Journal of Scientific and Technical Research
14 (2) 2024, 04-10
http://www.publishingindia.com/jstr

Actionable Cyber Threat Intelligence: An Overview and Framework

Neelima Kant[1*] and Amrita[2]
[1]Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India
[2]Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India
[*]Corresponding Author: neelimakant.spm@gmail.com

Abstract: Cyber-attack sophistication is on a definite rise; proactive security strategies need to keep up. In this respect, actionable Cyber Threat Intelligence is of paramount importance for identification, analysis, and mitigation of threats. This paper presents the existing methods of Cyber Threat Intelligence and proposes a new architecture that enhances the actionable capability of threat intelligence with artificial intelligence. It uses machine learning algorithms, Natural Language Processing, and Data Analytics to turn raw data into Actionable Insights, thereby allowing a business to take an informed decision and enhance cybersecurity.

The tactical and operational cyber threat intelligence is the focus, emphasizing tactics, techniques, and procedures (TTPs) that form the foundation of information necessary to exploit a particular organization's network strengths and weaknesses. In this process, this paper surveys a variety of methodologies in use in cyber threat intelligence and underlines the role of threat information in proactive cybersecurity, something very critical in threat and vulnerability reduction. It provides insight into entry points, tactics of threat actors, and system vulnerabilities.

However, in such a large and unstructured areas the task of cybersecurity intelligence becomes demanding. Tactical and operational threat intelligence helps in structuring the bulk of data in unison and turning it into action-based insights, hence enhancing security postures. Adequate machine learning technology is crucial to deal with such huge data volumes and speed up the time-consuming process of gathering actionable intelligence since it is not possible to sort through it manually in a field like cybersecurity that is changing by the minute.

Keywords: Advanced Persistent Threats (APT), Artificial Intelligence (AI), Cyber Threat Intelligence (CTI), Indicator of Compromise (IoC), Internet of Things (IoT), Machine Learning (ML), Vulnerability assessment.

I. Introduction

The enterprise is under cyber threats today that were unheard of a few decades ago. The failure of traditional security measures underlines the need to leverage proactive strategies underpinned by actionable intelligence. This section sets the background for the rest of the paper by underlining the importance of Actionable Cyber Threat Intelligence [1]. Any indication of possible harm, threat, or damage to individuals, groups, organizations, or to society at large is a threat. A threat may be deliberate or accidental, overt or and it can take many forms. Fear, anxiety, or discomfort may be felt and defensive actions are needed. In information technology, threats are termed as possible dangers that may cause a breach of confidentiality, integrity, or availability of information systems. Artificial intelligence in strengthening cyber threat detection, prevention, and response mechanisms has been paramount in the current cybersecurity landscape. Artificial intelligence system is applied in analyzing vast datasets.

By using machine learning techniques, it would help extract and identify a pattern of data invisible to human beings [2]. This, in turn will help AI quickly recognize several threats, whether new or old, as long as they have a clear indication such as malware, phishing attacks, and zero-day exploits. Since AI-driven security solutions would be able to adapt and respond to the evolution of threats, they play an important role in protecting sensitive data and critical infrastructure. AI can also do things like automating repetitive tasks like security incidents. This could enhance the defenses of an organization against more sophisticated attacks, simply by reducing error rates and response times relative to human intervention. With the continued struggle against evolving cyber-security threats in protecting the digital assets and integrity of digital ecosystems, AI continues to be one of the critical technologies.

Cyber Threat Intelligence is a dedicated specialist field concentrated on finding, assessing, and disseminating

information on future and current cyber threats. CTI goes deep into the understanding of threat actors' capabilities, intentions, and tactics in addition to their intended goals and objectives [3]. Many cybersecurity strategies and efforts focus on:

- Proactive identification and mitigation of potential threats improvement in incident response capabilities.
- Development of better defensive strategies identification and prioritization of vulnerabilities for patching and remediation.
- Conducting threat hunting and investigating security incidents are greatly influenced by the priceless insights gained from CTI.

On the subject of artificial intelligence and cybersecurity, cyber threat intelligence occupies a very important position. CTI detects, monitors, analyzes, and finally shares data on potential and actual cyber threats. By using Artificial Intelligence to collect and analyze vast datasets from various sources—including malignant software—Organizations can noticeably enhance their cybersecurity operations through the integration of Artificial Intelligence with Cyber Threat Intelligence. By the use of artificial intelligence, enterprises can actually detect known threats and discover new ones through fast processing of CTI data and identification of threat actors' tactics, patterns, and attack pathways. Planning and execution of security actions by this intelligence provide invaluable insights that can lead to the development and deployment of effective cyber security measures.

In summary, Fig. 1 shows how CTI power by AI can help enterprises to better arrange and manage their cybersecurity operations by detecting and solving potential threats. The organizations can significantly enhance their Cybersecurity Operations Integration with Artificial Intelligence (AI) and CTI. AI enables enterprises to proactively protect known threats and predict new ones by processing CTI data at an incredible speed, recognizing the actors' tactics, patterns, and attack pathways. The planning and execution of security actions in light of this intelligence provide valuable insights that can inform the development and fielding of effective cybersecurity countermeasures. Finally, as Fig. 1 demonstrates, AI-empowered CTI may help a company better coordinate and manage its cybersecurity operations by detecting and mitigating potential threats.

Fig. 1: Cyber Threat Intelligence (CTI): Planning and Direction [4]

The method almost invariably incorporates a feedback loop in the context of social media and CTI, with more than one phase from data collection to feedback-driven planning and direction in this approach as shown in Fig. 1. A generic form might be set out as:

- *Data Collection:* The initial step is to collect the data from different sources in the social media platform. Unless collected lawfully and ethically, this information may consist of public posts, comments, profiles, and even private or restricted information [4]. AI technologies can help a lot in the efficient collection and aggregation of the created data.
- *Processing:* The collected data has to be processed. To make the data serviceable, it has to be cleaned, standardized, and arranged. Data based on text can be, for example, analyzed using such AI-based techniques as sentiment analysis, NLP, from which valuable insights can be extracted.
- *Analyze:* The generation of data is analyzed here using AI algorithms. In social media data, AI is capable of

detecting trends, anomalies, and patterns [5]. To measure the level of threat, it can also be used to profile potential threat actors or to monitor conversations related to specific keywords or topics.

- *Distribution:* The extracted CTI, after analysis, is distributed to the appropriate parties, for example, threat response teams and Cybersecurity teams, amongst others, and decision-makers. AI can support this phase of the CTI life cycle by automatically disseminating information to ensure the right people get it in time.
- *Feedback:* This is a very important component of the CTI process—the feedback phase. AI can help in this stage by capturing sentiment from cybersecurity experts and others. Assessments of how effective security controls are, how effective is the threat landscape's Evolution, and the veracity of threat intelligence are some examples of the feedback that can be supplied.
- *Planning and Direction:* Through the use of a feedback loop, firms can take advantage of the analysis made by CTI and adapt their plans and strategy for cybersecurity. Ranking risks and vulnerabilities, recommending security solutions to match, and even automating responses to known attacks are some areas where AI can assist.

In order to adjust and improve the cybersecurity posture and make sure that it continues to be effective in tackling threats emerging from social media and other sources, the feedback-driven planning and guidance stage is essential. Organizations may safeguard their digital assets and reputation while staying ahead of cyberattacks with the aid of this iterative method [6]. Giving organizations the insight, they need to foresee risks and lessen the effect of security incidents is the ultimate goal of actionable threat intelligence. By taking a proactive stance, companies may make sure that these occurrences don't happen or that they can handle them quickly and efficiently when they do. The paper's following sections are arranged with great care. In addition to providing a thorough overview of actionable intelligence, Section II will point out existing approaches in ACTI and Section III will point out the challenges in achieving ACTI. The study will examine the issues of data processing related to artificial intelligence and machine learning techniques including AI based Framework in Section IV and Section V. We will offer our research findings and potential directions for investigation in Section VI and Section VII. A final summary will be provided in Section VIII, which will be followed by an extensive list of references.

II. Existing Approaches in Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is a dynamic domain that utilizes several techniques to detect and prevent cyber threats [7]. This section gives an overview of a few of the more common methods of CTI, mentioning the advantages and disadvantages of each.

- *Indicator of Compromise (IoC) Analysis*

  Advantages: IoCs or indicators of compromise are small units of information or artifacts such as file hashes, IP addresses, and URLs. IoC analysis happens to be a very fast and proactive technique good at detecting known threats and can be automated.

  Limitations: Since IoC analysis relies on historical data, it is not that potent against new or upcoming threats. Again, it can create false positives and totally fail to detect sophisticated attacks using unique tactics.

- *Signature-Based Detection*

  Advantages: Signature-based detection is based on known threat signatures or patterns that are predefined. It uses resources efficiently and is fairly precise in detecting known threats.

  Limitations: Signature-based detection cannot provide any protection against zero-day attacks or threats using polymorphic or evasive techniques [8]. It requires frequent updates to remain functional and can lead to false negatives on new threats.

- *Anomaly Detection*

  Advantages: Anomaly detection is based on machine learning and AI to recognize major deviations from previously set up baselines. It can find known and unknown threats hence it is versatile.

  Limitations: Anomaly detection can lead to a false positive result in cases where the baselines are not well set or when the model is not well trained [9]. It's resource-intensive and requires a complex setup.

- *Threat Intelligence Sharing Platforms*

  Advantages: Threat intelligence sharing platforms allow the sharing of the CTI among various organizations and cybersecurity communities. They provide collective defense and rapid identification of threats.

  Limitations: These require some level of trust between the participants and, at times, the sharing of sensitive data. It is not always easy to standardize and integrate shared threat intelligence effectively.

While such existing CTI methodologies are not without merit, there are clear limitations. With a fast-changing threat landscape, a more intelligent and flexible strategy is called for [10]. The obvious thing to state is that today's solutions should deliver real-time threat detection and response, contextual analysis, and zero-day threat handling. Clearly, this is not a challenge that a mix of AI and machine learning can't help to outperform; these can continuously learn from new threats, lower false positives, and improve the resilience of the future of CTI lies in disrupting cybersecurity postures [11]. More importantly, staying ahead in this dynamic environment of cooperation and information sharing between industries/organizations is critical to cyber threats.

III. Challenges in Achieving Actionable Intelligence

The pathway to actionable intelligence is paved with challenges that require serious consideration. In the digital age, where the volume of data is exponentially increasing, it is getting more and harder to cut through the noise and spot real threats [12]. We refer to this as information overload. Data quality is still a problem because errors and inconsistencies may compromise intelligence reliability. Intelligence timely disclosure is another critical challenge, because it may further challenge an organization from responding effectively to new emerging threats [13]. These challenges demonstrate the need for cyber threat intelligence to adopt a structured AI-driven platform for data processing, strengthening quality through continuous learning, and accelerate the processing of raw intelligence into useful insights.

IV. Artificial Intelligence in Cyber Threat Intelligence

This section explores the role of Artificial Intelligence in transforming Cyber Threat Intelligence elaborated in Fig. 2. Machine learning algorithms for pattern recognition, natural language processing for text analysis, and predictive analytics for proactive threat mitigation is discussed [14]. Real-world use cases demonstrating the effective integration of AI in threat intelligence is presented.

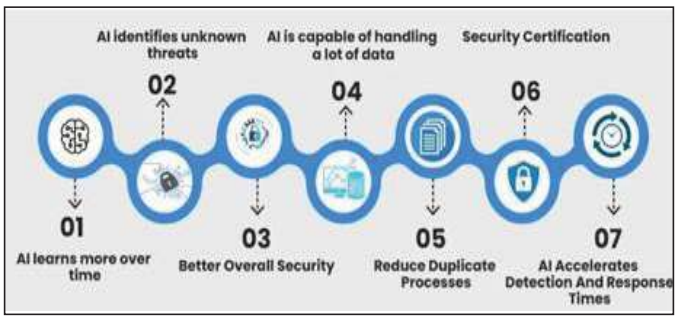

Fig. 2: Using Artificial Intelligence in Cybersecurity [7]

In the domain of Cyber Threat Intelligence, Artificial Intelligence acts as a game-changing force that is changing the face of security strategies. State-of-the-art machine learning algorithms—mainly due to their flexibility and learning capability for complex patterns—remain at the core of this change. Such algorithms provide possibilities for identifying very subtle anomalies and patterns from large sets of data, indicating cyber threats, which strengthen security systems in terms of detection capabilities.

Natural Language Processing (NLP) is applied to text analysis, helping AI systems understand the context and nuances of human language [15]. NLP deciphers the coded language—hidden in unstructured data coming from online forums, social media, Dark Web forums, and so on—to turn up unknown threats and give valuable insights into malicious activities.

Predictive analytics is yet another strong facet of AI that allows an organization to take a proactive stance against any potential threats. It finds threats in the form of cyber-attacks by analyzing historical data and extrapolating future trends [16]. This foresight would enable security teams to reduce the impact of new threats by hardening defenses and putting in place preventative measures at a very quick response rate. Specific application examples in the real world further support the effectiveness of AI in cyber threat intelligence [17]. The importance of integration of AI into threat intelligence procedures has included complex attacks, such as advanced persistent threats and zero-day vulnerabilities, which AI algorithms have correctly identified and interdicted [18]. These examples show some of the practical advantages of AI in empowering cybersecurity defenses and proactive protection of digital infrastructures against continuously changing threats.

V. AI-Based Framework for Actionable Cyber Threat Intelligence

More than ever, given today's dynamic digital environment, there is a need to institute robust cybersecurity measures. In view of the sophistication of cyber threats, they present continued challenges to keeping pace and staying one step ahead of the bad actors. One possible avenue to enhance actionable cyber threat intelligence, in light of this growing concern, is through an AI-based framework [8].

It interrogates vast amounts of data from multiple sources, such as network traffic and system logs, for threat intelligence feeds using the most cutting-edge artificial intelligence algorithms. In applying the machine learning algorithms described in Fig. 3, the system is able to identify patterns and anomalies indicative of potential security breaches or malicious activity. By adopting a proactive approach, businesses will now be in a position to detect and neuter threats before they escalate into full-blown cyber-attacks.

One of the main features of the AI-based framework is the capacity for threat identification and analysis automation. Traditional techniques for cybersecurity depend mostly on human participation, making them laborious and mistake-prone. With AI, organizations can speed up these procedures to answer risks more effectively. The system could learn continually about new cyber threats and update its algorithms to react to the changing cyber threats.

Another added advantage of the framework is that it makes it easier to provide actionability for the enterprise to make wise decisions fast. In turn, enterprises can distill complex data into actionable insights, ranking the risks by level of seriousness and potential effect on the company. This enables concentration on the minimization of critical security threats for better decision-making on the deployment of resources. Other than threat

detection and analysis, AI-based architecture makes proactive threat hunting easier. It allows them to stay ahead of adversaries and helps to prevent possible breaches before they happen due to the search for penetration signs in their network architecture. This proactive approach to threat detection is very important in today's cyber arena where attackers are looking for new ways to bypass security countermeasures.

Another critical component is the potential for the proposed framework to foster collaboration and sharing between organizations. Anonymization and aggregation of threat data make it possible for organizations to share vital intelligence without the risk of exposing sensitive data. By this approach, the cybersecurity posture of all parties concerned is strengthened, and a sense of community resilience against cyber-attacks is developed.

Moreover, the AI-driven architecture itself is flexible and scalable to meet the different requirements of various enterprises. It can be tailored to unique requirements and then adapted to evolving threat environments—whether deployed in small or large firms. Because it is scalable, every type of business can utilize advanced threat intelligence capabilities irrespective of financial or material resources.

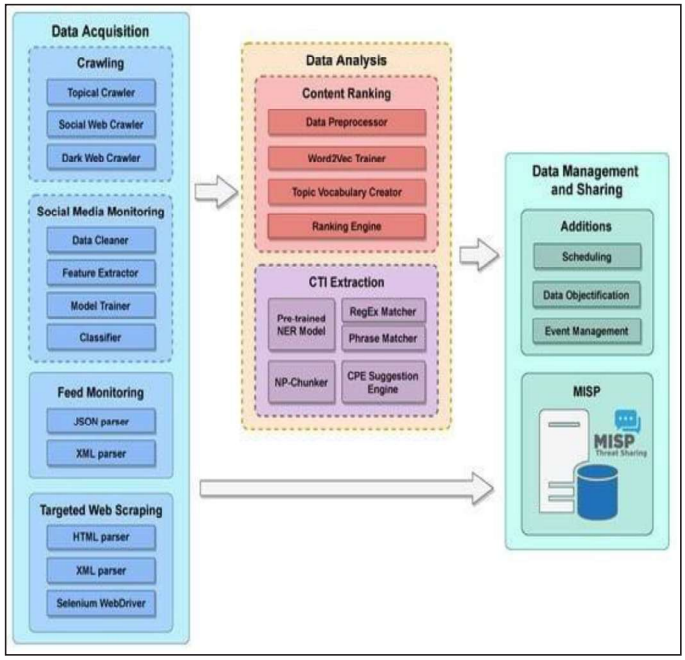

Fig. 3: Cybersecurity Threat Architecture [9]

VI. Case Studies and Validation

This includes the discussion of results, lessons learned, and how the framework improves an organization's cybersecurity posture [19]. Clearly, case studies illustrate how our AI-based platform for actionable cyber threat intelligence is used in real-world scenarios and improves the cybersecurity posture of an organization. We have observed results, priceless lessons, and major improvements in security techniques through these real-world scenarios [20]. Case studies conducted by the research prove the proof of concept of a framework that translates raw data into meaningful insights [21]. Unless an organization makes use of machine learning algorithms, natural language processing, and predictive analytics, it cannot stay several steps ahead of cyber adversaries to proactively modify defenses and quickly identify and mitigate risks [22]. The lesson learned from these deployments is one of survival through continuous learning and evolution in a changing cyber threat environment. The impact of the framework extends beyond rapid threat detection and eradication alone [23]. It builds trust with stakeholders and customers by embedding the culture of proactive cybersecurity within enterprises [24]. As a result, businesses can operate safely, innovate with confidence, and have trust in the digital sphere.

VII. Future Trends and Implications

This means organizations must be able to adapt to changing landscapes of cyber threats, which, in turn, demands insight into future trends and implications of cyber threat intelligence. The block-chain and other emerging technologies have the propensity for bringing about a complete change in the threat intelligence picture [25]. Quantum-resistant cryptographic algorithms will have to be developed since quantum computing has the capability to undermine traditional methods of encryption [26]. A blockchain-decentralized, immutable record could improve the integrity of threat intelligence data and support secure information sharing [27]. But these developments also raise ethical issues about the security of data, its privacy, and how AI should be applied appropriately in cybersecurity [28]. No less important are the implications for policy, since the new regulatory frameworks will have to accommodate the global dimension these cyber-risks take and to lay down standards for cooperation and sharing of threat intelligence. Enterprises must appreciate these future developments and their consequences to protect digital assets and preserve the integrity of the digital ecosystem.

VIII. Conclusion

Major findings are summarized at the end, and the role of actionable intelligence in this war against cyber-attacks is highlighted. The paper serves also to underline the need for integration of AI with cyber threat intelligence and to provide some information on future pathways for implementation and research into this most critical area. The paper provides a critical review of the domain pertaining to actionable cyber threat intelligence, which is very instrumental in mitigating advanced risks resulting from cyberspace. The actionable intelligence reflects remarkably in the current approaches that were critically analyzed and also given a creative proposition for an AI-based framework. Artificial Intelligence, combined with human knowledge, increases the speed and accuracy of

threat detection and makes the effectiveness of decision-making processes in view of the changing threats more proficient in cyber-attacks. A pledged hope in the fight against cyber attackers is the incorporation of AI into Cyber Threat Intelligence. It provides an enterprise with a proactive defense system due to the ability of the technology to analyze enormous amounts of data, spotting complex patterns and delivering insights in real-time. As the cyber world advances further, the interplay between human intellect and AI algorithms assumes pivotal roles. For improved cybersecurity efforts globally, future research should focus on key areas of research in enhancing AI models, ethical investigations, and collaborative frameworks. In this fast-moving digital decade, with morphing threats taking ever-more complicated forms, actionable intelligence remains our finest weapon. Ensuring the resilience of digital societies against the unending wave of cyber threats means paving the way for more secure cyberspace, embracing AI-driven solutions, and collaborative research efforts.

References

[1] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, 2023.

[2] Z. C. Khan, T. Mkhwanazi, and M. Masango, "A model for cyber threat intelligence for organisations," in *2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (ICABCD)*, IEEE, Aug. 2023, pp. 1-7.

[3] O. Kayode-Ajala, "Applications of cyber threat intelligence (CTI) in financial institutions and challenges in its adoption," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 6, no. 8, pp. 1-21, 2023.

[4] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, p. 101804, 2023.

[5] E. S. Bibri, J. Krogstie, A. Kaboli, and A. Alahi, "Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. *Environmental Science and Ecotechnology*, p. 100330, 2023.

[6] M. Lundgren, and A. Padyab, "A review of cyber threat (artificial) intelligence in security management," *Artificial Intelligence and Cybersecurity: Theory and Applications*, pp. 29-45, 2022.

[7] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, 2023.

[8] Z. C. Khan, T. Mkhwanazi, and M. Masango, "A model for cyber threat intelligence for organisations," in *2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (ICABCD),* IEEE, Aug. 2023, pp. 1-7.

[9] O. Kayode-Ajala, "Applications of cyber threat intelligence (CTI) in financial institutions and challenges in its adoption," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 6, no. 8, pp. 1-21, 2023.

[10] A. Lenka, M. Goswami, H. Singh, and H. Baskaran, "Cybersecurity disclosure and corporate reputation: Rising popularity of cybersecurity in the business world," in *Effective Cyber-Security Operations for Enterprise-Wide Systems*, IGI Global: Hershey, PA, USA, 2023, pp. 169-183.

[11] J. Kotsias, A. Ahmad, and R. Scheepers, "Adopting and integrating cyber-threat intelligence in a commercial organisation," *Eur. J. Inf. Syst.*, vol. 32, pp. 35-51, 2023.

[12] H. Gately, "Russian organised crime and ransomware as a service: State cultivated cybercrime," Doctoral Dissertation, Macquarie University, Sydney, Australia, 2023.

[13] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "CTI–issue and challenges," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, pp. 371-379, 2018.

[14] D. Schlette, M. Caselli, and G. Pernul, "A comparative study on cyber threat intelligence: The security incident response perspective," *IEEE Commun. Surv. Tutor.,* vol. 23, pp. 2525-2556, 2021.

[15] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, and D. Moher, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, no. 71, 2021.

[16] H. Suryotrisongko, Y. Musashi, A. Tsuneda, and K. Sugitani, "Robust botnet DGA detection: Blending XAI and OSINT for CTI sharing," *IEEE Access*, vol. 10, pp. 34613-34624, 2022.

[17] H. Moraliyage, V. Sumanasena, D. De Silva, R. Nawaratne, L. Sun, and D. Alahakoon, "Multimodal classification of onion services for proactive CTI using explainable deep learning," *IEEE Access,* vol. 10, pp. 56044-56056, 2022.

[18] E. Irshad, and A. B. Siddiqui, "Cyber threat attribution using unstructured reports in CTI," *Egypt. Inform. J.*, vol. 24, pp. 43-59, 2023.

[19] S. Ejaz, U. Noor, and Z. Rashid, "Visualizing interesting patterns in CTI using machine learning techniques," *Cybern. Inf. Technol.*, vol. 22, pp. 96-113, 2022.

[20] D. Mendez Mena, and B. Yang, "Decentralized actionable CTI for networks and the internet of things," *IoT*, vol. 2, pp. 1-16, 2020.

[21] J. Liu, J. Yan, J. Jiang, Y. He, X. Wang, Z. Jiang, P. Yang, and N. Li, "TriCTI: An actionable CTI discovery system via trigger-enhanced neural network," *Cybersecurity*, vol. 5, Art. no. 8, 2022.

[22] S. Gong, and C. Lee, "Blocis: Blockchain-based CTI sharing framework for sybil-resistance," *Electronics*, vol. 9, no. 3, p. 521, 2020.

[23] L. J. Borges Amaro, B. W. Percilio Azevedo, F. L. Lopes de Mendonca, W. F. Giozza, R. D. O. Albuquerque, and L. J. García Villalba, "Methodological framework to collect, process, analyze and visualize CTI data," *Appl. Sci.,* vol. 12, p. 1205, 2022.

[24] M. Al-Fawa'reh, M. Al-Fayoumi, S. Nashwan, and S. Fraihat, "CTI using PCA-DNN model to detect abnormal network behavior," *Egypt. Inform. J.*, vol. 23, pp. 173-185, 2022.

[25] T. Sun, P. Yang, M. Li, and S. Liao, "An automatic generation approach of the CTI records based on multi-source information fusion," *Future Internet,* vol. 13, p. 40, 2021,

[26] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. J. Pangalos, "Actionable threat intelligence for digital forensics readiness," *Inf. Comput. Secur.*, vol. 27, pp. 273-291, 2019.

[27] G. E. Raptis, C. Katsini, C. Alexakos, A. Kalogeras, and D. Serpanos, "CAVeCTIR: Matching CTI reports on connected and autonomous vehicles using machine learning," *Appl. Sci.,* vol. 12, p. 11631, 2022.

[28] M. Alsaedi, F. A. Ghaleb, F. Saeed, J. Ahmad, and M. Alasli, "CTI-based malicious url detection model using ensemble Gros, S.: Research directions in cyber threat intelligence," in *preprint arXiv:2001.06616*, 2020.