, anywhere. In January 2010, 15-year-old Pheobe Prince committed suicide as a result of cyberbullying.**Richard Power, [**5].Virus attacks continue to be the source of the greatest financial losses. Unauthorized access continues to be the second-greatest source of financial loss. Financial losses related to laptops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) are third and fourth. These four categories account for more than 74 percent of financial losses.

Dr. V.Tayal,"[6]. Cyber attacks detection is the process of monitoring and analyzing the events in computer systems or networks to discover the signals of possible incidents, which attempt to compromise the confidentiality, integrity, and availability of computer resources [1]. In general, cyber attacks detection system use misuse based and anomaly-based detection model for detecting cyber attackss [4]. Misuse-based cyber attacks detection system

Denning D E, "An Cyber attacks-Detection Model,"[7].A network based cyber attacks detection system monitor and analyze network traffics, and use multiple sensors for detecting cyber attackss from internal and external networks [7]. Network cyber attacks detection system analyzes the information gathered by the sensors, and returns a synthesis of the input of the sensors to system administrator or cyber attacks prevention system. System administrator carries out the prescriptions controlled by the cyber attacks detection system. Cyber attacks Detection System (IDS) is one of the most efficient technologies used in present for the identification of cyber attacks. This chapter aims at giving an overview of the previous work done in this field, evaluating current status of the work done and envisioning gaps in current knowledge.

Brief discussion of researchers done by various researches is given below:
In 1998, Wenke Lee and Salvatore J. Stolfo integrated Data mining technique in cyber attacks Detection. Two data mining technique i.e. association rule mining and frequent episode mining were implemented for the development of framework which are essential in describing program or user behavior, sendmail system call data and network tcpdump data was used for the construction of the detection model and performance evaluation. Perliminary experiments showed the promising results. The main problem faced by this model was the high false alarm rate.

In 2000, Wenke Lee et al developed a systematic framework for analyzing audit data and constructing cyber-attacks detection models. Under this Framework, a large amount of audit data was first analyzed using data mining algorithm in order to obtain the frequent activity patterns. These patterns were then used to guide the selection of system features as well as the construction of additional temporal and statistical features for another phase of automated learning. Classifiers based on these selected features are then inductively learned using the appropriately formatted audit data. These classifiers can be used as cyber-attacks detection models since they can classify (i.e, decide) whether an observed system activity is "legitimate" or "intrusive".

In 2000, The MITRE Corporation especially Chris Clifton and Gary Genkowith the communication electronics command of U.S. Army addressed the problem of high false alaram rate and used data mining to reduce it up to some extent by developing custom filters. These filters were constructed by sequential association mining. The aim of this approach was to reduce the false alarm stream based on known normal behavior in a particular environment.

In 2001, DipankarDasgupta and Fabio A. Gonzalez [] designed and implemented a classifier-based decision support component for ancyber-attacks detection system. This classifier-based cyber-attacks detection system monitored the activities of UNIX machines at multiple levels (from packet to user-level) and determined the correlation among the observed parameters during intrusive activites. This cyber-attacksdetection system can simultaneously monitored network activities at a packet level, process level system level and user level, it can detect both inside misuse and outside attacks. The main emphasis of this work was to examine the feasibility of using a classifier-based intelligent decision support subsystem for robust cyber-attacks detection. The developed system will perform real-time monitoring, analyzing, and generating appropriate response to intrusive activities.

In 2003, CAI Zhong Min GUAN Xiao Hong SHAO Ping PENG Qin Ke SUN GuoJi proposed a new approach to cyber-attacks detection based on rough set theory. The method is based on rough set theory and capable of extracting a set of detection rules with the minimum size to form a normal behavior model from the record of system call sequences generated during the normal execution of a process. It will detect the abnormal operating status of a process and thus report a possible cyber-attacks. The normal behavior model in terms of the sequences of system calls is first defined and how to apply the rough set theory as a powerful data mining tool to establish the model is discussed in this paper. The anomaly detection algorithm based on rough set theory is given in the paper. Compared with other methods, this method requires a smaller size of training data set, less efforts to collect training data and more suitable for real time detection. Experimental results show that this method is better than other methods reported in the literature in terms of detection resolution, required training data set and implementation for real time detection.

In 2004, M.Zang&J.T.Yaoproposed a novel rough set based feature selection approach called Parameterized Average Support Heuristic (PASH). This method is based on parameterized Lower approximation definition in rough sets. It makes use of rough set based heuristic functions.

These heuristic functions are used to decide which attribute is relevant to the target concept. The concepts in the rough set theory can manifest the property of strong and weak relevance .Thisheuristic function is simple and with low time complexity. However, this method only considers the dependency of the selected features. The other important information is ignored. The main advantages of PASH are: It considers the overall quality of the set of potential rules. In other words, it takes into account the average support of rules for every decision class. As a result, PASH produces a set of rules with balanced support distribution over all decision classes. It considers the predictive instances that are excluded by the existing methods. Predictive instances are instances that may produce predictive rules which hold true with a high probability but are not necessarily always true.

In 2005, H. GuneşKayacik, et.al.describes a feature relevance analysis which is performed on KDD 99 training set, which is widely used by machine learning researchers. Feature relevance is expressed in terms of information gain, which gets higher as the feature gets more discriminative. In order to get feature relevance measure for all classes in training set, information gain is calculated on binary classification, for each feature resulting in a separate information gain per class. The research employed decision trees, artificial neural networks and a probabilistic classifier and reported, in terms of detection and false alarm rates, that user to root and remote to local attacks which are very difficult to classify.

In 2006, AnazidaZainal et.al investigated the effectiveness of Rough Set Theory in identifying important features in building ancyber-attacks detection system. They mentioned that there are features that are really significant in classifying the data. Also, it has been proven that there was no single generic classifier that can best classify all the attack types. Instead, in some cases, specific classifier performs better than others. Thus, most of these works on feature selection lead to an ensemble or fusion of multiple classifiers IDS. Authors found that the main contribution of rough set theory is the concept or reducts. A reduct is a minimal subset of attributes with the same capability of objects classification as the whole set of attributes. Reduct computation of rough set corresponds to feature ranking for IDS. The results obtained indicate that the feature subset proposed by Rough Set is robust and has consistent performance throughout the experiment. This may be due to Rough Set Theory which heavily relies on the principle of lower and upper approximation and it suits well with the nature of traffic connection that has a grey area between what is normal and intrusive.

In 2006, Naveen I. Ghali proposed feature selection effective anomaly-based cyber-attacks detection In this paper a new hybrid algorithm RSNNA (Rough Set Neural Network Algorithm) is used to significantly reduce a number of computer resources, both memory and CPU time, required to detect an attack.

This algorithm uses Rough Set theory in order to select out feature reducts and a trained artificial neural network to identify any kind of new attaches. Tests and comparison are done on KDD-99 data set used for The Third International Knowledge Discovery and Data Mining Tools Competition, which was held in conjunction with KDD-99 The Fifth International Conference on Knowledge Discovery and Data Mining, The results showed that the proposed model gives better and robust representation of data as it was able to select features resulting in a 83% data reduction and 85%-90%time reduction and approximately 90%reduction in error in detecting new attacks.

In 2007, Mukkamala& Sung presents an approach based on Neural Networks and Support Vector Machines for Feature Selection for Cyber-attacks Detection. They concerned about using CI-type learning machines for cyber-attacks detection, which is a problem of general interest to transportation infrastructure protection since a necessary task thereof is to protect the computers responsible for the infrastructure's operational control, and an effective Cyber-attacks Detection System (IDS) is essential for ensuring network security. Artificial Neural Networks (ANNs) and Support Vector Machines (SVMs) are the two methods for feature ranking; the first one is independent of the modeling tool, while the second method is specific to SVMs. The two methods are applied to identify the important features in the 1999 DARPA cyber-attacks data set. It is shown that the two methods produce results that are largely consistent.

In 2009, B. Abdullah et.al applied genetic algorithm (GA) to network cyber-attacks detection system. Their approach uses information theory to filter the traffic data and thus reducing the complexity. They use a linear structure rule to classify the network behaviors into normal and abnormal behaviors. The system built is using two types of selected features of the network connections 18 out of 41 features that used for the target operating system (windows) and 31 out of 41 features selected Using information theory to identify the most important features of network connections, that maintaining high detection rate, so it can perform cyber-attacks detection process fast and could be applied to high speed networks.

In 2009, WafaS.Al-Sharafat&ReyadhNaoum make use of SSGBML to enhance the detection rate which is itself a problem in Cyber attacks Detection System (IDS). Steady State Genetic-Based Machine Learning Algorithm (SSGBML) offers the ability to detect cyber attackss especially in changing environments. In SSGBML, Zeroth Level Classifier System (ZCS) plays the role of detector by matching incoming environment message with classifiers to determine whether it is normal or cyber-attacks. Authors present a variety set of features that have been used by different researcher to detect network cyber attackss. These selected features have been used in SSGBML to find which set will give better detection rate than another. The effectiveness of the feature selection will gain better detection rate compared with others.

In 2009, MahbodTavallaeeet.al proposed a new data set, NSL-KDD, which consists of selected records of the complete KDD data set and does not suffer from any of the shortcomings. The important deficiency in the KDD data set is the huge number of redundant records. Hence the NSL-KDD data set does not include redundant records in the train set, so the classifiers will not be biased towards more frequent records. There is no duplicate record in the proposed test sets, therefore, the performance of the learners are not biased by the methods which have better detection rates on the frequent records.

The number of selected records from each difficulty level group is inversely proportional to the percentage of records in the original KDD data set. As a result, the classification rates of distinct machine learning methods vary in a wider range, which makes it more efficient to have an accurate evaluation of different learning techniques. The numbers of records in the train and test sets are reasonable, which makes it affordable to run the experiments on the complete set without the need to randomly select a small portion. Consequently, evaluation results of different research works will be consistent and comparable.

In 2010, AdetunmbiA.Olusola. et.al , presented the relevance of each feature in KDD '99 cyber attacks detection dataset for the detection of each class. Rough set degree of dependency and dependency ratio of each class were employed to determine the most discriminating features for each class. Empirical results showed that seven features were not relevant in the detection of any class. Selection of relevance features was carried out on KDD '99 cyber attacks detection evaluation dataset. Empirical results revealed that some features have no relevance in cyber attacks detection. These features include 20 and 21 (outbound command count for FTP session and hot login) while features 13, 15, 17, 22 and 40 (number of compromised conditions, attempted, number of file creation operations, is guest login, dst host error rate respectively) are of little significant in the cyber attacks detection.

In 2011, Ye Zheng-Wang researched based on clustering technique of cyber attacks detection and introduced the basic concept of several information theory, discussed how to apply the theory of information measurement to measure design data internal regularity of information entrophy, the method combind with clustering model establishment. The author established a data model by obtaining information entrophy clustering inside and clustering between relative entrophy and method of solve the cyber attacks detection based on entrophy clustering problem. A threshold was also

included because of which throughout the cyber attacks detection algorithm played a key role for each record. When it is placed in one clustering o-quinones, it can decide influence on the clustering entrophy thus making the clustering an accurate description.

In 2011, Z. Muda et al presented two methods for anomalous network packet detection based on the data stream mining paradigm. The first of these was an adopted version of the DenStream algorithm for stream clustering specifically tailored to evaluate network traffic. In this algorithm, individual packets are treated as points and are flagged as normal or abnormal based on their belonging to either normal or outlier clusters. The second algorithm utilized a histogram to create a model of the evolving network traffic to which incoming traffic can be compared using pearson correlation.

In 2011, Zachary Miller et al presented two methods for anomalous network packet detection based on the data stream mining. The first of these was an adapted version of the DenStream algorithm for stream clustering specifically tailored to evaluate network traffic in which individual packets were treated as points and were flagged as normal or abnormal based on their belonging to either normal or outlier clusters. The second algorithm utilized a histogram to create a model of the evolving network traffic to which incoming traffic can be compard using pearson correlation.

In 2012, Abhinav S. Raut and Kavita R. Singh analyzed the KDD'99 Cyber attacks Detection Dataset for Selection of Relevance Features. They considered a network based cyber attacks detection system in which the system needs to handle massive amount of network data in real-time. Network data comprises a variety of features, where there exist many irrelevant and redundant features that will drops the cyber attacks detection accuracy. Thus, for improving the anomaly detection accuracy, they implement important rough set based feature selection techniques, in which original data set is reduced to some essential feature subset based on certain defined criterion. First, they describe the Entropy-Based feature reduction technique, in which it determines only those attributes that provides more gain in information. Secondly Open-loop and Closed-loop based feature selection technique is used. Open-loop based feature selection is centered on selection of features based on between-class separability criterion and Closed-loop based feature selection based on feature selection criterion based on predictor performance to select the feature subset.

In 2012, Yogendra Kumar Jain and Upendra[ ] ,proposed an efficient cyber attacks detection based on Decision Tree Classifier Using Feature Reduction .The problem of processing a huge network cyber attacks data is reduced through feature selection to abbreviate the size of the network data involved .The authors analyzed four machine learning algorithms i.e. J48, BayesNet ,OneR,NB of data mining for the task of detecting cyber attackss and compared their relative performances. They found that J48 decision tree is the most suitable associated algorithm than the other three algorithms with high true positive rate & low false positive rate and low computation time with high accuracy.

In 2012, MradulDhakar and Akhilesh Tiwari [ ] proposed a novel hybrid model for IDS. It is a detection mechanism for detecting the intrusive activities hidden among the normal activities. They proposed a framework which may be expected as another step towards advancement of IDS. The framework utilizes the crucial data mining classification algorithms beneficial for cyber attacks detection. It is a hybrid cyber attacks detection framework based on the combination of two classifiers i.e. Tree Augmented Naive Bayes (TAN) and Reduced Error Pruning (REP). The TAN classifier is used as a base classifier while the REP classifier is used as a Meta classifier. The developed framework is an intelligent, adaptive and effective cyber attacks detection framework.

In 2012, Li Hanguang, and Ni Yu discussed an cyber attacks detection technology research based on Apriori algorithm. The author used Apriori algorithm which is the classic of association rules in Web-based Cyber attacks Detection System and applied the rule base generated by the AprioriAgorithm to identify a variety of attacks, improving the overall performance of the detection System. The author proposed an improved Apriori algorithm for cyber attacks detection. Improved algorithm without traversing the database computes support but the algorithm complexity increases while the data is huge taking up considerable memory and processor resources, computation time is not significantly improved.

In 2014, Abhinav S. Raut and Kavita R. Singh [] proposed feature selection for anamoly-Based Cyber attacks Detection using Rough set theory. For improving the anomaly detection accuracy, they are implementing important rough set based feature selection techniques, in which original data set is reduced to some essential feature subset based on certain defined criterion. Discuss the Entropy-Based feature reduction technique, in which it determines only those attributes that provides more gain in information. And another Open-loop and Closed-loop based feature selection technique. Open-loop based feature selection is centered on selection of features based on between-class reparability criterion and Closed-loop based feature selection based on feature selection criterion based on predictor performance to select the feature subset. These algorithms are implemented on KDD CUP 99 data set to obtain the low dimensional feature subset.

REFERENCES

[1] N. Kumari and A. K. Mohapatra, "An insight into digital forensics branches and tools," *Proceedings of theInternational Conference on Computational Techniques in Information and Communication Technologies*, 2016.

[2] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of DigitalEvidence*, vol. 1, no. 3, Fall 2002.

[3] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. San Diego, CA: Academic Press, 3rd edition, 2011, chapter 1.

[4] "Digital forensics," *Wikipedia*, the free encyclopedia,https://en.wikipedia.org/wiki/Digital_forensics.

[5] Dr. V.Tayal," Cyber Piracy in the Indian Information Technology Regime: Issues and Challenges" Cyber Law CybercrimeInternet an E-commerce, By Prof. Vimlendutayal, Bharat.

[6] C. Vidya, "*Cybercrimeto Cyber Terrorism*", Amicus Books, The ICFAI University Press.

[7] Richard Power, "1999 CSI/FBI Computer Crime and Security Survey," Computer Security Issues & Trends, Computer Security Institute, winter 1999.

[8] Denning D E, "An Cyber attacks-Detection Model," In IEEE Transaction on Software Engineering, Vol. Se-13, No. 2, pp. 222-232, February 1987.

[9] Lee, W, Stolfo S and Mok K , "Adaptive Cyber attacks Detection: A Data Mining Approach," In Artificial Intelligence Review, Kluwer Academic Publishers, 14(6), pp. 533 - 567, December 2000.

[10] Satinder Singh, Guljeet Kaur, **"**Unsupervised Anomaly Detection In Network Cyber attacks Detection Using Clusters," Proceedings of National Conference on Challenges & Opportunities in Information Technology RIMT-IET, MandiGobindgarh. March 23, 2007.

[11] Eric Bloedorn , Alan D. Christiansen , William Hill , Clement Skorupka , Lisa M. Talbot , Jonathan Tivel, "Data Mining for Network Cyber attacks Detection: How to Get Started," CiteSeer, 2001

[12] L. Portnoy, "Cyber attacks Detection with Unlabeled Data Using Clustering," Undergraduate Thesis, Columbia University, 2000.

[13] TheodorosLappas and KonstantinosPelechrinis, "Data Mining Techniques for (Network) Cyber attacks Detection Systems," http://citeseerx.ist.psu.edu/viewdoc/ download? doi=10.1.1.120.2533&rep=rep1&type=pdf.

[14] Dewan Md. Farid, NouriaHarbi, SumanAhmmed, Md. Zahidur Rahman, and Chowdhury Mofizur Rahman, "Mining Network Data for Cyber attacks Detection through Naïve Bayesian with Clustering", World Academy of Science, Engineering and Technology, 2010.

[15] The KDD Archive. KDD99 cup dataset, 1999. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[16] [X. Li and N. Ye., "A supervised clustering algorithm for computer cyber attacks detection," Knowledge and Information Systems, 8, pp498-509, ISSN 0219-1377, 2005

[17] Kruegel C., Mutz D., Robertson W., Valeur F., "Bayesian event classification for cyber attacks detection," In: Proceedings of the 19th Annual Computer Security Applications Conference; 2003.

[18] Portnoy L., Eskin E., Stolfo S.J., "Cyber attacks detection with unlabeled data using clustering," In: Proceedings of The ACM Workshop on Data Mining Applied to Security; 2001.

[19] Paxson V., "Bro: A System for Detecting Network Intruders in Real-Time", Computer Networks, 31(23-24), pp. 2435-2463, 14 Dec. 1999.

[20] D.Barbara, J.Couto, S.Jajodia, and N.Wu, "ADAM: A test bed for exploring the use of data mining in cyber attacks detection", SIGMOD, vol30, no.4, pp 15-24, 2001.

[21] P.Domingos, and M.J. Pizzani, "On the optimality of the simple Bayesian classifier under zero-one loss", m/c learning, Vol.29, no2-3, pp 103-130, 1997.

[22] F. Provost, and T. Fawcett, "Robust classification for imprecise environment," Machine Learning, vol. 42/3, 2001, pp. 203-231.

[23] Athanasios Papoulis and S. Unnikrishna Pillai,. "Probability, Random Variables and stochastic Processes ", McGraw-Hill, Fourth Edition, ISBN 0073660116, 2002

[24] P. Kabiri and A.A. Ghorbani, "Research on Cyber attacks Detection and Response: A Survey," International Journal of Network Security, 1, 84-102, September 2005

[25] A. Patcha and J-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Comput. Netw., 51, 3448-3470. ISSN 1389-1286. 2007.

[26] [T.M. Mitchell. Machine Learning. McGraw-Hill. ISBN: 0-07-115467-1, 1997.

[27] [21] N. Ben Amor, S. Benferhat and Z. Elouedi, "Naive Bayes vs Decision Trees in Cyber attacks Detection Systems," Proceedings of the ACM symposium on Applied computing, ISBN 1-58113-812-1, pages 420-424, New York, USA, 2004.

[28] M. Panda and M.R. Patra, "Network cyber attacks detection using naive bayes," IJCSNS International Journal of Computer Science and Network Security, 7, 258-263, 2007

[29] F. Gharibian and A.A. Ghorbani, "Comparative Study of Supervised Machine Learning Techniques for Cyber attacks Detection," In CNSR '07: Proceedings of the Fifth Annual Conference on Communication Networks and Services Research, Pages 350-358, Washington, DC, USA, 2007

[30] L. Portnoy, E. Eskin and S. Stolfo, "Cyber attacks Detection With Unlabeled Data Using Clustering," In Proceedings of the ACM Workshop on Data Mining Applied to Security, 2001.

[31] K. Leung and C. Leckie, "Unsupervised anomaly detection in network cyber attacks detection using clusters," Proceedings of the 28th Australasian conference on Computer Science, ISBN 1-920-68220-1, pages 333-342, Darlinghurst, Australia, Australia, 2005.

[32] W. Wang, X. Guan and X. Zhang, "Processing of massive audit data streams for real-time anomaly cyber attacks detection," Comput. Commun., 31, 58- 72. ISSN 0140-3664, 2008

[33] J. Song, K. Ohira, H. Takakura, Y. Okabe and Y. Kwon, "A Clustering Method for Improving Performance of Anomaly-Based Cyber attacks Detection System," IEICE Transactions on Information and Systems, E91-D, 1282-1291. ISSN 0916-8532, 2008

[34] E.J. Spinosa, A.P. de Leon F. de Carvalho and J. Gama, "Cluster-based novel concept detection in data streams applied to cyber attacks detection in computer networks," Proceedings of the ACM symposium on Applied computing, pages 976-980. ACM. ISBN 978-1-59593-753-7 , New York, NY, USA, 2008

[35] E. Leon, O. Nasaoui and J. Gomez, "Anomaly Detection Based on Unsupervised Niche Clustering with Application to Network Cyber attacks Detection," In Proceedings of the Congress of Evolutionary Computation, 2004.

[36] O. Nasraoui and R. Krishnapuram, "A Robust Estimator Based on Density and Scale Optimization and its Application to Clustering," In Proceedings of the Fifth IEEE International Conference on Fuzzy Systems, volume 2, pages 1031 – 1035, 1999.

[37] Harry Zhang, "The Optimality of Naive Bayes". FLAIRS conference 2004.

[38] Caruana, R. and Niculescu-Mizil, A., "An empirical comparison of supervised Learning algorithms". Proceedings of the 23rd international conference on Machine learning, 2006.

[39] George H. John and Pat Langley, "Estimating Continuous Distributions in Bayesian Classifiers," Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence. pp. 338-345. Morgan Kaufmann, San Mateo, 1995.
[40] An Overview of Issues in Testing Cyber attacks Detection Systems, http://www.net-security.org/article.php?id=528, 2003.
[41] [35] ShengYi Jiang, Xiaoyu Song, Hui Wang, Jian-Jun Han, Qing-Hua Li, "A clustering-based method for unsupervised cyber attacks detections", Pattern Recognition Letters 27 (2006) 802–810.
[42] SandhyaPeddabachigari, Ajith Abraham, CrinaGrosan, Johnson Thomas, "Modeling cyber attacks detection system using hybrid intelligent systems", Journal of Network and Computer Applications 30 (2007) 114–132.
[43] Cheng Xiang, Png Chin Yong, Lim SweeMeng, "Design of multiple-level hybrid classifier for cyber attacks detection system using Bayesian clustering and decision trees", Pattern Recognition Letters 29 (2008) 918–924.
[44] Arman Tajbakhsh, Mohammad Rahmati, AbdolrezaMirzaei, "Cyber attacks detection using fuzzy association rules", Applied Soft Computing 9 (2009) 462–469.
[45] B. Abdullah, I. Abd-alghafar, Gouda I. Salama and A. Abd-alhafez, "Performance Evaluation of a Genetic Algorithm Based Approach to Network Cyber attacks Detection System", 13th International Conference on Aerospace Sciences & Aviation Technology, ASAT- 13, May 26 – 28, 2009.
[46] Kamran Shafi, Hussein A. Abbass, "An adaptive genetic-based signature learning system for cyber attacks detection", Expert Systems with Applications 36 (2009) 12036–12043.
[47] Shi-Jinn Horng, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai,CitraDwiPerkas, "A novel cyber attacks detection system based on hierarchical clustering and support vector machines", Expert Systems with Applications 38 (2011) 306–313.
[48] Muamer N. Mohammad, NorrozilaSulaiman, Osama AbdulkarimMuhsin, "A Novel Cyber attacks Detection System by using Intelligent Data Mining in Weka Environment", Procedia Computer Science 3 (2011) 1237–1242.
[49] Z. Muda, W. Yassin, M. N. Sulaiman and N. I. Udzir, "A K-Means and Naïve Bayes Learning Approach for Better Cyber attacks Detection", Information Technology Journal, Vol. 10 No. 3, pp: 648-655, 2011.
[50] HeshamAltwaijry and Saeed Algarny, "*Bayesian based cyber attacks detection system"*, Journal of King Saud University – Computer and Information Sciences, Vol. 24, pp: 1–6, 2012.
[51] Li Hanguang and Ni Yu, "*Cyber attacks Detection Technology Research Based on Apriori Algorithm*", Elsevier, Physics Procedia, Vol. 24, pp: 1615-1620, 2012.
[52] Manikandan R., Oviya P and Hemalatha C, "*A New Data Mining Based Network Cyber attacksDetection Model*", Journal of Computer Application, Vol. 5, No. EICA2012-1, pp: 1-10, 2012.
[53] VikasMarkam, Lect. Shirish Mohan Dubey, "General Study of Associations rule mining in Cyber attacks Detection System", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, January 2012.
[54] NanditaSengupta, JaydeepSen, JayaSil, MoumitaSaha, "Designing of on line cyber attacks detection system using rough set theory and Q-learning algorithm", Neurocomputing 111 (2013) 161–168.
[55] Quinlan, J.R., 1993. C4.5: Programs for Machine Learning. Morgan Kauffman.
[56] Resendez,PMartinezandJAbraham,"AIntrodution to Digital Forensics," June 2014, https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics

