A Comprehensive Review -Application of Bio-inspired Algorithms for Cyber Threat Intelligence Framework

Manas Kumar Yogi [1], Dwarampudi Aiswarya[2]

Computer Science and Engineering Department, Pragati Engineering College(A), Surampalem, A.P, India

E-mail: [1]manas.yogi@gmail.com, [2]aiswarya.d@pragati.ac.in

Abstract

In most of the modern-day computing systems, security enhancements are a part of security design. The majority of the effort in providing robust security to a system is involved in the identification of cyber threats and how to recover from such cyberattacks. Many researchers have proposed sub-optimal strategies which has been the motivation of this research. This study summarises the research gaps and proposes research direction for mitigating the challenges concerned in that direction. This work reviews the current methodologies to provide a framework which can auto identify cyber threats and to determine how the bio-inspired algorithms can be applied to minimize the effort involved in identification and recovery from cyberattacks. Cyber threat intelligence frameworks serve as crucial elements in providing secure operating environment for the cyber practitioners. The design and development of cyber threat intelligence framework is challenging not only for the cost and effort involved in it but also due to intrinsic dependent entities of cyber security. This study proposes novel principles for bridging the identified research gaps through feature engineering, trust computing base, and bio-inspired based time optimization. There is a lot of research potential in this direction and this study is a sincere and ideal attempt towards the same goal.

Keywords: Cyber, Threat, Bio-inspired, Trust, Security, Intelligence

DOI: https://doi.org/10.36548/rrrj.2023.1.08

1. Introduction

The main motivation for applying bio-inspired algorithms in the spectrum of cyber security are discussed below [1-2]:

(1) The bio-inspired algorithms are adaptive in nature withstanding environmental situations.

(2) Such class of algorithms are robust enough to face faults and don't get effected by internal or external factors.

(3) The bio-inspired algorithms work in a complex factor based on limited set of features.

(4) The bio-inspired algorithms operate in a distributed manner and evolve its nature under dynamic changing conditions.

These attributes are the principal fixings toward making powerful and strong foundations in cyber-security. The idea of dangers/attacks has changed over the couple of years, and cyberattacks have become all the more intentionally designed and destructing. It is continually developing, and expansion in its number plainly features this danger [3]. In the past, the idea of attacks was fundamental, for example, violent attacks for password breaking and Denial of Services (DoS) for holding the assets; in this way, the proposed solutions were exposed to the characteristics of the threat, with no acknowledgment of global impact. For example, DoS attacks are prevented by giving a grace period to a attacking IP address or by denying an IP address (of planned machine/client), though, in the event that an attacker launches an intentionally designed DoS attacks, with the assistance of remotely located bots, the previously mentioned security procedures will be delivered pointless [4-5] . Presently, in this advanced time, the idea of attacks has developed and converted into intentionally designed procedures and virus eradication. In the future, it very well may be self-replicating viruses and attack devices. Accordingly, to stay up with the transformative progressions in cyberattacks, numerous individuals from this new field are engaged toward the advancement of bio-inspired innovative algorithms, to address the current and approaching difficulties for present and modern cyber-frameworks [6].

Table 1 enumerates the types of bio-inspired algorithms which are used to develop aspects of cyber security measures in recent times.

Table 1. Types of Bio-Inspired Algorithms and their Major Area of Research

S.No.	Bio-inspired algorithm	Major research area
1	Evolutionary Strategy	Vehicle routing issues, task scheduling, Structural optimization
2	Genetic Programming	Disease prediction, electric circuit synthesis, Robotics design
3	Particle swarm optimization	Image processing, computer vision, MANETS, multiclass databases, biomedical image processing
4	Ant Bee Colony Optimization algorithm	Image segmentation, pattern classification, project scheduling
5	Ant Colony Optimization algorithm	Classification problems under data mining, dynamic scheduling
6	Differential Evolution	Chemical engineering, filter design, multi-objective optimization problems
7	Artificial Immune System Algorithm	Computer security, virus detection, information retrieval, job shop scheduling, tuning of controllers

2. State of Current Research

1. Formal mathematical models exist for developing trust computing frameworks which focus on the assumptions of the attacker’s attack strengths. High complexity with respect to understanding and applying the trust models [7-8].
2. Rules based access methods for threat detection and classification which does not consider the uncertainty in attack patterns.
3. Efficient topic modeling for collecting cyber threat intelligence data but scarcity of open - source threat intelligence datasets for either analysis or benchmarking [9].

