International Journal of Research in Engineering, Science and Management
Volume 7, Issue 2, February 2024
https://www.ijresm.com | ISSN (Online): 2581-5792

Paradigm Shift in Adaptive Cyber Defense for Securing the Web Data

Dosanapudi Uday Kumar[1], Petikam Sai Rishi[2], Penmetsa Sai Ganesh Raju[3*], Vemana Lekhaj Valli Kumar[4]
[1]*Assistant Professor, Department of Information Technology, Vishnu Institute of Technology, Bhimavaram, India*
[2,3,4]*Student, Department of Information Technology, Vishnu Institute of Technology, Bhimavaram, India*

***Abstract*: In response to the growing demand for complicated computer tasks and handling large amounts of data, web applications are becoming more sophisticated. However, with the rapid advancements in online technology come significant concerns over security. Attackers are becoming more skilled and well-prepared, and cyberthreats are growing swiftly. Data transmitted via the internet must be more dependable and safer. Certain techniques, known as data provenance-aware techniques, are able to identify instances of data manipulation or unlawful access. They thoroughly examine the data to identify any potential risks and defend against various forms of assaults. Keeping web data and applications safe is a challenge for those in the cybersecurity field, especially as more people use the internet because these techniques can manage issues like missing or ambiguous information and are more effective at defending against internet attacks. They strengthen security by utilizing concepts found in nature, such as deception and camouflage. The effectiveness of these techniques for protecting web data and apps and developing more intelligent security measures will be examined in this article.**

***Keywords*: Web applications, Cybersecurity.**

1. Introduction

Web data has always come from a variety of sources and has been extensively utilized by several technological platforms. These days, artificial intelligence and machine learning are advancing these technologies even farther. But this isn't only a good thing—attackers now have more ways to take advantage of vulnerabilities.

Hackers are growing increasingly skilled at breaking into enterprises with complex algorithms and strong hardware. Because of their organization and coordination, there is a higher chance of large-scale attacks and a higher level of risk to web data. Conventional defense strategies, such as signature-based techniques, are out of date and inadequate for ensuring security and privacy. This can interfere with how businesses operate when under cyberattack.

We require defense strategies that are more flexible and agile to address these intricate security challenges.

Techniques influenced by nature are applied widely and have shown to be dependable and steady in resolving a wide range of issues. These techniques are particularly helpful since they can deal with inaccurate, ambiguous, and partial data, which makes them appropriate for adaptive cybersecurity.

Researchers have developed a novel concept named Nature-inspired Cyber Security (NICS) based on their observations of nature. This method builds a behavior-based security system by imitating the ideas and actions of wild creatures. Through network data analysis and the organization and combination of existing information, NICS provides a natural resilience effect and a range of adaptive protection measures. NICS techniques can also include deception and self-organization in their security solutions.

2. Related Works

We have developed a novel network testbed with the express purpose of evaluating security protocols grounded in Nature-inspired Cyber Security (NICS). This testbed is equipped with an extensive toolkit to facilitate these investigations. It allows us to test the effectiveness of our suggested techniques by simulating NICS security with and without specific attacks enabled. By examining several aspects such as network devices, load, communication kinds, and more, we may examine how the network responds to an active attack. This testbed offers a consistent method for looking at and contrasting various security methods.

We have also tested our NICS-based approach in conjunction with current Intrusion Detection Systems (IDS) to identify web attacks. In this study, we classified hostile activity and sent out early alarms for the Intrusion Detection System using a framework called Firefly Optimization.

3. Related Issues and Challenges

Nature-inspired Cyber Security (NICS) presents a unique set of problems in addition to the many advantages it offers over conventional protection strategies. Processes must be extensively customized, adjusted, and configured in order to implement NICS. Every time it is used in a new context, extensive testing and analysis are needed. This is mostly due to the fact that NICS is still a relatively new idea and that it depends on behavior-based mechanisms, which can be complicated. Thus, NICS implementation can be difficult and time-consuming at first.

Furthermore, before NICS can produce the intended outcomes, additional problems must be resolved.

*Corresponding author: 20pa1a1283@vishnu.edu.in

By experimenting with various nature-inspired algorithms on diverse kinds of networks and application domains, they are investigating the possibilities of NICS.

It is often difficult to understand and mimic the exact relationships and processes of nature, and then to implement them for a stable security mechanism.

- Troubleshooting of NICS-based defense mechanisms are also difficult and requires dedicated manpower in the organization.
- Management of False Positive alert is also very critical and it may hinder the overall system response.
- Additional cost for training and maintenance.
- Many nature-inspired algorithms are yet to be explored. They may perform better than the experimented ones

4. The Future Ahead

In order to constantly address threat management challenges, organizations are focusing more and more on putting information security rules into place and enforcing them. They are looking for defense systems that are more automated, intelligent, and adaptable. Cybersecurity that draws inspiration from nature (NICS) offers a number of exclusive features, including cyberdeception, automated threat detection, self-regulation, and even autonomous computing.

When the cost of an attack exceeds the possible reward for the attacker, a state known as cyber immunity, can be attained with the use of NICS. Emerging defense technologies like NICS, AI/ML, and quantum computing will soon transform security systems as they exist now. In addition to offering improved network visualization, these future technologies will be more accurate, self-learning, and dependable in thwarting assaults and maintaining business continuity.

5. Conclusion

We've talked about the promise of Nature-inspired Cyber Security (NICS), related initiatives, and what lies ahead for this exciting new security paradigm. Still, a fully NICS-based security solution hasn't been fully realized yet.

However, with ideas like network camouflage, cyber deception, and honeypots currently in use, the future of NICS appears bright. When it comes to developing an automated, self-regulating, and adaptive defense system, NICS can be helpful, especially in areas where operational data is dispersed, lacking, or poorly maintained.

The purpose of this editorial is to draw attention to the potential of NICS and to entice readers to learn more about and play around with this new security technology.

References

[1] SK Shandilya, S Upadhyay, A Kumar, AK Nagar, “AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis, Future Generation Computer Systems,” 2022.

[2] SK Shandilya, “Design and Analysis of NICS Based Web Attack Detection for Advanced Intrusion Detection System, Iberoamerican Knowledge Graphs and Semantic Web,” 2021.

[3] Gautam, R., Kaur, P. & Sharma, M., “A comprehensive review on nature inspired computing algorithms for the diagnosis of chronic disorders in human beings,” Prog Artificial Intelligence, 8, 401–424, 2019.

[4] Michael Warner. Cybersecurity: A pre-history. Intelligence and National Security, 27, 2012

[5] Hong S. Choi M. S. Lee S. J. Kim T. W. Lee S. W. Ha B. N. Lim, I. H., “Security protocols against cyber-attacks in the distribution automation system,” IEEE Transactions on Power Delivery, 25(1):448–455, 2010

[6] Robert Dewar, “The “triptych of cyber security”: A classification of active cyber defense,” International Conference on Cyber Conflict, CYCON, pp. 7–21, 2014.

[7] Dewar, Robert, Active Cyber Defense, 2017.

[8] Ricardo Neisse, Gary Steri, Igor Nai Fovino, and Gianmarco Baldini, “Seckit: A model-based security toolkit for the internet of things,” Computers Security, 58, 2015.

[9] Neal Wagner, Cem S¸. Sahin, Jaime Pena, and William W. Streilein, “Automatic generation of cyber architectures optimized for security, cost, and mission performance: A nature-inspired approach,” pp. 1–25, 2019.

[10] Vajiheh Hajisalem and Shahram Babaie, “A hybrid intrusion detection system based on abc-afs algorithm for misuse and anomaly detection,” Computer Networks, 136, 02, 2018.