iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57396

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

Cyber Security Challanges for Online Trading

Mr. Himanshu Tiwari[1] , Mr. Alok Kumar[2]
[1, 2]*Assistant Professor, Dept. of Computer Science and Engineering, Greater Noida Institute of Technology, Greater Noida.*

Abstract: ***Today Security is a fundamental component in the computing and networking technology. The first and foremost thing of every network designing, planning, building, and operating a network is the importance of a strong security policy. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. Online trading facilitates as a financial platform form for buying and selling shares, bidding, product sale or purchase using computers. The vital online trading between B2B, B2C and C2C transaction data may be under siege due to spywares, malwares, Hijackers and intruders. Often trading secrets and portfolios are in risk with network attackers who tracks unauthorizedly the personalized data of business clients. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.***
Keywords: Cryptography, Encryption, Key, Cookies, Digital Signatures

I. INTRODUCTION

Cyber security is a strategic collection of defensive systems which protects computers, servers, mobile devices, electronic systems, networks and data from malicious attacks [1][2]. The global security attacks over cyber space are enormously increasing at high rate of confidentiality risks [5]. The early detection and recommendation of risk avoidance strategies are keen interest of Cyber Security [3]. The US government introduced Cyber laws to enforce security with a legal framework over cyber space earlier to 2013. The Network Security innovations insisted to discover strong cryptographic environments in securing business data among open networks. Increased data explosion and vulnerabilities caused by advanced hackers placing many challenges daily upon cyber security framework [6]. The process of buying and selling of things over Internet is referred as E-Commerce activity [7]. The trading now is becoming online in almost majority of companies to enhance their business borders and increasing the investors [6].

Network Security management is different for all types of situations and is necessary as the growing use of internet. A home or small office may only require basic security where as large businesses may need high- maintenance and advanced software and hardware to prevent malicious attacks from hacking and other attacks. New Threats Demand New Strategies as the network is the door to your organization for both legitimate users and would-be attackers. For many years, IT professionals have built barriers to stop any unauthorized entry that could compromise the organization's network. And this network security is important for every network designing, planning, building, and operating that consist of strong security policies. The Network Security is constantly evolving, due to traffic growth, usage trends and the ever changing threat landscape.

While considering network security, it must be emphasized mostly that the whole network should be remain secure. Network security does not only mean the security in the computers at each end of the communication chain. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Hence, securing the network is just as important as securing the computers and encrypting the message which we want to be kept private. When developing a secure network, the following need to be considered.

1) Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
2) Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
3) Information security protects the integrity and privacy of data, both in storage and in transit.
4) Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
5) Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data.

Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

Due to deep integration between the world and the internet, the network framework always experiences various kinds of attacks. Identification of these attacks is a technical issue and currently the area of concern these days. Cyber-attacks fall into a broader context than what is traditionally called information operations. Information operations integrated use of the main capabilities of electronic warfare, psychological, computer network, military trickery and security operations in coordination with special support and relevant abilities and to penetration, stop, destroy or hijack human descisions and It is one of the decision-making processes of national institutions.

II. THE SCALE OF CYBER THREAT

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by Risk Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

With the scale of the cyber threat set to continue to rise, global spending on cybersecurity solutions is naturally increasing. Gartner predicts cybersecurity spending will reach $188.3 billion in 2023 and surpass $260 billion globally by 2026. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

III. TYPES OF ATTACK

Networks are subject to attacks from different malicious sources. And with the advancement and increasing use of internet attach is most commonly growing on increasing. The main categories of Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation. A system must be able to limit damage and recover rapidly when attacks occur. There are some other types of attack that are also necessary to be considered:

1) A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose of a passive attack is to gain information about the system being targeted; it does not involve any direct action on the target.
2) Passive attacks include active reconnaissance and passive reconnaissance. The word *reconnaissance* comes from the military term that refers to the act of exploring an enemy territory to gather information. In a computer security context, reconnaissance is the act of exploring a system or network in order to gather information before conducting a full attack.
3) Active Attack In an active attack, the attacker tries to bypass or break into secured systems in the going on communication. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. The unauthorized attacker’s monitors, listens to and modifies the data stream in the communication channel are known as active attack. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.
4) Insider Attack According to a Cyber Security Watch survey insiders were found to be the cause in 23 percent of security breaches, and a further 23 percent may have been due to the actions of insiders. More than half of respondents to another recent survey said it's more difficult today to detect and prevent insider attacks than it was in 2015, and 53 percent were increasing their security budgets in response to insider threats, while a significant number of breaches are caused by malicious employees - or former employees - many are caused by well- meaning employees who are simply trying to do their job.
5) Distributed Attack A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a ―trusted component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.
6) Close-in Attack A close-in attack involves someone trying to get physically close to network components, data, and systems in order to learn more about any network.

These attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. One popular form of close in attack is social engineering. In a social engineering attack, the attacker compromises the network or system through social interaction with a person, through an e-mail, message or phone. Various tricks can be used by the individual to present information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to get unauthorized access to a system or network

7) Phishing Attack In phishing attack the hacker tries to create a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message trying to motivate the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

8) Password Attack An attacker attempts to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords [9]. A brute-force attack is when the attacker tries every possible combination of characters

9) Hijack Attack In a hijack attack, a hacker takes over a session between you and another person and disconnects the other person from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accidently. This may lead to loss of information and creates problem for the user.

10) Exploit Attack In this type of attack, the attacker knows a security problem within an operating system or a part of software and leverages that knowledge by exploiting the vulnerability.

In modern times, social media is a significant cause of cyberbullying, which can affect many teenagers to commit suicide. Adolescent social media users are psychologically abused by anomalous person's messages, emails, tweets, and reactions. Therefore, misbehaving users such as Sybil accounts can be detected by analyzing data related to user's behavior in the social networks and other sites. In order to differentiate between malicious and legitimate actors in the social network, many researchers have adopted the most widely used machine learning classifiers.

IV. CHALLENGES OF CYBER SECURITY

Even though technology is providing tremendous opportunities for the business sector, the challenges accompanying these opportunities cannot be ignored. One of the challenges is in the form of a cyber security threat, the intensity of which is increasing day by day.

There are basically two questions are arising in current scenario:

- What are the real concerns about the cybersecurity threats in e-commerce business?
- How these threats can be addressed and minimized?

This conceptual analysis aims to contribute to understanding cybersecurity in e-commerce. Many of today's researchers focus on technology's support in business and ignore the challenges technology is bringing to the company. This work highlights cybersecurity as one of the most critical issues related to technology used in industry (e-commerce). It is focused on some cybersecurity issues, e.g., social engineering, denial of services, malware, and attacks on personal data and other important data. Although the scope of cybersecurity is huge, we only discuss some most common types of security breaches. We provide base to this analysis on multiple data sources like books, journal articles, magazines articles, newspapers, blogs, etc. to answer the research questions.

1) Cyber-attack theory, the cyber-attack theory (CAT) believes that information is the main part of any cyber-attack and states that the success of cyber-attacks depends on the information owned by the attackers at the time of the attack and the information modification or gained during the attack. Each system has configuration information that plays a important role in a cyber-attack. It is necessary for a cyber-attacker to have this information. This information includes the information about the system, i.e., configuration information, the system data, etc. It describes any system or device to be targeted by the set of informative parameters, which the attackers want to get or modify. Apart from that, the attackers have also information about similar systems, technical skills, etc. which is helpful in conducting such attacks.

2) Information security theory, the information security theory (IST) states that "Information security is a conscious or subconscious process in which people and organizations tries to create sustainably viable resources, from information".

According to the objectives of information, individuals and organizations secures information from risks and threats by applying suitable control measures. Trying to keep the information protected according to the need of organization and individual make the information sustainable resources. To be more specific, it focuses on the protection of information, suitable for the type and sensitivity of the information and its strategic use for the organization and other entity.

3) System theory the system-theoretic process analysis is an approach that takes the interaction of each and every component of a system into account to make a system safer and more secure (Thomas, 2016). It is developed by Leveson to find out hazardous states and unsafe control actions which cause accidents or system losses. In addition, it also generates comprehensive safety requirements to stop the happening of known hazardous scenarios (Leveson, 2004). It integrates factors like software, hardware, human, organizational and safety, etc. for the identification of potential threats and risks.

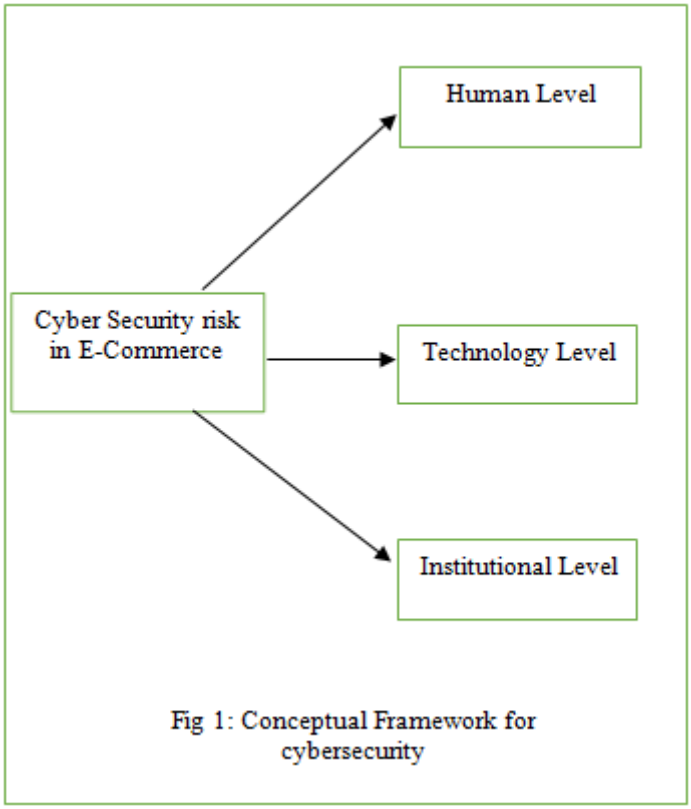


Fig 1: Conceptual Framework for cybersecurity

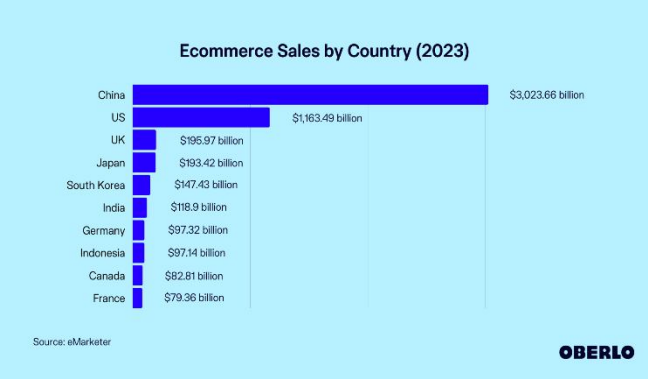
We divide the cyber security concerns in e-commerce at three different levels and proposed the following framework as shown in Figure 1.

a) *Human Level:* Cyber security issues occur due to humans (employees, attackers, and consumers) either lacking the proper knowledge and skills to use the e-commerce technology or not following the protocols related to Cyber security. And if they are attackers, then they know more about the technology, organization, and the users of the technology, i.e., they possess more information. Employees and customers, who are using a particular e-commerce technology must have sufficient knowledge, skills, and information to use the technology properly and to complete a business transaction successfully.

b) *Organization Level:* At the organizational level, security concerns occur due to inadequate rules, regulations, and policies to implement the security protocols and use the systems according to the law. If cybersecurity is not the theme of an e-commerce organization's strategy, it is impossible to address it. Organizations need to invest in training, enhancing security controls and measures, and must continuously be searched for the vulnerabilities and their possible solution at the management level. If it ignores the need for something that should be done to address cybersecurity threats, they may become a cause of potential damage in the future. Organizations should adopt new procedures and policies to overcome the cybersecurity threats as per market demand, organizational need, and attackers' skills and knowledge.

c) *Technology:* E-commerce organization often does not invest much to implement a suitable and safe technology, due to which cybersecurity risks increase. It is necessary for e-commerce organizations to invest significantly in hiring new and more secured technology. Maybe it is expensive but more beneficial in the longer term.

d) *E-commerce:* E-commerce is an enormously growing field that came into being due to the advancement and convergence of technology and the internet, where people do many activities related to commerce. In other words, e-commerce refers to the selling and buying of products online. It involves an online money transfer in exchange for completing the business activity. E-commerce uses digital means to develop and perform different actions and transactions among organizations or groups or between a firm and a customer. According to a study, there are more than 21 million – 489 million e-commerce websites across the globe. Figure 2 shows the country-wise e-commerce sale in 2023.



Fugure 2: E-Commerce sales by country

The world is shifting from in-store to online shopping, and big companies like Alibaba, Amazon, etc., are leading the transition. Due to this shift, technological advancements are being made to further online business processes. E-commerce provides an ease for customers to buy something and has also proved itself one of the powerful agents for business transformation.

V. TECHNOLOGIES FOR PROVIDING SECURITY TO THE NETWORK

Internet threats will continue to be a problematic issue in the global world as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with attacks mentioned earlier. Some of these mechanisms along with advance concepts are mention in this section.

Cryptographic Systems: Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

Firewall: The firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front-line defense mechanism against intruders to enter in the system. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. The most widely sold solution to the problems of Internet security is the firewall. This is a machine that stands between a local network and the Internet, and filters out traffic that might be harmful. The idea of a ―solution in a box has great appeal to many organizations, and is now so widely accepted that it's seen as an essential part of corporate due diligence. Firewalls come in basically three flavors, depending on whether they filter at the IP packet level, at the TCP session level, or at the application level.

Driving Security to the Hardware Level To further optimize performance and increase security, Intel develops platforms also include several complementary security technologies built into multiple platform components, including the processor, chipset, and network interface controllers (NICs). These technologies provide low-level building blocks upon which a secure and high performing network infrastructure can be sustained. These technologies include Virtualization Technology, Trusted Execution Technology and Quick Assist Technology.

Secure Socket Layer (SSL) The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.

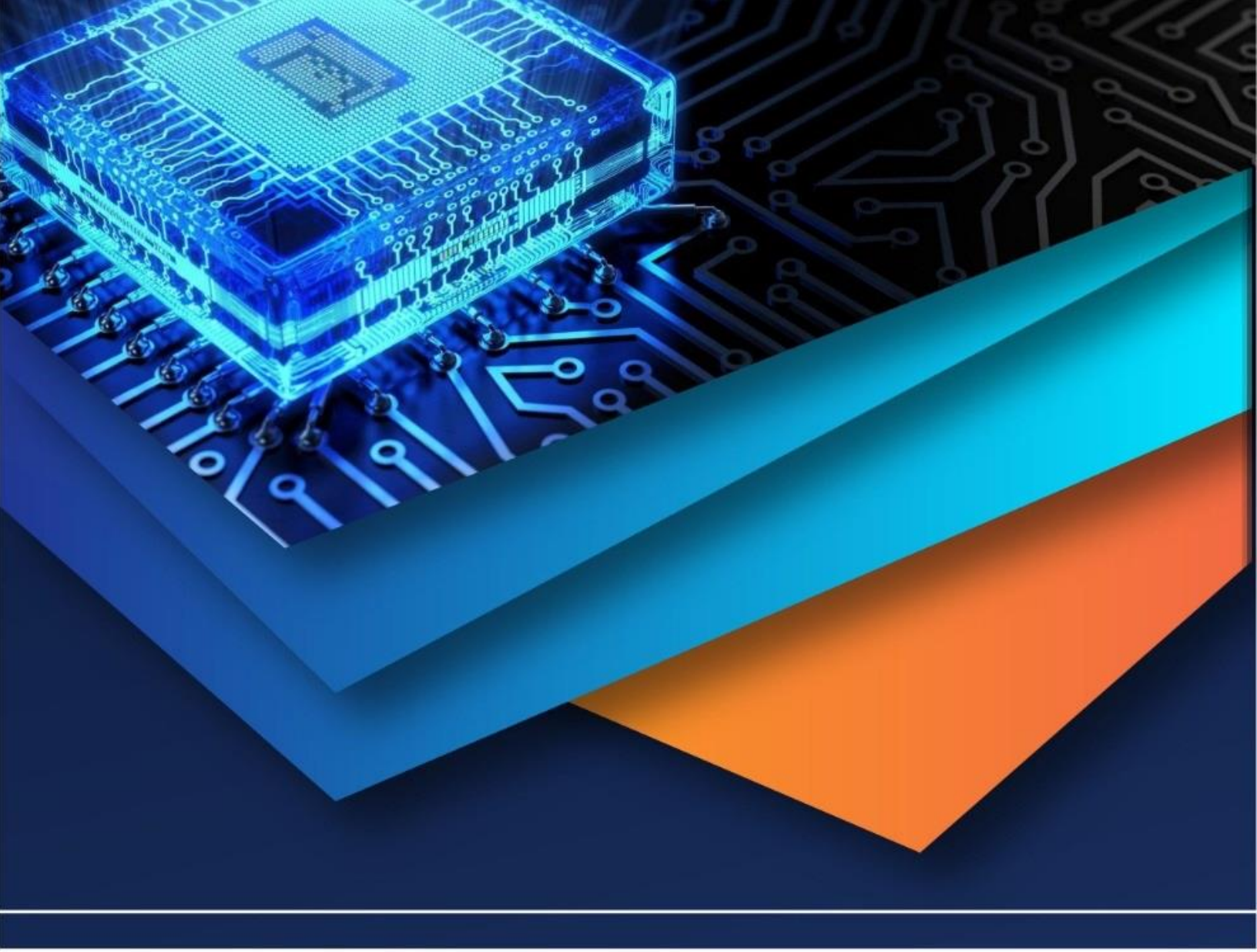
Dynamic Endpoint Modelling Observable's Security Solution, represents a profoundly new way to look at IT security. It models each device on your network, so you can understand normal behavior and quickly take action when a device starts acting abnormally. There's no need to install agents on the devices, or attempt to use deep packet inspection, giving you a powerful solution to overcome these new security challenges.

VI. CONCLUSION

Security is a very difficult and vital important topic. Everyone has a different idea regarding security' policies, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. The name of e-commerce is attractive and the need of the modern-day business market, but it is facing the challenge of cyber security threats. Although firms continuously invest a lot to address the issue, it is not easy. Personal and organizational data are often the target of cyber-attacks. Without a doubt, technology offers new ways of doing business and provides many additional benefits, but cyber security concerns will always be there. Investing and enhancing the security of e-commerce is substantially essential for getting a competitive advantage and for the success of e-commerce business.

REFERENCES

[1] Rammanohardas, "Artificial Intelligence in Cyber Security", Journal of Physics, Conference on Artificial Intelligence and modern applications, 240-ECS Meeting, 2021..
[2] Md. Shafiur Rahman, Sajal Halder, U. Kumar Acharjee, "An Efficient Hybrid System for Anomaly Detection in Social Networks", Springer, Article.No:10,Vol.4, DOI: https://doi.org/10.1186/s42400-021-00074-w, 2021.
[3] M. Humayun and M.Niazi, " Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study", Arabian Journal of Science & Engineering, DOI: 10.1007/s13369-019-04319-2, PP: 1245-1250, 2020.
[4] Alex Mathew, "Machine Learning in Cyber-Security Threats", International Conference on IoT Based Control Networks & Intelligent Systems, DPI:10.2139/ssrn.3769194, 2020.
[5] Anand Shinde, "Introduction to Cyber Security: Guide to the World of Cyber Security", ISBN: 978-1-63781-642-4, Notion-Press, 2020.
[6] I Agrafiotis, Jason R C Nurse, "A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-Attacks and understanding how they Propagate", Journal of Cyber Security, DOI:doi.org/10.1093/cybsec/tyy006, Vol.4, Issue-1, 2018.
[7] Muhammad Kashif, Sheraz Arshad Malik, "A Systematic Review of Cyber Security and Classification of Attacks in Networks", IJACSA, Vol.9, No.6, PP:201-207,2018.
[8] Ahmad, S. F., Alam, M. M., Rahmat, M. K., Mubarik, M. S., and Hyder, S. I. (2022). Academic and administrative role of artificial intelligence in education. Sustainability 14:1101. doi: 10.3390/su14031101.
[9] Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., and Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network 2, 123–138. doi: 10.3390/network2010009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY