iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.48433

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 10 Issue XII Dec 2022- Available at www.ijraset.com

An Outlook on the Status of Security Performance in The Light of Intelligence

Monisha Gottam

Abstract: ***An outlook on the status of security performance in light of intelligence focuses on the business aspects and needs of organizations. The security plan needs to be integrated with the business and should be developed in collaboration with different groups within an organization. Organizations need to have a culture that embraces security and intelligence. Security performance is one of the top concerns of modern businesses. Companies must look at the underlying causes of their problems in order to fix them. A good cybersecurity posture is often measured by a lack of data breaches. Lack of specific metrics, however, may be an indication that a company does not have a strategic mindset. Attacks and malfunctions are extremely costly. Detection involves identifying suspicious behaviors and alerting the appropriate personnel. An important challenge in detecting suspicious activity is finding the right balance between false alarms and coverage. An effective security program must be able to mitigate attacks while reducing false alarms. The growing reliance on artificial intelligence (AI) is creating a new kind of cyber-vulnerability. Developers often overlook AI security, leaving it open to attack by adversaries. Attacks can take the form of basic manipulations and probes or adversarial AI. As the number of computer systems increases, so do the risks they pose to the security of data and systems. This article examines the importance of security performance, the role of the cloud, machine learning-based security models, and incident response. We also look at the importance of a security model that incorporates intelligence. Finally, this report also identifies five critical areas in which Intelligence attacks pose a high risk to organizations.***
Keywords: Security Performance, AI, Cybersecurity, SME, Ransom-ware, Wi-Fi network, SME, CARG

I. INTRODUCTION

An outlook on the security performance of companies has shown that cyber-security is still not at par with business objectives. Although most respondents feel that their current cybersecurity efforts are adequate, only a minority feel that their companies have made significant progress. In addition, the vast majority feels that there is still room for improvement. However, while net satisfaction levels rose over the past year, the percentage of respondents who are completely satisfied with their current security posture dropped. As a result, the demand for cybersecurity solutions has increased exponentially (Liu, *et al.*, 2020). According to Bhargava & Agrawal, (2021) many major companies have jumped into the market and are focusing on new products and solutions to protect their organizations. For example, IBM has launched the Security X-Force, a threat intelligence task force focused on detecting cyber-attacks. The cybersecurity market is split into two major segments: large enterprises and small and medium enterprises. The SME segment is projected to grow at the highest CAGR, while the large enterprises segment is expected to grow at the lowest CAGR. The growth of the small and medium enterprises segment can be attributed to the growing demand for digital privacy and end-point security solutions. Another growing segment is the healthcare segment, where Internet security solutions are helping healthcare organizations protect their customer health records. Increasing sophistication of cyber-attacks has made it necessary for organizations to upgrade their cyber- security platforms. As a result, many vendors are implementing artificial intelligence and machine-learning capabilities in their security solutions. To implement such solutions, organizations must deploy high-end IT infrastructure (Khan, *et al.*, 2022).

II. LITERATURE REVIEW

To effectively protect an organization, it is essential to understand all aspects of its business. This includes the people and assets it protects. In order to develop a security plan, different groups within the organization should be involved in its development. Then, the team can make appropriate notations prior to making a change to the security system. This will ensure that security personnel are informed of the change. The rise of Intelligence has brought new challenges to Cyber Security. AI-powered attacks and information warfare are turning data into a vulnerability. As a result, organizations are having to rethink their Cyber Security strategy. In literature review, we will look at patterns of attack, detection, and the ease of detecting attacks. To ensure security performance in a business environment, it is essential that security teams are well- informed and have a comprehensive understanding of the business. Consequently, they must be engaged in the creation of a security plan, involving all parts of the organization (Liu, *et al.*, 2020).

A. Analysis of Recent Trends

New security technologies are being introduced quickly. Among the most common security tools are Identity and Access Management and Data Loss Prevention. About half of companies have adopted these technologies. Another popular security technology is Security Information and Event Management, which is used by 49% of organizations. Many companies are now incorporating these tools to ensure the protection of sensitive information (Bhargava & Agrawal, 2021).

B. Sources of Intelligence

While collecting intelligence is a complex process, it can be made simpler with the help of tools. The OSINT Framework, developed by security researchers, is one such tool. It contains a large collection of links to a large number of intelligence resources (Khan, *et al.*, 2022).

C. Challenges for Security Teams

As security teams face increasingly complex threats, they must be able to respond quickly and proactively to protect their organization. Unfortunately, many organizations don't have the necessary cybersecurity skills to meet this challenge. Many companies struggle to find qualified security professionals, which leads to turnover and burnout. AI can help address this problem by allowing security teams to respond automatically to threats (Dilek, Cakır & Aydın, 2015).

D. Attacks on AI systems

Attacks on AI systems can occur in many different ways. One common way is to manipulate input. This could be anything from tampering with stop signs to changing small details in a digital photograph. These attacks can be extremely harmful because they can cause the AI system to produce incorrect results. Another common attack is to disrupt an automatic security system by misclassifying regular events as threats. This could result in the system being taken offline. AI systems are particularly vulnerable to these types of attacks. Even small manipulations can give an adversary access to the system, allowing them to make changes and even poison it. However, some traditional cybersecurity policies may be able to mitigate the impact of AI attacks. For example, if an attacker supplies an image to the AI system, the AI would generate a version of the image that would fool a content filter. It would look similar to the original, but not exactly the same. Attacks on AI systems can also be carried out by exploiting a system's open APIs. This can allow attackers to craft malicious code using an AI system's model, datasets, and other assets. As a result, it can replace many of the traditional methods of stealing data, stealing models, and probing behavior (Baechler & Margot, 2016).

E. Patterns of Attack

Attack patterns are a way of categorizing the types of attacks and defining mitigations. They describe a minimum set of nodes from the root node to the leaf node that can be exploited to achieve a goal. These attack paths may be part of a larger tree or a sub-tree. One of the most common types of cyber-attacks is point-of-sale intrusions (Allen & Chan, 2017). These attacks target the architecture of a computer system and can be caused by various vulnerabilities in the protocols and authentication strategies. In addition to this, these attacks can be disruptive and can result in the loss of intellectual property. In addition, attackers use different types of attack techniques to achieve their objective. For example, they may attempt to make a target system unreachable to legitimate traffic, cause financial harm, or steal critical data. These attacks can be automated, or manual (Li, 2018).

F. Detection

The threat landscape for cyber systems is constantly evolving, increasing in complexity, scale, and speed. Cybercriminals are increasingly employing new techniques to access confidential data and disrupt critical infrastructure. Microsoft 365 Defender, which utilizes AI techniques, is designed to protect against these attacks. According to Microsoft, its software will prevent 9.6 billion malware threats by 2021. In addition, it will stop 35.7 billion malicious emails and 25.6 billion attempts to hijack customer accounts. Detection in cyber security performance in light of intelligence refers to how a person notices a certain action, event, or activity. A perceivable attack is not necessarily ostentatious; it can be as subtle as a piece of tape placed on a stop sign. Humans are conditioned to ignore small changes in their environment, and this is why perceivable attacks may go undetected. They may also be designed to avoid detection and be undetectable. Detection involves analyzing the security ecosystem, identifying malicious activities, and putting mitigation measures in place to counter them. This is an ongoing process, and smart people and technologies will be able to work together to ensure security (Hameed & Alomary, 2019).

G. Ease of Attack

Digital malicious attacks are increasing in frequency and complexity. Every day, new computer viruses, codes, and applications are released into the world. These attacks are typically multi-vectored, utilizing polymorphic code to attack an organization. However, there are ways to protect against them. Cyber-attacks target vulnerable resources, such as computers or industrial and mechanical controls. The resulting damage can be extensive. The attacker may gain access to an organization's Wi-Fi network, its social media accounts, its operating system, or even its confidential data. Some cyber-attacks can even affect a person's transportation schedule. Active cyber-attacks range from attacks that aim to gain access to and use information on a target system to ransom-ware attacks. Other types of attacks include brute-force attacks that attempt to guess a user's passwords, or cross-site scripting, which allows an attacker to insert client- side scripts into a web page and bypass access control (Liu, *et al.*, 2020).

III. RESEARCH METHODOLOGY

The current state of intelligence is not without its challenges. While no single agency has advocated for the elimination of a dedicated Intelligence (IC) unit, there are those that continue to push for compartmentalization. The primary mission of the intelligence community is to reduce uncertainty and provide warning of potential threats (Bhargava & Agrawal, 2021). Decision makers, ranging from the White House to local jurisdictions, rely on the insights of intelligence community analysts. As a result, the list of individual customers and agency customers is long and diverse. A SIEM is a key element of the intelligence lifecycle, but not every organization has one in place. For this reason, the security team will need to create a way to correlate information. Object-oriented databases are one way to accomplish this task, but they require a lot of time and effort to set up and maintain. In addition, the volume of security data can overwhelm the system. Adapting behavioral, social science and digital principles to national security contexts is a key element in improving intelligence analysis (Khan, *et al.*, 2022).

1) *Internet of Things (IOT):* As AI replaces human labor in everyday tasks, it is increasingly important for companies and governments to adopt proactive measures to protect themselves from cyber-attacks. By taking proactive measures, organizations can utilize AI to their advantage while minimizing the associated attack threat (Dilek, Cakır & Aydın, 2015). For example, a hacker could use AI algorithms to infiltrate the nation's borders, disrupting security or safety-critical infrastructure. A market analysis of cybersecurity solutions in the US and Europe finds that large enterprises account for a large share. They have increased their investment in technology infrastructure and have a high volume of data. In addition, they are also investing in AI-based security solutions. They typically use multiple networks, servers, storage equipment, and endpoint devices. However, large enterprises are particularly vulnerable to cyber-attacks and face a number of challenges (Baechler & Margot, 2016).
2) *Cloud security:* Organizations are grappling with the challenges of handling massive streams of data. While some use cases have clear requirements such as storing historical data, others require real-time or time- series data. Depending on the use case, organizations must decide which data to store in its original granularity, and which to aggregate or pre-analyze. As storage capacity continues to grow, the need for agility and scalability becomes apparent. Although cloud computing offers many advantages, it also poses some security challenges. The most common barriers are cost and security concerns. In fact, 15 percent of organizations report experiencing at least one cloud security incident. While these incidents are rare, they should not be underestimated. Organizations that adopt cloud services should address the challenges associated with them in order to maintain a safe cloud computing environment (Allen & Chan, 2017).
3) *Machine learning-based Security Model:* The use of a machine-learning-based security model in cyber security is an effective way to counter malicious threats. The technology is capable of identifying malicious threats and reducing alert fatigue. Cybersecurity practitioners must be cautious when using this technology, as the results may not be what they are looking for. While machine learning is a powerful tool, it is not a panacea. Cybercriminals will continue to develop their skills to exploit security flaws. It is therefore critical for companies to combine the latest technology with the expertise of the industry. Machine learning can help cybersecurity teams prevent future attacks by identifying the patterns that occur in a given data set. However, to be effective, data needs to be structured for decision-making. Additionally, data must be collected from various sources to ensure that it has a complete context. This will help cybersecurity teams be proactive in their response to potential attacks and minimize time spent on routine tasks. There are several techniques that can help a cybersecurity team develop an effective machine learning-based security models (Li, 2018).

a) One such technique is reinforcement learning. This method is based on the principle that a system should learn from previous experiences in order to avoid repeating mistakes. The model also uses a combination of unsupervised and supervised learning techniques.

b) Another type of machine learning technology is deep neural networks. These artificial intelligence algorithms are designed to be able to identify new malware based on their historical data and make predictions. As such, machine learning is an essential part of cyber security solutions. In fact, Trend Micro has been integrating this technology into its security solutions since 2005.

c) The quality and quantity of input data are critical for machine learning-based security models. If the data being fed to the algorithms is too small, the model cannot make sense of it. In addition, the data must be in the same "language" that the algorithms use. The data used to train machine learning algorithms can be freely obtained from the public. The use of a machine-learning-based security model is an effective approach for detecting malicious cyber activities. This method uses neural networks and reinforcement learning techniques to identify botnet traffic and other malicious cyber activity. These techniques can also be used for detection of intrusions.

4) *Incident Response:* To keep the United States safe, our intelligence agencies gather information both within and outside of our country. Such information provides us with insights that we cannot otherwise obtain. These insights can guide policy decisions and warn us of potential threats. For example, intelligence can help us make better decisions when we are abroad and identify foreign leaders who might pose a threat to the U.S (Hameed & Alomary, 2019).

IV. RESULTS AND DISCUSSIONS

The security performance of organizations is a crucial factor in securing their information systems. Yet, most organizations don't have the ability to monitor their entire network. To prevent attacks and maintain the integrity of their intelligence systems, companies must first prioritize their assets and risks according to their criticality (Liu, *et al.*, 2020).

