A review on Cybersecurity and its challenges

Madhusmita Rout
Department of Computer Science and Engineering
Lovely Professional University, Punjab

Amandeep Kaur
Department of Computer Science and Engineering,
Lovely Professional University, Punjab.

Abstract- The emerging of new technology is making easier for people to access things in seconds just like the platform of the internet as it has become a crucial part of everyone's life. It enables people to share information worldwide very fast. But the most challenging here is the security of systems as cyber-crimes are increasing day by day. Cyber threats are now very complex and evasive. Though many organizations have come forward with various solutions using different tools as privacy is a major concern for the data amount is very large to handle nowadays and regular updates are required to confront such attacks. This paper focuses on an analysis of cybersecurity and its challenges with the application of different strategies implementations.

keywords- cybersecurity, cyber-crimes, attacks, IoT, block chain.

I. INTRODUCTION

As we know, information security is very important so proper measures and updating services are offered. It generally means to protect the data and reduce the probability of attacks [1]. A possible risk could be transferred or reduced or accept it but the risk management is calculated before taking such a step. Overall cybersecurity is a bit costlier so the risk of compromise is evaluated based on the financial status of an organization. The goal is to provide better security to all the systems and its confidentiality, integrity, and availability of data [1]. The vulnerabilities are specified based on the means of attack. Today everything is so dependent upon the internet that cyberspace was introduced for IT systems which provides a lot of benefits [2]. As the developments of new technologies are very rapid the risks of being affected are also high which is very difficult to maintain. Cybersecurity compromise is a huge loss for any industry so the possibilities of attacks and the consequences are observed regularly. Efficient methodologies are being adopted by a different organization to prevent such acts because data breaches have become very common and the intruders can be from both inside and outside. It is a dangerous risk because it is connected to the government sector, public sector, health sector, financial platforms, etc... The loss because of cyber-attacks is very high now mostly due to ransomware attacks. As attacks are now multi vectored and very difficult to trace the source of attacks. So information technology security specialists are employed in every organization. The number of professionals is very less in a cybersecurity department as per the needs of a sector. Now a day's various programs related to it are encouraged to be enrolled through various courses. The primary focus is to make aware people about the importance of security as usual as the privacy of each individual. Recently, block chain has gained popularity for its security features thus using it for cybersecurity is considered for IoT, smart cities, cloud computing, etc [3] [4].

1.1 CYBERSECURITY

Cybersecurity means to provide overall protection to the cyberspace. It is an essential part of an organization. It is used to prevent hackers from doing any unauthorized access to a confidential platform. Globally, it is expected to cost 133$ billion by 2021. The attacks could be carried out in any networks or computers by spreading viruses, malware, etc. It is very important to protect data from such attacks. Most IoT devices are vulnerable and also people are victims by malware delivered to their emails. Many people fall into such traps and frauds because of no awareness of cybersecurity. All the organizations have a separate department for it so to prevent any form of security compromise. Cybersecurity includes parameters like,

- identify threats
- identify vulnerabilities
- access and calculate the risk
- respond to the incidents
- strategies and plans
1.2 CYBERCRIMES AND ATTACKS

Cybercrime can be said as an illegal activity that includes identity theft, data breaches by breaking into a network or any computer systems [5]. It happens because the hackers want to get illegal access to the personal data of people for stealing money or compromise their systems for benefits etc. In the IT sector, cyber-crimes are very frequent. Cyber-attacks include DOS, probing, attacks on MANET, VANET and Wireless sensor networks, malware, viruses, phishing, hacking, spamming, etc... which is launched either by a passive or active attack [5] [6]. The motivation behind an attack could be intentional like Cyber Espionage, Cyberwarfare or Hacktivism [6]. As the frequency of cyber-attacks is increasing, various solutions and patches are being experimented for finding an efficient way to deal with cyber-attacks. The applications of artificial intelligence are widely used. Now AI is being introduced with methods likes Pattern Recognition, (ANN) Artificial Neural Networks, Speech recognition, Computational Intelligence, Machine Learning, Deep learning, Fuzzy logic, Intelligent Agents, etc... for finding an optimal solution to Cybercrimes activities [7]. Data mining is a subfield of AI which helps to extract such data which can help to show unusual behaviour of a particular case. There are many available tools for evaluating these problems. It includes methods basically as Association Rules, clustering analysis, outlier detection approaches [8].

One of the most dangerous cyber-attacks is recorded to be "WannaCry" which was launched by attackers on 13th may, 2017 by spreading a ransomware crypto worm with a demand of 300S-600$ by bitcoin that affected around 200000 computers in 150 countries [9].

II. RELATED WORKS

Khatoun et al. [10] discussed various factors regarding cybersecurity in smart cities which compromises of many sectors like government, health, transportation, etc... as industrial control systems are mostly connected to the internet. They have presented a table related to many projects and initiatives started by different countries. The characteristics of security standards in an organization must be in terms of organizational, technical and legal. Recommendations for various security standards are given.

Belgaum et al. [11] presented a framework using the Analytic Hierarchy Process approach to show how much areas of a smart city that is affected in terms of cybersecurity challenges. They have collected data from questionnaires, experts and considered nine factors. Then they have measured the weight of each factor and found that the smart security factor is the most important and the smart building factor is the least significant area with 0.058%. This research can help to identify the weightage of the areas to determine various solutions for the security challenges.

Tounsi et al. [12] surveyed technical threat intelligence(TTI) in cyber-attacks and classified the TTI into different sub-domains. As the traditional approaches i.e. heuristic and signature are not sufficient to solve the present complex problems, industries are now employing quality standards tools for the multi- vectored cyber-attacks which has to be much reliable and resistant. The TTI tools are categorized as per the needs required for an organization to meet its standards.

Moore et al. [13] developed a novel method to detect cyber-attacks happening through electronic control units (ECUs) in vehicles which shown an accuracy of over 90%. They have applied machine learning techniques with a state modelling approach that developed an intrusion detection system (IDS) that uses utilizes a convolution neural network for the detection of unusual requests of data pairs and controller area network bus commands. The IDS is based on controller area network (CAN) data for image conversion(2D). The data is taken from a CAN bus which shows the data of a compromised electronic control unit. Unmapped CAN bus messages show a variation in data when attacks occur. In the future, non-square filters for the CNN process can be used and CAN bus commands could be made efficient by improving its automated learning.

Kravchik et al. [14] studied the 1D convolutions and auto encoders networks and proposed a method to detect any evasion attack. It is mainly focused on the security of industrial control systems and their impacts. Public datasets have been chosen for the experiment namely Secure Water Treatment (SWaT) which contains a record of 36 attacks, BATADAL dataset represents a water
distribution network and WADI dataset (contains 16 attacks) Principle component analysis is used for data pre-processing and feature extraction purposes. Anomaly Detection and Scoring Method is used to reach the threshold detection point. The results show that the performance is better achieved than previous works. Further studies can be conducted on the proposed method by using the adversarial poisoning attacks.

Riaz et al. [15] stated a survey about the authentication and access control models for cloud/edge enabled end devices with the problems. The attacks could be on users (DOS, Access control Issues, account hijacking, advanced persistent threats), cloud or fog environment (malicious Insider, Insecure APIs, Shared Technology Issue, system and application vulnerabilities), database (data loss, data breaches). A detailed analysis of performance analysis of existing techniques of various proposed methodologies is compared based on some criteria to see if it is meeting the requirements or not. A few of the challenges are to identify a compromised node, privacy violation, resource restriction, network availability, decision latency, etc...

III. CYBERSECURITY CHALLENGES

Challenges in cybersecurity are toughest as the trends are in demand and also the new attacks are exploiting the vulnerabilities easily. Trends like web servers, cloud computing, fog computing, encryption, Mobile Networks, advanced persistent threats, etc... have a huge impact on security measures like Malware scanners, password authentication, access controls, anti-virus software tools, etc... [16]. It has become a major concern over the past years as the threats are getting more complex and launched by highly skilled hackers so many patches and solutions are already prepared before for such acts because every time a new attack is ready to be launched and as per risk management if it fails to defend the platform then a huge loss is going to happen. Therefore, all the known attacks studied and the pattern of occurring is followed to prepare for the next issues and also the types of attacks shows further different types of attack that can take place in the future.

Figure 2: Iots and smart cities

3.1 IOTs (Internet of Things)

IoT enabled devices are more likely to be vulnerable as each layer of IoT can be compromised by various means of attacks. The cyber-physical systems are at much risk. The challenges in IoT devices could be in supply chains, big data, industry control systems for which the solutions like a cybersecurity architecture, data mining methods, security analytics could be considered [17]. As the security needs can be different for every device the solutions can be put as per the defined requirements and states. A flow-control loop process is introduced using STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege) method to build a threat model under various classifications with countermeasures that specify different threats and be helpful to deduce cybersecurity requirements [18].

I. SMART CITIES

The smart city is a huge interconnected network comprised of different sectors like the government sector, critical infrastructure sectors, health sectors, transport sectors, smart building sectors with benefits like smart building services, efficient urban services and cyberspace services [10]. Cybersecurity challenges like vulnerabilities of radiofrequency identification (RFID) tags and smartphones, data sharing and communications, data management and policy compliance, data breaches, authentication, mobile networks, Supervisory Control and Data Acquisition (SCADA) networks, virtualization, management strategy, configuration errors, patch updates, etc... are very common as itself the proper security measures are lacking in systems [19]. The privacy has to be secure in each node of the network.
IV. CONCLUSION
Cyber threats already consist of huge risks for every organization. The risk is evaluated based on the recent weightage of attacks launched using different paths. The countermeasures are depended upon the updated programs and plans by the security analysts to defend any type of attack before any compromise of data and privacy. The focus is to improve the efficiency and detection ability of the systems to ensure safety. In recent years, hybrid approaches like cloud computing, artificial intelligence, data mining, Big data, etc. are being followed to defend such threats. As many methods are already developed for security but could be enhanced by experimenting with real-world datasets within the cyberspace domains to enhance the countermeasures of an organization.

REFERENCES