Table 2. Different Methods of Bio-Inspired Cyber Security

S. No.	Ref. No.	Type of bio-inspired algorithm	Application area in cyber security
1	[11]	Ant Foraging, Ant colony, Bird foraging	Intrusion detection, Vulnerability Assessment
2	[11]	Genetic mutation	DDoS Mitigation
3	[11]	Genetic mutation	DDoS Attack deterrence
4	[11]	Genetic mutation	Reconnaissance
5	[11]	Swarm intelligence	Rule based intrusion detection
6	[12]	Cell Regulation	DoS Mitigation
7	[13]	Self/Non Self Determination	Anomaly based intrusion detection

3. Identified Research Gaps [10]:

1. Absence of robust models for trust computing base.

2. Non-optimization of cyber threat intelligence in threat detection frameworks.

3. Efficient methodology for recovery from severe insider attacks in a network.

4. Methodologies Proposed

4.1 For bridging the Research Gap 1

A data centric trust computing framework which uses time-based optimization as an embedded component in a bio-inspired algorithm is proposed. The major advantage will be the feature of determinism by using the class of bio-inspired algorithm [11].

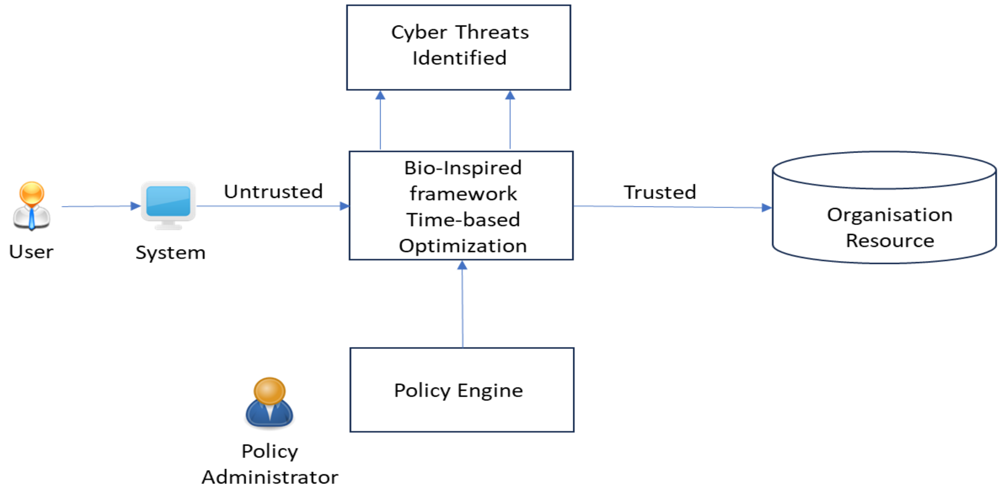

Figure 1. Data Centric Trust Computing Framework

A trust management system which uses the aspect of reputation as input element for Ant Colony algorithm can help in enhancing the security of an organization [14]. It can be done with the help of adjustments in the security and privacy factor. Network resources can also be considered during the adjustment of trust factor and each participating entity can work on the updation of the reputation table. The limitation of this algorithm is that it does not contain the property of service discrimination, i.e., if reputation of a node is poor, then over the time, it cannot be improved [15]. Hence research has to be done in future to develop a mechanism to give chance to such nodes to improve their reputation so that, over time they can become a part of the trust computing environment.

4.2 For bridging the Research Gap 2

Due to the presence of many optimization techniques inherent in the bio-inspired algorithms, the cyber threat intelligence can be converged with a high rate. This intelligence will propel to develop a cyber threat detection model with metaheuristics so that the performance of the framework does not degrade [16].

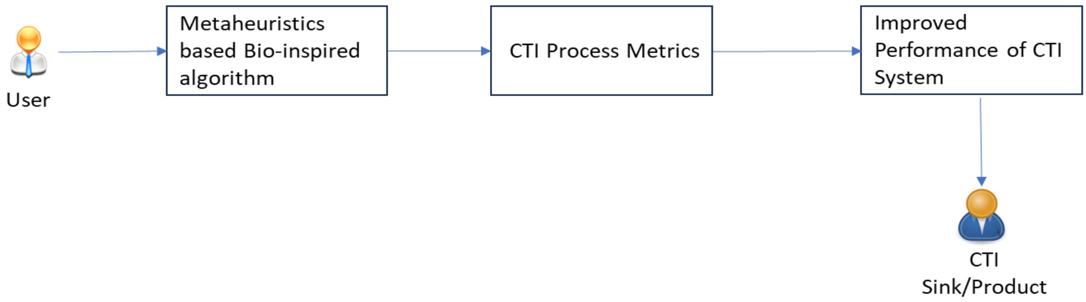
User
Metaheuristics based Bio-inspired algorithm
CTI Process Metrics
Improved Performance of CTI System
CTI Sink/Product

Figure 1. Performance Aware Cyber Threat Intelligence Model

A performance aware Cyber Threat Intelligence (CTI) model depends on factors like effectiveness of the threat intelligence model as well as degree of attack resistance. With the help of bio-inspired model, the convergence rate can be measured which indicates the optimal level of threat intelligence gathered which in turn is helpful in estimation of the performance level of the CTI framework. Simulation results using the bio-inspired algorithms are helpful in knowing if the performance of the CTI framework is increasing or not [17]. If performance is not increasing, then the participating parameters can be fine-tuned further.

4.3 For bridging the Research Gap 3

A one-size fits all security measure cannot handle insider threat. It has been observed that insider threats and attacks arise due to malicious intent but they can be stopped from occurring if proper cyber rules are followed within the company and its employees. Data breaches may be harmful or harmless but security practices must be in place to handle all such inadvertent situations.

Using feature engineering through the bio-inspired algorithms, the point of recovery from a severe attack can be identified as a global minimum and threat models can be developed subsequent to that which will eventually help the security operations centre to reduce the overall system security cost.

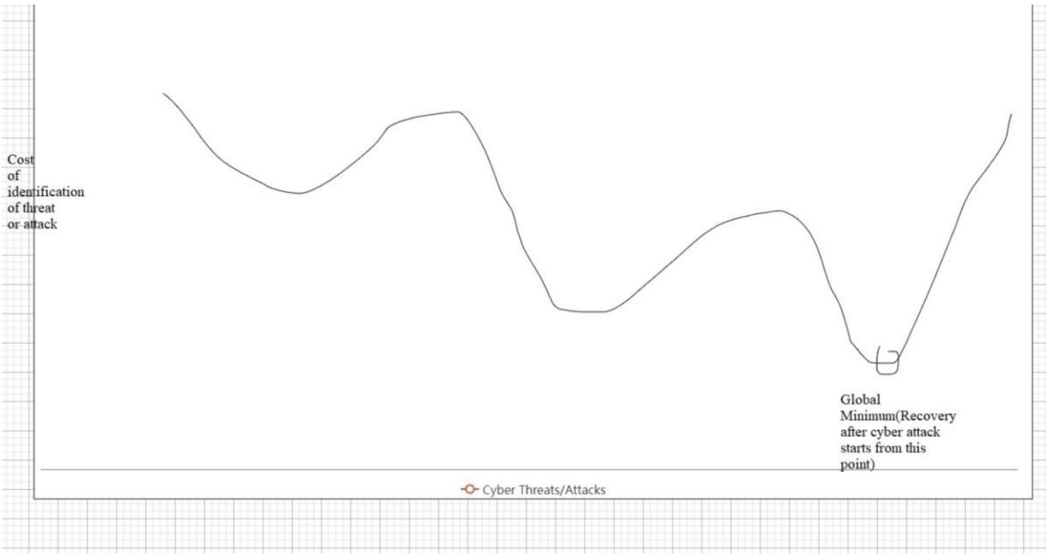

Figure 3. Feature Engineering through Bio-Inspired Algorithm for Recovery from Cyber Attacks

The intrusion detection system raises an alarm when it observes an unusual traffic and is on the lookout for a suspicious activity by anyone. Novel approaches like Binary Swarm Particle Optimization, Binary Firefly Optimization and Modified Cuttlefish Algorithm have been applied to data pertaining to attack datasets and they have shown appreciable results. These datasets are very much similar to real world datasets including the network flows from various source IPs to destination IPs with suitable timestamp. The researchers have extensively used the CICIDS2017 dataset which has information related to up-to-date common attacks [17].

5. Research Findings and Contribution of Research

The research findings can be listed as below:

1. None of the existing mechanisms provide any co-operating mechanism between the security entities, i.e., flexibility is largely constrained.
2. Global risk mitigation with respect to CTI framework is still a challenge due to non-compatible standards operating among the major security compliance organisations.
3. Global threat policy optimization is also a limitation currently due to no correspondence between the state-of-the-art application of bio-inspired algorithms and cyber regulations.

4. Due to independence of cyber threat parameters with respect to time, the bio-inspired consensus protocols need an immediate reformulation, thereby incorporating local dependent parameters in the form of boundaries.

Table 3. Major Contribution of Bio-inspired Algorithms [17]

Motivation	**Technique**	**Security Mechanism**	**Adaptivity**
Swarm Intelligence	Ant colony optimization, Particle swarm optimization	Threat detection, Attack response	offline
Genetic Mutation	Route mutation, Host mutation	Protection, Response, Recovery	online
Bio-Regulation	Cellular Regulation	Response, Recovery	online

6. Future scope

The main motivation of applying bio-inspired algorithm in designing a robust framework for cyber threat intelligence is the evolving nature of big data as threat data and the evolving nature of bio-inspired algorithms. So both the technique and nature of data evolution are in sync with each other. Another challenge in future will be the lack of human expertise in applying bio-inspired algorithms for threat detection and threat prevention. Moreover, the quality of threat data is fuzzy and lacks clarity hence the bio-inspired algorithm's convergence rate to predict a threat or cyber-attack is a challenge for the researchers working in this domain. A special organization named as Cyber Threat Alliance is formed to score and share quality data which are regarded as definite threat data. Development of a common trust computing base depends on aspects of privacy and many companies hesitate disclosing sensitive data pertaining to the company’s internal affairs. Moving beyond the techniques of restricted group based access and mechanisms of ranking the user and their privileges will be useful in the future.

7. Conclusion

Cyber threat intelligence will become the backbone for securing any business or non-business organisation in the future due to the severity of cyberattacks increasing day-by-day. The investment on cyber infrastructure is also increasing every year, hence the investment returns on design and implementation of cyber threat intelligence framework will balance this aspect. Cyber-crime incident handling as well as prevention will help the companies to a greater extent. The weakness of a cyber-perimeter in times of breach by malicious entities will help the cyber security analysts to track the vulnerabilities and mitigate them with a proactive approach rather than risking a reactive approach. This study enumerates the robustness of bio-inspired algorithms to design such Cyber Threat Intelligence model, which includes high degree of adaptability and other dynamic factors which will go a long way in the area of applying such intelligent mechanisms in protecting the cyberspace in the future.

References

[1] Apurv Singh Gautam, Yamini Gahlot, and Pooja Kamat. Hacker forum exploit and classification for proactive cyber threat intelligence. In International Conference on Inventive Computation Technologies, pages 279–285. Springer,2019.

[2] Liang Guo, Senhao Wen, Dewei Wang, Shanbiao Wang, Qianxun Wang, and Hualin Liu. Overview of cyber threat intelligence description. In International Conference on Applications and Techniques in Cyber Security and Intelligence, pages 343–350. Springer, 2021.

[3] Mauro Conti, Tooska Dargahi, and Ali Dehghantanha. Cyber threat intelligence: challenges and opportunities. In Cyber Threat Intelligence, pages 1–6. Springer, 2018.

[4] Ajay Modi, Zhibo Sun, Anupam Panwar, Tejas Khairnar, Ziming Zhao, Adam Doupé, Gail-Joon Ahn, and Paul Black. Towards automated threat intelligence fusion. In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), pages 408–416. IEEE, 2016.

[5] Asif Karim, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti, and Mamoun Alazab. A comprehensive survey for intelligent spam email detection. IEEE Access, 7:168261–168295, 2019.

[6] Asif Karim, Sami Azam, Bharanidharan Shanmugam, and Krishnan Kannoorpatti. Efficient clustering of emails into spam and ham: The foundational study of a comprehensive unsupervised framework. IEEE Access, 8:154759–154788, 2020.

[7] Char Sample, Jennifer Cowley, Tim Watson, and Carsten Maple. Re-thinking threat intelligence. In 2016 International Conference on Cyber Conflict (CyCon US), pages 1–9. IEEE, 2016.

[8] Vasileios Mavroeidis and Siri Bromander. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 European Intelligence and Security Informatics Conference (EISIC), pages 91–98. IEEE, 2017.

[9] Gartner Inc. Definition: Threat intelligence, May 2013. https://www.gartner.com/en/documents/2487216/definitionthreat-intelligence.

[10] TianyiWang and Kam Pui Chow. Automatic tagging of cyber threat intelligence unstructured data using semantics extraction. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), pages 197–199. IEEE, 2019.

[11] Rauf, Usman. "A taxonomy of bio-inspired cyber security approaches: existing techniques and future directions." Arabian Journal for Science and Engineering 43.12 (2018): 6693-6708.

[12] Mthunzi, Siyakha N., et al. "A bio-inspired approach to cyber security." Machine Learning for Computer and Cyber Security. CRC Press, 2019. 75-104.

[13] de Sá, Alan Oliveira, Luiz FR da C. Carmo, and Raphael CS Machado. "Bio-inspired active system identification: a cyber-physical intelligence attack in networked control systems." Mobile Networks and Applications 25.5 (2020): 1944-1957.

[14] Nicolaou, Andreas, Stavros Shiaeles, and Nick Savage. "Mitigating insider threats using bio-inspired models." Applied Sciences 10.15 (2020): 5046.

[15] Balasaraswathi, Veeran Ranganathan, Muthukumarasamy Sugumaran, and Yasir Hamid. "Feature selection techniques for intrusion detection using non-bio-inspired and bio-inspired optimization algorithms." Journal of Communications and Information Networks 2 (2017): 107-119.

[16] Otor, Samera Uga, et al. "An improved bio-inspired based intrusion detection model for a cyberspace." Cogent Engineering 8.1 (2021): 1859667.

[17] Balasaraswathi, M., et al. "Internet of things (Iot) based bio-inspired artificial intelligent technique to combat cybercrimes: a review." Internet of Things in Smart Technologies for Sustainable Urban Development (2020): 141-155.

Author's Biography

Manas Kumar Yogi, currently working as Assistant Professor in Computer Science and Engineering department of Pragati Engineering College (Autonomous), Surampalem, A.P., India. He has over 11 years of teaching and industry experience. His area of interests includes cyber security, machine learning, soft computing, and cyber physical systems. He has published over 150 papers in various reputed national, international journals as well as in conferences.

Dwarampudi Aiswarya currently working as Assistant Professor in Computer Science and Engineering department of Pragati Engineering College (Autonomous), Surampalem, A.P., India. She has over 6 years of teaching experience. Her area of interest includes cyber security and machine learning, data science. She has published 6 papers in various reputed international journals.