1) *Prioritize assets and risks by criticality*: The first step in creating a cybersecurity plan is to prioritize your assets and risks by criticality. The next step is to link each critical asset to its associated risk. You can do this by having the initial stakeholder team review your critical asset matrix and verify the critical function of each item. As the process progresses, include other stakeholders to refine the articulation of your business risks and priorities. Next, you should create a network inventory and baseline. This inventory should contain information about the type of assets and the operating system that they are running on. Once you have a baseline, you can identify which assets are most vulnerable to attack. You should also develop a cyber-security policy for the network, including how to detect suspicious activity. Developing a cyber-security plan is not an easy task, but it is crucial to protect your enterprise and its assets. The task is time-consuming and requires specialized knowledge. Security specialists must assess thousands of risks and controlsto decide which ones to prioritize. Without prioritization, organizations are left scrambling to allocate resources across the enterprise. In addition, their budgets are competing with other investments, such as new technologies (Bhargava & Agrawal, 2021).

2) *Implement capabilities-based security at the language level:* Language-based security is a computer-security technique that makes use of the properties of programming languages to prevent vulnerabilities. Specifically, it enforces application-level security by evaluating the behavior of software applications in terms of the programming language used to specify the application. Unlike ACL-based security, which can only protect against physical threats, language-based security can protect against virtual threats. The key to this system is the ability to encrypt data. A key, also known as a capability, is a non-forgeable token of authority. This capability should be unique and unreproducible. For example, if a program wants to encrypt a document, it must include a capability identifier. This way, a computer will be unable to copy or decode a file containing sensitive data. This capability-based solution can address many of the memory vulnerabilities that plague modern computing systems. Because of its lightweight implementation, it can be implemented with little to no disruption to the existing software. The CompartOS architecture extends this capability concept to the hardware memory and programming-language pointers and provides secure memory access to all components of the system (Khan, *et al.*, 2022).

3) *Create benchmarks for cybersecurity initiatives:* It is imperative that cybersecurity efforts are aligned with intelligence and national security objectives. The Department of Defense has a critical role to play in defending the country from cyber-attacks. Moreover, it must invest in effective detection methods and multifactor authentication. Additionally, it must bolster its cybersecurity teams and perform regular testing of patches, backups, incident response plans, and incident response tools. Finally, it must develop cybersecurity-specific benchmarks (Li, 2018). To achieve these goals, the federal government must modernize its cybersecurity approach and enhance its visibility of cyber-threats. To do so, the government must improve its use of cloud-based secure services and accelerate the adoption of integrated cyber-security tools. In addition, the Federal government needs to invest in technology and personnel to combat cyber-attacks (Liu, *et al.*, 2020). In addition, it needs to

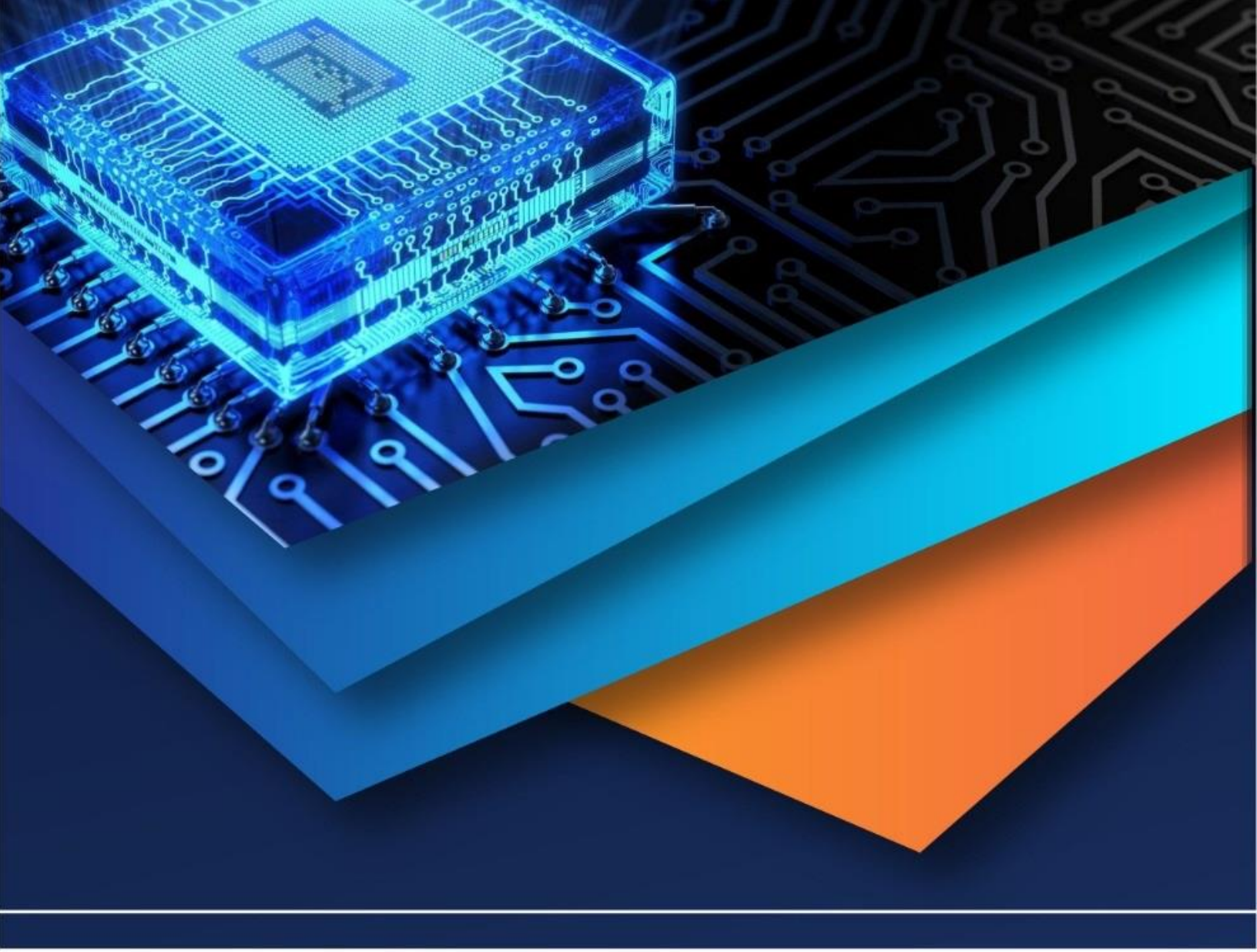
communicate cybersecurity metrics to non-technical stakeholders in ways that are easily understood. Incorporating benchmarks and industry comparisons can make these metrics more understandable. One of the most important metrics to be considered is cost. It is important to demonstrate how cybersecurity is saving the organization money or creating revenue (Bhargava & Agrawal, 2021; Khan, *et al.,* 2022).

V. CONCLUSION

Despite the increased sophistication of computer systems, Organizations are still vulnerable to attacks. The consequences of malfunctioning and misclassification can be severe in high-stakes domains. Fortunately, there are a number of techniques that can help organizations minimize their risks. Security practices must continually adapt to changing threats. New technologies and uses of existing technology create new attack avenues. Organizations must keep up-to-date on the latest practices in cyber security to protect themselves from new threats and vulnerabilities. However, this can be difficult for organizations with limited in-house resources or staff. Commercial organizations should adopt the principles of military cyber security in order to protect their data and systems. The SOC at Greenback Financial is responsible for detecting, diagnosing, and managing cyber incidents. However, it did not use its expertise to identify future threats. Cyber-attacks often use eavesdropping to intercept communication and steal sensitive data while in transit. This method is often difficult to detect, and it relies on unsecured network communications. In some cases, hackers install bugs in telephones to listen to conversations and review network activity. This new approach is transforming the way commercial organizations approach cyber-defense. The approach is aimed at shifting the behavior of organizations from reactive to proactive. The new approach builds on research expertise and practitioner-researcher collaboration to transform cybersecurity practice. The authors of this study are both researchers and practitioners.

REFERENCES

[1] Allen, G., & Chan, T. (2017). Artificial intelligence and national security. Cambridge, MA: Belfer Center for Science and International Affairs.
[2] Baechler, S., & Margot, P. (2016). Understanding crime and fostering security using forensic science: The example of turning false identity documents into forensic intelligence. Security Journal, 29(4), 618-639.
[3] Bhargava, N., Bhargava, R., Rathore, P. S., & Agrawal, R. (Eds.). (2021). Artificial Intelligence and Data Mining Approaches in Security Frameworks. John Wiley & Sons.
[4] Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552.
[5] Gui, G., Liu, M., Tang, F., Kato, N., & Adachi, F. (2020). 6G: Opening new horizons for integration of comfort, security, and intelligence. IEEE Wireless Communications, 27(5), 126-132.
[6] Hameed, A., & Alomary, A. (2019, September). Security issues in IoT: a survey. In 2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT) (pp. 1-5). IEEE.
[7] Khan, S. U., Eusufzai, F., Azharuddin Redwan, M., Ahmed, M., & Sabuj, S. R. (2022). Artificial Intelligence for Cyber Security: Performance Analysis of Network Intrusion Detection. In Explainable Artificial Intelligence for Cyber Security (pp. 113-139). Springer, Cham.
[8] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY