Artificial intelligence techniques to achieve Cyber Security: An Emerging Challenge in e-Governance

Dipen Saini
DAV College, Jalandhar

Abstract **-** Information and communication technology refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, transmission systems and network based control and monitoring systems. Now days, Information and communication technology has provided us ways for faster and better communication, retrieval of data and utilization of information to its users. E-governance is basically the application of ICT which provides government services to the citizens through internet. In developing countries like India where literacy rate is quite low, people are not aware about the benefits of ICT and e-Governance so they do not use ICT to much extent and are not much aware about the benefits of e-Governance services to them. There are large numbers of obstacles in implementing e-Governance in India. There exists many challenges in e-Governance like poverty, Lack of technical knowledge, Language Dominance, Services are not accessible everywhere. Besides these challenges, one of the biggest challenges for all the companies which provide online services to the public is Cyber security. Cyber security is an emerging challenge for E-governance and E-commerce. This paper highlights on cyber threats and cyber security. In this paper, I have described some data mining and machine learning techniques to achieve cyber security.

Keywords: ICT, E-governance, Cyber threats, Cyber security, Data mining, Machine learning techniques.

I. INTRODUCTION

E-governance or electronic governance refers to use of Information and Communication Technologies (ICT) to provide various types of government services and information to citizens and organisations. In other words we can say that e-Governance involves ICT, especially internet, to improve the way of delivering government services to citizens and, various government organisations. E-governance is not limited to public sector only, it also includes private sector .Internet plays a vital role in e-Governance in providing all the government services to the citizens and organisations. The use of internet not only provides better and faster way of services but also brings transparency between the government and the citizens. In developed countries it is very easy for the government to provide its services to the citizens via means of internet, but in developing countries like India where literacy rate is very low and most of the people living below poverty line, it is very difficult for the government to provide its services to the citizens by means of internet. [1]

II. CHALLENGES IN E-GOVERNANCE

It's very difficult to implement e-Governance in India. There are large number of obstacles in the implementation of e-Goverance in India.Some of the major challenges in the implementation of e-Governance is as follows: [2]

a) *Language problem:* E-governance applications are implemented in programming languages which are written in English language and, English language may not be easily understandable and written by most of the people so diversity of people in context of language is a huge challenge for implementing e-Governance. India is a country where people belong to different states speak different languages, so it becomes a challenge for the government to write e-Governance applications which are to be implemented for the whole nation in more than one language.

b) *Poverty:* We all know that most of the people living in India are below poverty line so Internet access is too expensive for the poor in developing countries like India. Installing the necessary telephone lines needed for internet or email access is equally unaffordable in most poor countries.

c) *Literacy rate:* Literacy can be defined as the ability to read and write with understanding in any language. Literacy rate of India is very low, a huge obstacle in the implementation of e-Governance projects. Illiterate people are not able to access the e-Governance applications and it's very difficult to train them how to use e-Governance applications, hence the projects do not get much success. Much of the Indian people are not literate and those who are literate, they do not have much knowledge about Information Technology (IT) which is a combination of internet and computer. Most of the people in India are not much aware about the usage of Information Technology. In India, having such low rate of IT literacy, it is very difficult to implement e-Governance. We can say that IT illiteracy is a major obstacle in the implementation of e-Governance in India. So, if we want to implement e-Governance successfully in India, first of all Indian people must be made aware about the usage of Information Technology.

d) *Services are not easily accessible:* The concept of e-Governance is claiming for increased efficiency and effectiveness of the government, but these goals will be achieved only if the service will be available to the 100% of the citizens. So, every service should be accessible by anybody from anywhere and anytime. Even if the users of Internet are growing but still there is a major part of Indian population which is not able to access e-Governance activities for variety of reasons, e.g. some people may have limited access to Information and

Communication Technologies and devices. Therefore, government has to provide internet access through public terminals as a part of their universal access efforts.

e) *Privacy and security:* A critical obstacle in implementing e-Governance is the privacy and security of an individual's personal data that he/she provides to the e-Governance applications to obtain government services. With the implementation of e-government projects, some effective measures must be taken to protect the personal information of the people. Lack of security standards can make the hackers, hack someone's personal information and misuse it. So, lack of security standards will limit the use of e-Government projects and it will effect on the development of new e-Government projects.

f) *Cyber security:* Now days, Cyber security is the biggest problem for all the organisations providing online services to the public. Cyber security is basically a solution to cyber threats or we can say cyber attacks. Cyber-attack is any type of offensive manoeuvre employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. Thus, cyber security is an emerging challenge in e-Governance.

III. CYBER SECURITY

Now days, hackers are utilizing personal computers remotely to conspire, proselytize, recruit accomplices, raise funds, and collude during ongoing attacks. Adversarial governments and agencies can launch cyber attacks on the hardware and software of the opponents' cyber infrastructures by supporting financially and technically malicious network exploitations. Cyber criminals threaten financial infrastructures, and they could pose threats to national economies if recruited by the adversarial agents or terrorist organizations. Similarly, private organizations, e.g., banks, must protect confidential business or private information from such hackers. For example, the disclosure of business or private financial data to cyber criminals can lead to financial loss via Internet banking and related online resources. In the pharmaceutical industry, disclosure of protected company information can benefit competitors and lead to market-share loss. Individuals must also be vigilant against cyber crimes and malicious use of Internet technology. [3]

To secure cyber infrastructure against intentional and potentially malicious threats, growing collaborative effort between cyber security professionals and researchers from institutions, private industries, academia, and government agencies has engaged in exploiting and designing a variety of cyber defense systems. Cyber security researchers and designers aim to maintain the confidentiality, integrity, and availability of information and information management systems through various cyber defense systems that protect computers and networks from hackers who may want to intrude on a system or steal financial, medical, or other identity-based information.

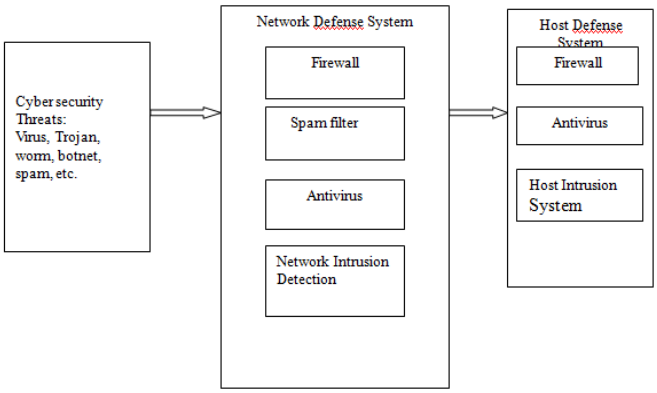

Fig.3.1 Conventional cyber security system

As shown in Figure 3.1, conventional cyber security systems address various cyber security threats, including viruses, Trojans, worms, spam, and botnets. These cyber security systems combat cyber security threats at two levels and provide network- and host-based defenses. Network-based defense systems control network flow by network firewall, spam filter, antivirus, and network intrusion detection techniques. Host-based defense systems control upcoming data in a workstation by firewall, antivirus, and intrusion detection techniques installed in hosts.[4]

Conventional approaches to cyber defense are mechanisms designed in firewalls, authentication tools, and network servers that monitor, track, and block viruses and other malicious cyber attacks. For example, the Microsoft Windows operating system has a built-in Kerberos cryptography system that protects user information. Antivirus software is designed and installed in personal computers and cyber infrastructures to ensure customer information is not used maliciously. These approaches create a protective shield for cyber infrastructure.

Many higher-level adaptive cyber defense systems can be partitioned into components as shown in Figure 3.2. Figure 3.2 outlines the five-step process for those defense systems. Each step is discussed below:

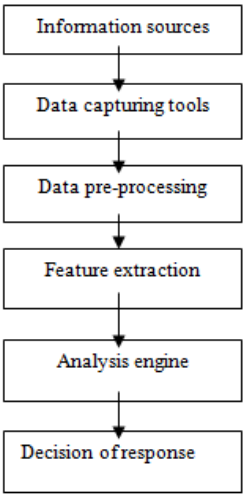

Fig.3.2 Adaptive defense system for cyber security

Data-capturing tools, such as Libpcap for Linux, Solaris BSM for SUN, and Win cap for Windows , capture events from the audit trails of resource information sources (e.g., network). Events can be host-based or network-based depending on where they originate. If an event originates with log files, then it is categorized as a host-based event. If it originates with network traffic, then it is categorized as a network-based event. A host-based event includes a sequence of commands executed by a user and a sequence of system calls launched by an application, e.g., send mail. A network-based event includes network traffic data, e.g., a sequence of internet protocol (IP) or transmission control protocol (TCP) network packets. The data-pre-processing module filters out the attacks for which good signatures have been learned.[5]

A feature extractor derives basic features that are useful in event analysis engines, including a sequence of system calls, start time, duration of a network flow, source IP and source port, destination IP and destination port, protocol, number of bytes, and number of packets. In an analysis engine, various intrusion detection methods are implemented to investigate the behaviour of the cyber infrastructure, which may or may not have appeared before in the record, e.g., to detect anomalous traffic. The decision of responses is deployed once a cyber attack is identified. As shown in Figure 3.2, analysis engines are the core technologies for the generation of the adaptation ability of the cyber defense system. As discussed above, the solutions to cyber security problems include proactive and reactive security solutions.

a) *Proactive security solutions:* Proactive approaches anticipate and eliminate vulnerabilities in the cyber system, while remaining prepared to defend effectively and rapidly against attacks. To function correctly, proactive security solutions require user authentication (e.g., user password and biometrics), a system capable of avoiding programming errors, and information protection [e.g., privacy-preserving data mining (PPDM)].PPDM protects data from being explored by data-mining techniques in cyber security applications.

b) *Reactive security solutions:* The second line of cyber defense is composed of reactive security solutions, such as intrusion detection systems (IDSs). IDSs detect intrusions based on the information from log files and network flow, so that the extent of damage can be determined, hackers can be tracked down, and similar attacks can be prevented in the future.

IV. DATA MINING AND MACHINE LEARNING

a) Data mining

Due to the availability of large amounts of data in cyber infrastructure and the number of cyber criminals attempting to gain access to the data, data mining, machine learning, statistics, and other interdisciplinary capabilities are needed to address the challenges of cyber security. Because IDSs use data mining and machine learning, we will focus on these areas. Data mining is the extraction, or "mining," of knowledge from a large amount of data. The strong patterns or rules detected by data-mining techniques can be used for the nontrivial prediction of new data. In nontrivial prediction, information that is implicitly presented in the data, but was previously unknown is discovered. Data-mining techniques use statistics, artificial intelligence, and pattern recognition of data in order to group or extract behaviours or entities. Thus, data mining is an interdisciplinary field that employs the use of analysis tools from statistical models, mathematical algorithms, and machine learning methods to discover previously unknown, valid patterns and relationships in large data sets, which are useful for finding hackers and preserving privacy in cyber security. [5]

Data mining is used in many domains, including finance, engineering, biomedicine, and cyber security. There are two categories of data-mining methods: supervised and unsupervised. Supervised data-mining techniques predict a hidden function using training data. The training data have pairs of input variables and output labels or classes. The output of the method can predict a class label of the input variables. Examples of supervised mining are classification and prediction. Unsupervised data mining is an attempt to identify hidden patterns from given data without introducing training data (i.e., pairs of input and class labels). Typical examples of unsupervised mining are clustering and associative rule mining. [6]

b) Machine learning

Learning is the process of building a scientific model after discovering knowledge from a sample data set or data sets. In machine learning, A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E. For example, a computer program that learns to play checkers might improve its performance as measured by its ability to win at the class of tasks involving playing checkers games, through experience obtained by playing games against it. In general, to have a well-defined learning problem, we must identity these three features: the class of tasks, the measure of performance to be improved, and the source of experience. [8]

A checkers learning problem:

Task T: playing checkers

Performance measure P: percent of games won against opponents

Training experience E: playing practice games against itself

Machine-learning methods use training patterns to learn or estimate the form of a classifier model. The models can be parametric or unparametric. The goal of using machine-learning algorithms is to reduce the classification error on the given training sample data. The training data are finite such that the learning theory requires probability bounds on the performance of learning algorithms. Depending on the availability of training data and the desired outcome of the

learning algorithms, machine-learning algorithms are categorized into **supervised learning** and **unsupervised learning.**

Supervised learning

In supervised learning, pairs of input and target output are given to train a function, and a learning model is trained such that the output of the function can be predicted at a minimum cost. Let us say we want to learn the class C, of a "family car." We have a set of examples of cars, and we have a group of people that we survey to whom we show these cars. The people look at the cars we show them and label them, the cars that they believe are family cars are positive examples and the other cars are negative examples. Class learning is finding a description that is shared by all positive examples and none of the negative examples. Doing this, we can make a prediction: Given a car that we have not seen before, by checking with the description learned, we will be able to say whether it is a family car or not. Or we can do knowledge extraction: This study may be sponsored by a car company, and the aim may be to understand what people expect from a family car. After some discussions with experts in the field, let us say that we reach the conclusion that among all features a car may have, the features that separate a family car from other cars are the price and engine power. These two attributes are the inputs to the class recognizer. Note that when we decide on this particular input representation, we are ignoring various other attributes as irrelevant. Though one may think of other attributes such as seating capacity and colour that might be important for distinguishing among car types, we will consider only price and engine power to keep this example simple. [7]

The supervised learning methods are categorized based on the structures and objective functions of learning algorithms. Popular categorizations include artificial neural network (ANN), support vector machine (SVM), and decision trees.

Support vector machine

The main purpose of a support vector machine is to produce a separation boundary (linear or otherwise) in a feature space such that subsequent observations can be automatically classified into separate groups. A good example of such a system is classifying a set of documents into positive or negative sentiment groups. Similarly, we could classify emails into spam or non-spam. SVM's are based on the concept of an optimal separating hyper plane, which motivates a simple type of linear classifier known as a maximal margin classifier.

Unsupervised learning

In unsupervised learning, no target or label is given in sample data. Unsupervised learning methods are designed to summarize the key features of the data and to form the natural clusters of input patterns given a particular cost function. The most famous unsupervised learning methods include k-means clustering, hierarchical clustering, and self-organization map. Unsupervised learning is difficult to evaluate, because it does not have an explicit teacher and, thus, does not have labelled data for testing.

V. Proactive security solutions

Traditionally, proactive security solutions are designed to maintain the overall security of a system, even if individual components of the system have been compromised by an attack. Recently, the improvement of data-mining techniques and information technology brings unlimited chances for Internet and other media users to explore new information. The new information may include sensitive information and, thus incur a new research domain where researchers consider data-mining algorithms from the viewpoint of privacy preservation. This new research, called PPDM is designed to protect private data and knowledge in data mining. PPDM methods can be characterized by data distribution, data modification, data-mining algorithms, rule hiding, and privacy preservation techniques.

The objective of PPDM is to prevent unauthorized users from accessing private information, such as private data-mining or machine-learning results. Privacy preservation and data mining worked in parallel. In PPDM, researchers adopt a large number of privacy preservation techniques in data-mining and machine-learning algorithms to preserve knowledge security.

PPDM methods consist of six procedures: modification of the original data for privacy preservation, collection of data, modification of the aggregated data for privacy preservation, PPDM algorithms, reconstruction of the mining results for individual data points, and performance evaluation of the PPDM result. The modification of the original data points attempts to avoid the breach of sensitive information in the individual data points or the privacy violation of participants. In contrast to the commonly employed data mining or machine learning methods, PPDM requires the input to be modified. After collecting the data, the aggregated data needs to be further processed so that the data source ID or other private information is blocked.

VI. REACTIVE SECURITY SOLUTIONS

Cyber intrusion is defined as any unauthorized attempt to access, manipulate, modify, or destroy information or to use a computer system remotely to spam, hack, or modify other computers. An IDS intelligently monitors activities that occur in a computing resource, e.g., network traffic and computer usage, to analyze the events and to generate reactions. In IDSs, it is always assumed that an intrusion will manifest itself in a trace of these events, and the trace of an intrusion is different from traces left by normal behaviours. To achieve this purpose, network packets are collected, and the rule violation is checked with pattern recognition methods. An IDS system usually monitors and analyzes user and system activities, accesses the integrity of the system and data, recognizes malicious activity patterns, generates reactions to intrusions, and reports the outcome of detection. The activities that the IDSs trace can form a variety of patterns or come from a variety of sources. According to the detection principles, we classify intrusion detection into the following modules: misuse/signature

detection, anomaly detection algorithms, hybrid detection, and scan detector and profiling modules. Furthermore, IDSs recognize and prevent malicious activities through network- or host-based methods. These IDSs search for specific malicious patterns to identify the underlying suspicious intent. When an IDS searches for malicious patterns in network traffic, we call it a network-based IDS. When an IDS searches for malicious patterns in log files, we call it host-based IDS.

a) Misuse/ Signature Detection

Misuse detection, also called signature detection, is an IDS triggering method that generates alarms when a known cyber misuse occurs. A signature detection technique measures the similarity between input events and the signatures of known intrusions. It flags behaviour that shares similarities with a predefined pattern of intrusion. Thus, known attacks can be detected immediately and realizably with a lower false-positive rate. However, signature detection cannot detect novel attacks.**SVM technique can be used at network and ANN technique used at host level.**

b) Anomaly Detection

Anomaly detection triggers alarms when the detected object behaves significantly differently from the predefined normal patterns. Hence, anomaly detection techniques are designed to detect patterns that deviate from an expected normal model built for the data. In cyber security, anomaly detection includes the detection of malicious activities, e.g., penetrations and denial of service. The approach consists of two steps: training and detection. In the training step, machine-learning techniques are applied to generate a profile of normal patterns in the absence of an attack. In the detection step, the input events are labelled as attacks if the event records deviate significantly from the normal profile. Subsequently, anomaly detection can detect previously unknown attacks. However, anomaly detection is hampered by a high rate of false alarms. Moreover, the selection of inappropriate features can hurt the effectiveness of the detection result, which corresponds to the learned patterns. In extreme cases, a malicious user can use anomaly data as normal data to train an anomaly detection system, so that it will recognize malicious patterns as normal.**SVM technique can be used at network and ANN technique used at host level.**

c) Hybrid Detection

Most current IDSs employ either misuse detection techniques or anomaly detection techniques. Both of these methods have drawbacks: misuse detection techniques lack the ability to detect unknown intrusions; anomaly detection techniques usually produce a high percentage of false alarms. To improve the techniques of IDSs, researchers have proposed hybrid detection techniques to combine anomaly and misuse detection techniques in IDSs. Examples for hybrid detection techniques are **ANN technique can be used both at host level and network level.**

d) Scan Detection

Scan detection generates alerts when attackers scan services or computer components in network systems before launching attacks. A scan detector identifies the precursor of an attack on a network, e.g., destination IPs and the source IPs of Internet connections. Although many scan detection techniques have been proposed and declared to be able to detect the precursors of cyber attacks, the high false-positive rate or the low scan detection rate limits the application of these solutions in practice. Some examples of scan detection techniques are **Rule based technique can be used for both host and network level.**

VII. A CASE STUDY USING MISUSE/ DETECTION SIGNATURE

a) Misuse/Signature Detection

Misuse detection, also called signature detection, is used to recognize specifically unique patterns of unauthorized behaviour to predict and detect subsequent similar attempts. These specific patterns, called signatures, include patterns of specific log files or packets that have been identified as a threat. Each file is composed of signatures, which are unique arrangements of zeros and ones. For example, in a host based intrusion detection system (IDS), a signature can be a pattern of system calls.

In network-based IDS, a signature can be a specific pattern of the packet such as packet content signatures and/or header content signatures that can indicate unauthorized actions such as improper FTP initiation. The packet includes source or destination IP addresses, source or destination TCP/UDP ports, and IP protocols such as UDP, TCP, and ICMP, and data payloads. As shown in Figure 7.1, misuse/signature detection methods match the learned patterns and signature of attacks to identify malicious users. If the learned patterns and signature of attacks match, the system will alert the system administrator that a cyber attack has been detected. Then, the administrator will attempt to label the attack. The related information will be delivered to an administrator. For example (see Figure 7.1), if we have an attack signature as "Login name = 'Dipen'," then, when any data matches this signature, the system will alert the administrator that anomalous events have been detected. Signature detection methods typically search for known potentially malicious information by scanning cyber infrastructure and, thus, make decisions based on a significant amount of prior knowledge of the attack signatures. For these solutions to work, the security software will need to obtain collections of known cyber attack characteristics. Therefore, the quality and reliability of the signature detection results rely on the frequent updating of the signature database. For example, antispyware tools usually use signature detection techniques to find malicious software embedded in a computational system. When a signature-based antispyware tool is active, it scans files and programs in the system and compares them with the signatures in the database. If there is a match, the tool will alert the system administrator that spyware has been detected and will provide information associated with the spyware, such as the name of the software, the danger level, and the location of the spyware, to cyber administrators. This technique often locates known threats. However, this

technique may cause false alarms. A false alarm is an instance in which an alert occurs although unauthorized access has not been attempted. For example, a user may forget a login password and make multiple attempts to sign into an account. Most site accounts lock for 24 h after three failed login attempts. Attempts after this point can be regarded as attacks. Depending on the robustness and seriousness of a triggered signature, an alarm or notification will be reported to the proper authorities.

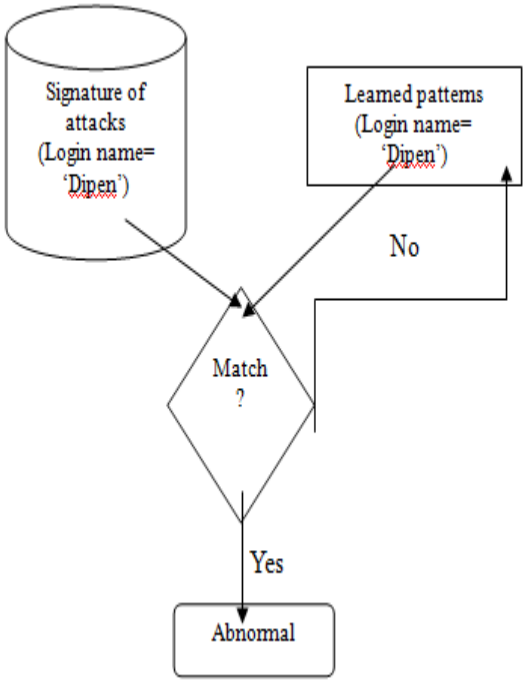

Fig.7.1 Misuse detection using "if-then" rules

b) Machine Learning in Misuse/Signature Detection

As shown in Figure 7.2, a typical misuse/signature detection system consists of five steps: information collection, data pre-processing, misuse/signature identification by matching methods, rules regeneration, and denial of service (DoS) or other security response. The data resources include cyber attribute data such as audit log, network packet flow, and windows registry. Data pre-processing prepares input data for pattern learning by reducing noises and normalizing, selecting, and extracting features. Once these steps have been performed, domain experts or automatic intelligent learning systems build intrusive learning models, such as rule-based expert systems, based on prior knowledge of malicious code and data and vulnerabilities in cyber infrastructures. Then, we can apply the learned classification models or rules to the incoming data for misuse pattern detection. If any cyber information is found to be similar to the attack patterns in an apriority rule, then decisions will be made automatically by software or manually by cyber administrators after further analysis. Consequently, misuse/signature detection can be simply understood as an "if–then" sequence as shown in Figure 7.1.

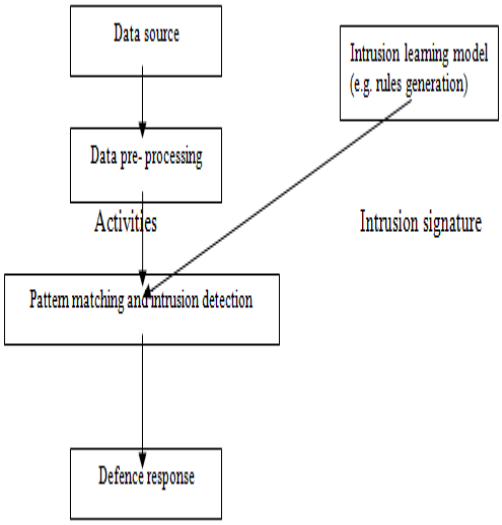

Fig.7.2 Workflow of misuse/signature detection system

Machine-learning methods play several core roles in misuse detection systems. These approaches can provide feature selection in the data pre-processing step and help build rules or perform pattern classification and recognition in signature identifications. As shown in Figure 7.2, machine-learning algorithms can improve pattern matching and intrusion detection by intelligently comparing the misuse/signature patterns with the collected cyber information. As the training data for the build-up of rules or other machine-learning models are labelled as normal, anomalous, or as specific attack types, most of the machine-learning methods employed in misuse detection systems are supervised. Subsequently, these detection techniques rely on the similarity measure between input events and the signatures of known intrusions. They flag the event that is close to a predefined pattern of intrusion. Thus, known attacks can be detected immediately and realizably with a lower false-positive rate. However, signature detection is ineffective for detecting novel attacks.

c) Misuse/Signature Detection using Machine learning technique (SVM)

The SVM conducts structural risk minimization, e.g., true error on unseen examples, while ANN focuses on empirical risk minimization. Subsequently, SVM selects a number of parameters based on the requirement of the margin that separates the data points but not based on the number of feature dimensions. This feature allows SVM to be compatible with more applications. SVM has two significant advantages over ANN when applied in intrusion detection: speed and scalability. Speed is important for real-time detection, and scalability is important for the huge cyber infrastructure information flow. In addition, SVM is capable of updating training patterns dynamically. This feature is important when attack patterns change.

In S. Mukkamala, G. Janoski, and A. H. Sung (2002), SVM was applied to identify attack and misuse patterns associated with computer security breaches, such as consequence of

system software bugs, hardware or software failures, incorrect system administration procedures, or failure of the system authentication. SVM intrusion detection procedures include three steps: first, input and output pairs must be extracted from the user logs, web servers, and the authority log. Second, the SVM model is trained over the numerical data obtained in the first step, and third, the classification ability of SVM model is tested. The raw information that originates in system log files of user activities consists of various types of attributes related to command, HTTP, and class labels normal or anomalous. Weights were assigned to system commands and user activities to indicate the potential status as an anomaly. For example, an rm (command of remove) command received a weight of four and a rm − r* was (remove everything in a directory and include the removed material in its subdirectory) assigned a weight of five, because the second weight posed a greater threat to the system. For example, in HTTP activities, "Read only actual html pages or images" were assigned weight of one, while "Read and attempt to access directory pages" were assigned a weight of two. "Read and attempt to access directory pages" received a higher weight because it may be related to malicious queries to the server. [9]

Mukkamala et al. (2002) presented a training set of 699 data points that contained actual attacks, probable attacks, and normal patterns. Eight features were obtained after pre-processing, and all the data values were normalized to [0, 1]. The testing set consists of 250 data points and eight features. The estimated precision was better than 85.53% on the training data set and 94% on the testing data set. SVM proved to be more efficient in the training and running processes than ANN. This experiment demonstrated that SVM could simulate security scenarios using the SVM component to adapt to individual information systems, to provide real-time detection, and to minimize false alarms immediately after detecting true attacks.

VIII. CONCLUSION

It's very difficult to implement e-Governance in India as there are large numbers of obstacles in the implementation of e-Governance in India. Out of all, cyber security is an emerging challenge in the implementation of e-Governance. Cyber security is not limited to e-Governance only; it is an emerging challenge for all the companies and organisations which provide online services via internet to the public and other organisations. In this paper, I have discussed different types of cyber security solutions and mentioned data mining and machine learning techniques like PPDM, support vector machine (SVM), artificial neural network (ANN) to achieve cyber security more efficiently.

IX. REFERENCES

[1] Pardeep Mittal, Amandeep kaur. E-Governance – A challenge in India, International journal of Advanced Research in computer Engineering & technology, ISSN-2278-1323, vol.2 issue 3, pp 1196-1199, March 2013.
[2] Pooja agrawal et al. Security issues of E-Governance, International Journal of Advances in Computer Networks and Security.
[3] Sen gupta et al. e-Commerce security – A life cycle approach, Journal of Indian Academy of Sciences, vol.30, pages 119-140, 2005.
[4] Shailendra Singh, Sanjay Silakari. A Survey of Cyber Attack Detection Systems, International Journal of Computer Science and Network Security, ISSN-1738-7906, Vol.9 No.5, pp1-10, May 2009.
[5] Xindong Wu, Gong Wu, Wei Ding. Data miming with big data, IEEE transactions on Knowledge and Data engineering, ISSN 1041-4347, page 97-107, 2013.
[6] Ian H.Witten and Eibe Frank. Data mining – Practical Machine Learning tools and techniques. Morgan Kaufmann Publishers.
[7] Ethem Alpaydin. Introduction to Machine learning.MIT Press, Cambridge.
[8] Tom M.Mitchell. Machine Learning. McGraw-Hill Science.
[9] S.Mukkamala, A.H. Sung. Intrusion detection using support vector machine. In Proceedings of Advanced Simulation Technologies Conference, pp.178-183, 2002.

I am Dipen saini working as an Assistant Professor in Dav college,Jalandhar. My Research areas are Software testing, swarm intelligence, Artificial intelligence.