iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49894

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 III Mar 2023- Available at www.ijraset.com

Self-Defending Networks

Pramod K[1], Aswathy Venu[2]
[1]*Assistant Professor, Nehru College Of Engineering and Research Centre*
[2]*Department Of MCA, Nehru College Of Engineering and Research Center*

Abstract: ***As the nature of the threat in networks evolves daily, it is vitally important that defense techniques evolve as well. Earlier threats from both internal and external sources were gradual and can be easily tracked and destroyed. But now Internet worms are spread all over the world, so it is essential for protection systems and the network itself to respond immediately to threats. The basis of community self-defense is the importance of countering threats in the community. Every device found in a community plays a vital role in keeping the community safe. This guarantees the security of statistics and protects the community from internal and external threats. It identifies and responds to threats, isolates infected servers and structures, and then reconfigures the network in response to the attack. Self-Defending Networks are proactive and automated computer networks that are designed to detect, prevent, and respond to security threats. They use advanced technologies like machine learning, artificial intelligence, and behavioral analysis to monitor network traffic, identify potential security breaches, and take action to prevent them. By deploying SDNs, organizations can achieve a higher level of security for their networks and protect their assets from a wide range of cyber threats.***
Keywords: Self Defending Network (SDN), End-Point Protection, Network Security, Incidence Response.

I. INTRODUCTION

With the number of computer networks growing day by day, it is also important to make them more secure and reliable. Security concerns increase as more and more data traverses networks, requiring more complex and reliable protection for networks. Therefore, it is very important to ensure the security of both software and hardware components in the network. For a more secure network, a proper analysis of all types of threats that may occur in the network must be performed, followed by proper network design. This white paper discusses the need for artificial intelligence in network security to make networks intelligent. This white paper also introduces the next-generation smart network, a Self-Defending Network (SDN), a network that analyzes all known and unknown threats that may come across the network. This self-defense network provides protection against internal as well as external threats. Minimize data threats with the network capable of handling large amounts of data and information very quickly.

II. LITERATURE SURVEY

Anshuman Kumar , Abhilash Kamtam and U C Patkar make a research on “Self Defending Approach Of A Network” and describe that Because the nature of network threats changes every day, it is important that protection methods evolve as well. Previously, threats from both internal and external sources were slow and easy to track and eliminate. But now that Internet worms are spreading globally, it's important that security systems and the networks themselves respond promptly to threats. The foundation of network self-defense is critical to responding to threats on the network. Each device on the network plays an important role in network security.This ensures data security and protects the network from internal and external threats. Detect and respond to threats, isolate infected servers and systems, and reconfigure networks in response to attacks.

Duane De Capite make a research on “Self Defending Networks: The Next Generation Of Network Security” this research provides a overall view on protect your community with self-regulating network protection solutions that combat each internal and external threats. provides an overview of the safety components used to design proactive network security helps community safety professionals recognize what the present day gear and techniques can do and how they interact affords distinct records on how to use integrated control to growth safety consists of a layout guide with step-by using-step implementation instructions Self-defending Networks: the next era of network security enables networking professionals apprehend how to deploy an end-to-end, integrated community security answer. It presents a clear view of the various components that may be used at some stage in the network to now not most effective reveal visitors however to allow the network itself to grow to be more proactive in preventing and mitigating network assaults. This security primer presents particular perception into the whole range of Cisco protection answers, showing what each detail is capable of doing and how all the portions work together to shape an quit-to-quit Self-protecting network. at the same time as other books generally tend to awareness on character safety components, presenting in-intensity configuration hints for

various gadgets and technology, Self-protecting Networks rather offers a high-degree review of the entire range of technologies and techniques that incorporate the latest questioning in proactive community protection defenses.

S. Neelavathy Pari , D.Sridharan conduct a research on "Design Of Cross Layered Security Architecture To Mitigate Misbehaving Nodes In Self Defending Networks " and states that Countermeasures for node misbehavior and selfishness are mandatory necessities in cell advert hoc network (MANET). Selfishness nodes reason missing in transmission which can not be solved with the aid of classical safety mechanisms as this method pay attention handiest in the correctness and integrity of an operation. on this paper, we advise a new routing protocol relied on course Routing Protocol (TPRP) to enforce cooperation a few of the nodes of the MANET and to save you selfish behavior. each mobile node within the network keeps a records structure referred to as trust and reputation table (TRT) to preserve song of other node's conduct. finding out a node to be malicious involves choice making and therefore it's far a problem of uncertainty. The best way to address uncertainty is by using the means of chance. So we make use of Bayesian possibility mathematical version to calculate accept as true with cost that lies between zero and 1. If the agree with price goes underneath the brink believe, then the node is called as malicious and excluded from the community. © EuroJournals Publishing, Inc. 2012.

Brian McKenna conduct a survey on "Network Futures: Dumb And Fast ,Or Smart And Self-Defending?" and describe that the human immune system is being invoked increasingly more as a metaphor for the way ICT networks must work. Cisco CEO John Chambers regaled RSA 2006 delegates ultimate month with a tale of ways his company's self-protecting community idea is inspired through human biology. Others are extra sceptical. Evan Kaplan, CEO of SSL VPN dealer Aventail spoke approximately this development to Brian McKenna, for Infosecurity nowadays, at RSA in San José. © 2006 Elsevier Ltd. All rights reserved.

Nicholas Bambos make a research on "Short Paper: Dynamic Risk Mitigation For 'Self Defending' Network Security" and make a conclusion, they introduce1 a novel probabilistic modeling2 framework, which captures key overall performance tradeoffs bobbing up in records network protection. Given a hard and fast of assets to be had to guard and guard a network, how have to those be dynamically configured to maximize the safety stage? exceptional aid configurations enable numerous community defense modes. except the capital and operational fees of the assets, there are also 'invasiveness' costs associated with stresses that community users experience due to protection measures. How should these charges be balanced and the way ought to the network dynamically configure its safety resources to correctly shield itself? Taking a threat management factor of view, we expand a parsimonious bendy model, taking pictures the above troubles in a unified manner. The model enables the formula of key optimization schemes for dynamically controlling the network protection modes thru 8db290b6e1544acaffefb5f58daa9d83 algorithms. It presents a systematic design framework for 'self-defending' networks that may autonomously maintain their integrity within the presence of changing destructive situations. © 2005 IEEE

III. METHODOLOGY

The methodology used in this study are :

A. End-Point Protection

Protective the quit-point in any network may be very essential.Any non-sanitized quit person linked to a network can come to be harmful hazard to the network. This non-sanitized stop person then turns into the weakest link within the network and can without difficulty by targeted by means of an attacker. For this Cisco has delivered Cisco security Agent software that's taken into consideration as Intrusion prevention tool. operating for the quit-points like quit customers and servers, it is designed to correlate appropriate and suspicious behaviour and save you new attacks, even before a security patch or "signature" can replace the network's antivirus or different safety software. Configuring the running gadget and the network firewall in a new way protects the stop user records and information. the safety agent detects all styles of malware or worms on stop-user structures and protects them with by using supplying safety patches and antivirus updates. the security Agent additionally guarantees relaxed and efficient transmission of information over the network, minimizing threats to cease-consumer systems.

B. Admission Control

Any user whilst first of all joins the network is furnished various safety regulations and degree of get right of entry to is granted to every person in the network. these types of work is executed by way of the network Admission control. network Admission control assists in determining the extent of get entry to that is need to be granted to every user. It also divides the stop user among network administrator and end person hence presenting the get entry to degrees to each user in keeping with its kind and priorities. NAC additionally controls the access by way of interrogating devices when linked to determine whether or not they comply security policies or no longer. NAC makes use of this information to determine appropriate network admission policy enforcement for each

endpoint based on the security country of the OS and associated packages instead of sincerely on who's soliciting for get right of entry to. except detecting, analysing, and performing on community behaviour, Cisco safety Agent can song which programs are established on a unmarried pc or workgroup; which programs use the network; the identity of all remote IP addresses with whom a server or computer pc communicates; and the nation of all applications on far flung systems, which include user-specific installation information and whether or not undesired programs are attempting to run.

C. Infection Containment

It's the potential of SDN to discover unauthorized structures or network attacks as they arise and hence reacting accurately and minimizing the impact of the breech on the network. It particularly follows these 3 steps:

1) *Identify Infected Systems:* Figuring out the inflamed device within the community is the first step inside the containment. due to the fact threats are evolving exponentially it will become very tough to perceive the inflamed device because of the dynamic nature of the chance. Self-protecting network also creates independent systems which speedy responds to the systems on every occasion they get inflamed.
2) *Contains The Outbreak:* whenever any outbreak or infected machine is found within the network it plays following operations to reduce the effect of the outbreak and to comprise the outbreak in the community:

a) Makes use of the automated tool.
b) Disables the connectivity.
c) Disables the services
d) Gets rid of the vulnerability.

3) *Keep Records Of Every Action Taken:* It becomes very critical to maintain file of all of the movements that are taken by means of the community throughout outbreak in order that the network can resume its services from wherein it had left. some containment additionally requires transient amendment or configuration which needs to be eliminated after the incident. For all these it will become very critical to preserve a solid report of each and each moves which are taken.

D. Incident Response

It's the services that the Self-defending network offers on every occasion any incident take area within the community. each time it unearths any incidents inside the network, it speedy responds to it provides the appropriate offerings and takes all of the vital steps that desires to be taken right away. all of the movements are taken through suitable nodes and those moves are taken in real time. all the nodes paintings in integration to provide safety approach to incident and making the network more potent. It takes the expertise of the community infrastructure and offerings, protecting it with emergency plans, and installing equipment and scripts that takes on the spot moves whenever any incident takes location.

IV. LOGO OF SELF-DEFENDING NETWORKS

V. WORKING

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

VI. FEATURES

1.Real-time threat detection and response: Self-defending networks use advanced technologies to detect and respond to threats in real-time. This allows for quick action to be taken to prevent security breaches.

1.Automated incident response and mitigation: In case of a security breach, self-defending networks can automatically trigger incident response procedures to contain the damage and prevent further attacks.

1.Continuous monitoring and analysis of network traffic: Self-defending networks continuously monitor network traffic for any unusual activity or suspicious behavior. This allows for early detection of potential threats.

1.Advanced analytics and machine learning algorithms: Self-defending networks use advanced analytics and machine learning algorithms to identify and prevent potential threats. This allows for proactive measures to be taken to prevent attacks before they happen.

1.Integration with other security solutions: Self-defending networks integrate with other security solutions, such as firewalls, intrusion detection and prevention systems, and anti-virus software, to provide comprehensive protection for the network.

VII. EXAMPLES

Here are a few examples of how Spam Assassin is used in real-world scenarios:

1) *Cisco Self-Defending Network:* This is a network security solution that uses a combination of technologies to automatically detect, prevent and respond to threats. It includes features such as intrusion prevention, firewall protection, and endpoint security.
2) *Darktrace:* Darktrace is an AI-based cyber-defense platform that uses machine learning algorithms to detect and respond to cyber threats in real-time. It uses unsupervised learning to build a baseline of normal network behavior, and then uses this baseline to detect anomalies that may indicate a cyber-attack.
3) *Palo Alto Networks:* Palo Alto Networks is a network security solution that includes a number of features designed to detect and respond to threats in real-time. It uses behavioral analytics and machine learning algorithms to identify threats, and can automatically take action to prevent them from spreading.

VIII. HOW SELF DEFENDIND NETWORKS WORKS?

1) *Threat Intelligence:* Self-defending networks use a combination of internal and external threat intelligence sources to identify known and emerging threats. These sources might include vulnerability databases, threat feeds, and security research reports.
2) *Machine Learning:* Machine learning algorithms are used to analyze network traffic and identify anomalies that may indicate a cyber attack. These algorithms are trained to recognize patterns in network traffic and behavior that are associated with specific types of threats.
3) *Behavioral Analytics:* Behavioral analytics techniques are used to build a baseline of normal network behavior. This baseline is used to detect deviations from normal behavior, which may indicate a cyber attack. Behavioral analytics techniques can also be used to identify insider threats and other malicious activities.

A. *Which Algorithm Used ?*

Self-defending networks use a variety of algorithms to detect and respond to cyber threats. Here are some of the algorithms that are commonly used in self-defending networks:

1) *Machine Learning Algorithms:* Machine learning algorithms are used to analyze network traffic and identify anomalous behavior that may indicate a cyber attack. These algorithms can be trained to recognize patterns in network traffic and behavior that are associated with specific types of threats, and can be used to automatically detect and respond to these threats.
2) *Behavioral Analytics Algorithms:* Behavioral analytics algorithms are used to build a baseline of normal network behavior, and to detect deviations from that baseline that may indicate a cyber attack. These algorithms can be used to identify insider threats and other malicious activities, as well as to detect and respond to external threats.
3) *Signature-based Detection Algorithms:* Signature-based detection algorithms are used to identify known threats based on their unique signatures. These algorithms can be used to detect and respond to malware, viruses, and other types of known threats.

B. *Rules And Algorithms Used*

1) *Anomaly Detection Algorithms:* Anomaly detection algorithms are used to detect patterns in network traffic and behavior that are unusual or unexpected. These algorithms can be used to detect and respond to new and emerging threats that do not have known signatures.
2) *Decision Trees:* Decision trees are used to make automated decisions about how to respond to cyber threats. These trees can be constructed based on predefined rules and policies, and can be used to guide automated responses to threats.
3) *Bayesian Networks:* Bayesian networks are used to model the probability of different events occurring in a network, and to make automated decisions about how to respond to threats. These networks can be used to detect and respond to threats in real-time.

IX. APPLICATIONS

1) *Firewall:* Firewalls are used to monitor and control network traffic, and to prevent unauthorized access to the network. They can be configured to block traffic from known malicious sources, and can be used to detect and prevent the spread of malware and other threats.
2) *Intrusion Prevention Systems (IPS):* IPS systems are used to detect and prevent unauthorized access to the network. They can be configured to block traffic from known malicious sources, and can be used to detect and prevent the spread of malware and other threats.

3) *Endpoint Detection and Response (EDR) Systems:* EDR systems are used to monitor and protect individual endpoints, such as laptops, desktops, and mobile devices. They can be used to detect and prevent malware infections, as well as to respond to other types of cyber threats.

X. ADVANTAGES

Self-defending networks offer several advantages over traditional network security solutions. Here are some of the key advantages of self-defending networks:

1) Real-time Threat Detection and Response: Self-defending networks use advanced artificial intelligence (AI) and machine learning algorithms to detect and respond to security threats in real-time. This allows organizations to quickly and effectively respond to threats as they arise, minimizing the potential damage and reducing the risk of a successful cyber attack.
2) Automation and Efficiency: Self-defending networks automate many of the tasks associated with network security, such as threat detection, analysis, and response. This can significantly reduce the workload on IT teams, enabling them to focus on more strategic and high-value activities.
3) Comprehensive Network Security: Self-defending networks provide comprehensive network security, encompassing multiple layers of protection such as firewalls, intrusion detection and prevention systems (IDPS), and endpoint protection. This can provide organizations with a more holistic approach to network security, reducing the risk of gaps or weaknesses in the network security posture.
4) Scalability: Self-defending networks are designed to be highly scalable, enabling organizations to easily add or remove network resources as needed. This can be especially beneficial for organizations with rapidly changing network environments, such as those that are growing rapidly or undergoing a digital transformation.
5) Reduced Risk and Increased Resilience: Self-defending networks are designed to be highly resilient, with multiple layers of protection and redundancy built in. This can significantly reduce the risk of a successful cyber attack, and help ensure that the network can quickly recover from any security incidents that do occur.

In summary, self-defending networks offer a number of key advantages over traditional network security solutions, including real-time threat detection and response, automation and efficiency, comprehensive network security, scalability, and reduced risk and increased resilience.

XI. DISADVANTAGES

While self-defending networks offer several advantages, they also come with some potential disadvantages that organizations should be aware of before implementing them. Here are some of the disadvantages of self-defending networks:

1) *False Positives and False Negatives:* A self-defending network relies heavily on artificial intelligence and machine learning algorithms to identify and respond to threats. However, these algorithms may sometimes produce false positives or false negatives, leading to either unnecessary alerts or missed threats. This could result in wasted time and resources, or worse, the failure to detect and respond to a serious security threat.
2) *Technical Complexity:* Implementing a self-defending network can be technically complex, and may require specialized knowledge and expertise to configure and maintain. Organizations may need to invest in additional resources and training to effectively implement and manage a self-defending network.
3) *High Cost:* Implementing a self-defending network can be expensive, especially for small and mid-sized businesses. Organizations may need to invest in advanced hardware and software, as well as additional staffing and training to effectively implement and manage a self-defending network
4) *Dependence on Automation:* Self-defending networks rely heavily on automation to detect and respond to threats. While this can be beneficial in terms of speed and efficiency, it also means that organizations may become overly dependent on automation and may not have the necessary human oversight to ensure that the network is functioning effectively
5) *Complexity in Integration:* Integrating a self-defending network with existing security infrastructure can be complex, and may require significant time and effort to ensure that the network is integrated effectively and securely.

In summary, while self-defending networks offer many benefits, organizations should carefully consider the potential disadvantages before implementing them. It is important to ensure that the organization has the necessary technical expertise, resources, and budget to effectively implement and manage a self-defending network. Additionally, organizations should have a plan in place to address potential false positives or false negatives, as well as any technical or operational issues that may arise.

XII. SCOPE OF FUTURE RESEARCH

The future scope of self-defending networks is promising, as advancements in technology and increased adoption of automation and AI are driving the development of more sophisticated and effective self-defending networks.

One potential area of future development for self-defending networks is the use of advanced machine learning algorithms to improve threat detection and response. This could include the use of deep learning models to analyze network traffic and behavior, as well as the integration of natural language processing (NLP) to help identify and respond to threats in real-time.

Another potential area of development is the integration of self-defending networks with other emerging technologies such as blockchain and the Internet of Things (IoT). By leveraging the decentralized and distributed nature of blockchain, self-defending networks could potentially provide more secure and reliable protection against cyber threats. Similarly, by integrating with IoT devices and sensors, self-defending networks could provide more granular visibility into network activity, enabling more effective threat detection and response.

As more organizations adopt cloud-based infrastructure and services, the future of self-defending networks may also involve the development of cloud-native security solutions. This could include the use of cloud-based machine learning algorithms to analyze network traffic and behavior, as well as the integration of security tools directly into cloud platforms to provide a more seamless and integrated security experience.

Overall, the future of self-defending networks is likely to be characterized by continued advancements in automation and AI, as well as increased integration with other emerging technologies. As cyber threats continue to evolve and become more sophisticated, self-defending networks will play an increasingly important role in protecting organizations against these threats.

XIII. CONCLUSION

Self-defending networks is a critical component of a robust cybersecurity strategy. By automating the detection and response to security threats, a self-defending network can significantly reduce the time it takes to mitigate an attack, thereby reducing the risk of data breaches and other security incidents.

One of the key advantages of a self-defending network is its ability to identify and respond to both known and unknown threats. Traditional security technologies such as firewalls and IDPS are typically only effective against known threats, but a self-defending network uses AI and machine learning algorithms to identify patterns and anomalies that may indicate a new or unknown threat. This allows the network to quickly adapt to new threats and respond accordingly, reducing the risk of a successful attack.

Another advantage of a self-defending network is its ability to automate security processes. Automation allows the network to operate at a much faster pace than would be possible with human intervention, enabling it to detect and respond to threats in real-time. This can significantly reduce the time it takes to detect and respond to a security incident, minimizing the potential impact on the organization.

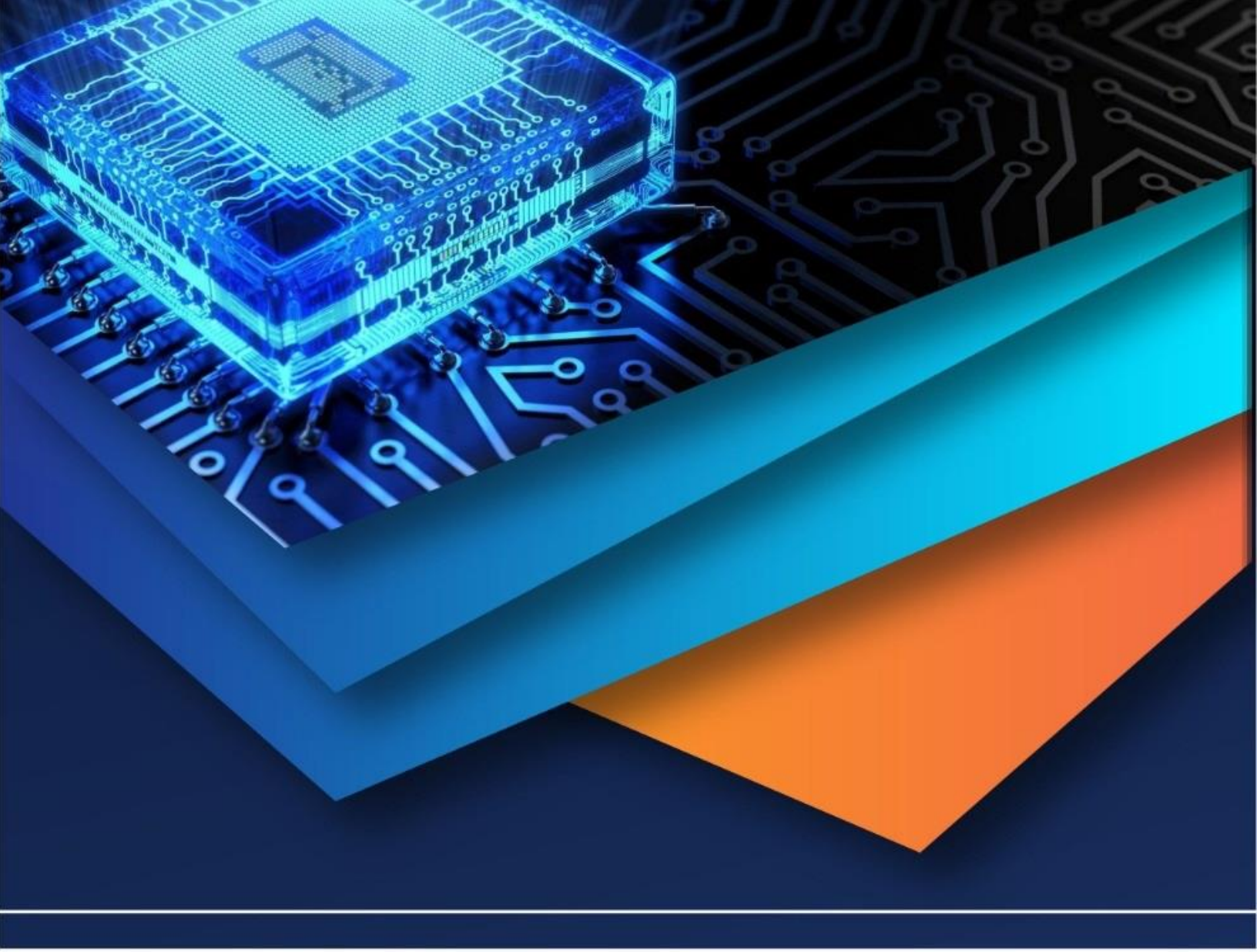
However, it is important to note that a self-defending network is not a substitute for a comprehensive security program. It should be implemented in conjunction with other security measures, such as access controls, firewalls, and intrusion detection systems, to provide a layered defense approach. Additionally, a self-defending network must be properly configured, maintained, and updated to ensure that it remains effective against evolving threats.

In conclusion, a self-defending network is a powerful tool for protecting against cybersecurity threats. It provides real-time protection and enables organizations to quickly respond to attacks, reducing the risk of data breaches and other security incidents. However, it must be implemented with care and attention to both technical and organizational considerations, and should be used in conjunction with other security measures to provide a comprehensive defense approach.

REFERENCES

[1] Kalaivani Chellappan, Ahmed Shamil Mustafa, Mohammed Jabbar Mohammed, Aqeel Mezher Thajeel, “Layered Defense Approach: Towards Total Network Security”, from International Journal of Computer Science and Business Information(IJCSBI), Vol. 15, No. 1. JANUARY 2015.
[2] Yaoxiaoyang, “Study on Development of Information Security and Artificial Intelligence”, from 2011 Fourth International Conference on Intelligent Computation Technology and Automation.
[3] Cisco Self-Defending Networks http://www.cisco.com/go/selfdefend
[4] Enn Tyugu, “Artificial Intelligence in Cyber Defense”, 2011 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011 © CCD COE Publications.
[5] AK. Ghosh, C. Michael, M. Schatz. A Real-Time Intrusion Detection System Based on learning Program Behavior. Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection, 2000, pp.93-109.
[6] B. Iftikhar, A. S. Alghamdi, “Application of artificial neural network in detection of dos attacks,” in SIN ’09: Proceedings of the 2nd international conference on Security of information and networks. New York, NY, USA: ACM, 2009, pp. 229–234.

[7] D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, "Application of artificial neural networks techniques to computer worm detection," in International Joint Conference on Neural Networks (IJCNN), 2006, pp. 2362–2369.
[8] C.-H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, vol. 36, no. 3, Part 1, 2009, pp. 4321–4330.
[9] Self-Defending Networks | IPTP Networks https://www.iptp.net/en_US/business-solutions/security/self-
[10] The Importance of a Self-Defending Network | Allied Telesis https://www.alliedtelesis.com/in/en/blog/importance-self-



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY