IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

“Beyond The Blackboard: CTI As A Catalyst For Educational Innovation"

Radhika S.N
Department of CSE,JNNCE
Shivamogga, India

Aaliya Waseem
Department of CSE,JNNCE
Shivamogga, India

Abstract—Cyber Threat Intelligence (CTI) performs a key position in fighting cyberattacks, however its achievement mainly depends on the quality of the data predicted. This paper affords an automated approach to evaluate CTI via combining both the reliability of its resources and the relevance of its content material. Using a correlation graph and gadget gaining knowledge of strategies, the technique affords a comprehensive evaluation of CTI records. Testing on real-world datasets shows that this technique extensively improves the accuracy and effectiveness of risk intelligence.

In the training zone, the adoption of CTI may be especially precious as establishments face increasing cyber risks with the upward push of online gaining knowledge of, management systems, and research activities. Incorporating CTI can help faculties and universities enhance their defences in opposition to phishing, ransomware, data breaches, and other cyber threats, ensuring the protection of data and the uninterrupted delivery of educational services.

Keywords—Cyber threat Intelligence, security, education sector.

I. Introduction

The emerging scope of cyberattacks has made Cyber Threat Intelligence (CTI) a critical tool for corporations to live in advance of malicious activities. CTI facilitates come across, prevent, and mitigate cyber threats by way of presenting critical insights into potential dangers. Although, the worth of CTI in large part relies upon its quality, which may vary based totally on the trustworthiness of the assets and the availability of the content material. While existing research has a tendency to assess those elements one after the other, there may be a want for an extra complete evaluation method. This paper analysis advises an automated approach that combines both factors to enhance the accuracy and reliability of CTI, ensuring higher protection.

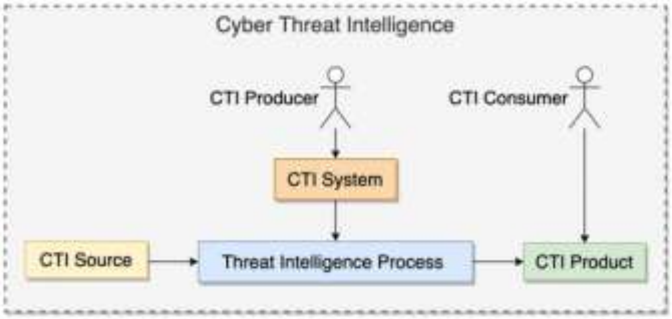


Fig1 : CTI Key Concepts relationships.

The lack of clear definitions in Cyber Threat Intelligence (CTI) regularly leads to confusion, as exclusive authors use diverse terms for the same standards. Fig.1 addresses the hard and fast of primary definitions for key CTI phrases.

Threat intelligence procedure: The steps taken by security analysts to turn raw facts into beneficial statistics.

CTI supply: Any information source that facilitates realisation and guard in opposition to cyber threats.

CTI product: The very last outcome of the threat intelligence procedure that meets positive exceptional standards.

CTI producer: An entity that creates CTI merchandise by making use of the risk intelligence procedure.

CTI patron: An organisation that makes use of CTI to boost its defences or make cybersecurity selections.

CTI gadget: Any gadget or tool that allows carrying out parts of the threat intelligence method.

Vast definition: CTI is the field in which details from different resources are analysed to understand cyber threats, with the attackers' reasons and techniques.This evaluation helps defenders in detecting, stopping, or preferably predicting cyber assaults and making knowledgeable selections.

The education sector is expanding day by day and a top target for cyber threats as colleges, schools, and universities are increasing and rely on virtual equipment and online systems. With sensitive records like student records, economic data, and research. Here are some of the key threats the education sector faces.

Phishing: Cybercriminals trick personnel and college students into sharing personal facts via fake emails, calls or messages, mainly to steal credentials.

Data Breaches: Sensitive data, like educational and monetary statistics, can be stolen and misused, mainly to identity theft and loss of consideration.

DDoS Attacks: When the school data overloads, networks cause them to crash, stop online instructions and access to essential assets.

Insider Threats: Staff or students, both deliberately and by chance, misuse the information, leading to facts leaks or system disruptions.

Theft of Intellectual Property: Most of the time the research records and patents are targeted, which harms the institution's recognition and economic status.

Cloud Security Issues: Vulnerabilities in cloud-based systems can display sensitive facts and disrupt services.

Unsecured Personal Devices: Students or staff using non-public gadgets for schoolwork cans accidently offer access factors for cyber attacks if their gadgets are not secure.

Strengthening cyber security in those areas is vital for protective the schooling zone from evolving threats.

II.RELATED WORK

The [1] Cyber hazard intelligence (CTI) is turning into a powerful tool inside the combat in opposition to malicious online activities. However, the effect of CTI relies upon largely on how true the statistics are. Current research shows that CTI quality comes from either the supply or the content material. In this paper, automatic technique is introduced to assess CTI exceptional through combining the trustworthiness of CTI sources with the reliability of CTI content. The correlation graph is built to analyse how special CTI feeds have interaction, the use of an iterative set of rules to measure the trustworthiness of each feed. Then the content of the CTIs is used for the machine to gain knowledge for assessing the availability based on diverse content material metrics. By combining both the trustworthiness of the feed and the fineness of the content,it provides a greater whole technique for assessing CTI. The experiments using real records, show that this method can efficiently degree and enhance CTI quality.

The [2] CTI is crucial for identifying and reducing cyber and bodily threats to prevent potential attacks. With the speedy development of technology like ICT, IoT, and Industry 5.Zero, there was an explosion of records on modern-day and ability cyber threats targeting agencies. As a result, sharing CTI among organizations may be fairly beneficial, assisting them respond fast to attacks and mutual advantages via collaboration. However, exchanging CTI across distinctive organizations comes with huge demanding situations. These consist of felony and regulatory troubles, compatibility between one of kind structures, and ensuring records reliability. Unfortunately, the cutting-edge kingdom of CTI sharing isn't always well understood, making it tough to fully cope with the desires and challenges groups face whilst sharing this intelligence. This paper, offers a complete evaluate of CTI sharing, beginning with the fundamentals of CTI and the way it has advanced in figuring out threats and threat actors. Additionally, the fundamental demand is highlighted in situations concerned in CTI sharing and compare how present answers attempt to tackle those issues. Lastly, the numerous suggestions promising future research regions to help guide the continued improvement of powerful CTI sharing practices.

In [3] Addressing Advanced Persistent Threats (APTs) is important for governments, companies, and cybersecurity groups. APT-Scope is a brand new gadget that enables analyze Cyber Threat Intelligence (CTI) by means of accumulating, enriching, and reading real-international statistics. It builds a community of relationships between distinct entities and makes use of system getting to know to predict connections among them.This helps to identify APT group aliases(false identities) and unknown attackers.APT-Scope executed properly in exams, reaching a 96%, 57% schooling score and 92.36% check rating, making it a treasured tool for tracking and responding to APT threats.

The [4] upward thrust of the Internet of Things (IoT) and Industry 5.0 has dramatically modified the cyber threat panorama, requiring organisations to discover new approaches to manage dangers.CTI sharing has become a key awareness, but sharing sensitive facts can pose dangers like information leaks or reputational damage. While some methods use blockchain to decorate privateness, many lack dynamic decision-making and quality-grained control over what is shared. In this paper, the Priv-Share is endorsed, a blockchain-based total framework that addresses those gaps. By the usage of differential sharing, trustless delegation, and democratic management, Priv-Share gives scalable and secure CTI sharing. Each theoretical and practical (the usage of Ethereum), show that Priv-Share is a feasible answer for real-global use.

The [5] Proactive cyber-hazard assessment is becoming more vital because it prevents cyber incidents across various sectors via shielding statistics integrity, confidentiality, and availability. With the growing connectivity of cyber-bodily systems, there's greater uncertainty around rising vulnerabilities. This paper introduces a statistical framework for assessing and prioritizing cyber-vulnerabilities underneath uncertainty. The use of mid-quantile regression to deal with ordinal danger checks and compare it with different techniques for ranking dangers. The version is tested on both simulated and actual statistics, permitting to evaluate special methods and talk how constrained information of vulnerabilities affects selection-making in cybersecurity.

The [6] digitization of agriculture, significant to Agriculture 4.0, has added many advantages however additionally expanded cyber security dangers. With clever farming technologies turning into extra not unusual, the rural region is now a goal for cyberattacks.This paper opinions present cyber hazard intelligence (CTI) techniques for smart farming infrastructures (SFIs) and creates an in depth guide to CTI tools suitable for this context. A key locating is the need for a virtual Chief Information Security Officer (vCISO) in clever agriculture. Although not but extensively used, a vCISO ought to appreciably improve safety by using providing strategic steering, growing strong protocols, and handling real-time cyber threats. This would be vital for shielding the meals supply chain and making sure resilience against evolving cyber dangers inside the digital age.

In [7] Global cyber-assaults have severe impacts on economies, societies, and individuals, but present day research lacks AI-pushed answers for offering USA-extensive cyber danger intelligence. This paper introduces an AI-primarily based gadget that automatically gathers and analyses cyber-assault facts from social media. The machine makes use of superior AI algorithms for duties like anomaly detection, prediction, sentiment analysis, and vicinity detection. Between October 11 and October 31, 2022, it accrued over 30,000 statistics on cyber threats and analyzed almost 3800 cyber-related tweets in 37 languages, translating non-English ones. This device, the first to use a CNN-based method to stumble on and expect global cyber-attacks, helps choice-making across a couple of platforms like IOS, Android, and Windows.

In [8] Cyber-hazard attribution, identifying the attacker behind a cyber-attack, is hard because attackers use strategies to cover their identification. After an attack, investigators gather proof from machine logs and submit reports; however these reviews come in different codec's, making it hard to extract useful statistics. Manually studying these unstructured reviews is tough, so this study aims to increase an automated technique to profile cyber threat actors (CTAs) the usage of natural language processing (NLP) and machine mastering.

The method includes extracting key functions like approaches, tools, malware, and goal companies the usage of a specialized embedding model referred to as "Attack2vec." This version, trained especially on cyber security statistics, plays better than popular models. Machine learning algorithms like selection timber, random forests, and help vector machines are used to classify CTAs, accomplishing excessive accuracy (96%), precision (96.4%), recollect (95.58%), and F1-score (95.75%).

In [9] Cognitive biases are commonplace intellectual mistakes caused by the simplified questioning processes. In intelligence communities, especially where clinical and cyber intelligence overlap, those biases can create severe cyber security risks. These errors are considerable and have an effect on maximum analysts, regardless of intelligence or potential. A loss of connection to the natural world all through development can grow the tendency for ecological harm and enlarge those cognitive biases. The biases are difficult because of their deep roots in human evolution. This paper shows a brand new model in which scientific and cyber intelligence paintings collectively, led by a "Symbiont" or "Cybiont" parent. This function could use pc networks to fast proportion and manipulate knowledge, supporting reduced ecological effect and improve techniques to counter biases in intelligence work.

In [10] CTI is a treasured tool for fighting cyberattacks, but its value depends on its first-class.Most contemporary strategies verifies CTI pleasant through looking at both the supply and content material separately. In this paper, the automated method to assess CTI great by way of combining both the trustworthiness of the resources and the availability of the content material. A correlation graph to analyze CTI feeds and use system mastering to assess content material availability. The technique provides an extra entire evaluation of CTI high-quality, and assessments on actual statistics show that it really works efficaciously to enhance chance intelligence.

III. METHODOLOGY

Cyber Threat Intelligence (CTI) in the education sector facilitates faculties, and universities to guard against the cyber attacks through gathering and analysing data on potential threats. Below Fig.2 shows how CTI works.

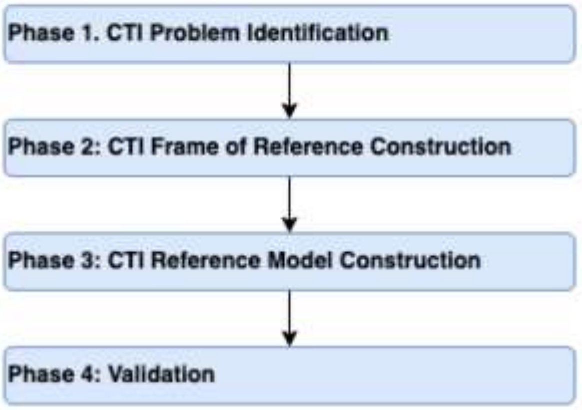

Phase 1. CTI Problem Identification
Phase 2: CTI Frame of Reference Construction
Phase 3: CTI Reference Model Construction
Phase 4: Validation

Fig 2: CTI model design methodology

Data Collection: CTI gathers statistics from extraordinary assets, consisting of online hobby, emails, and network logs, to perceive capacity dangers like phishing, ransomware, or fact breaches.

Threat Analysis: Experts analyze the accumulated data to understand the character of these cyber threats, who is probably at the back of them, and what methods they're the use of.

Sharing Information: The information/findings are shared with IT groups and faculty directors, helping them brief up their cybersecurity systems.

Real-Time Alerts: CTI tools can offer real-time signals while a danger are detected, permitting faculties to reply quickly to capability assaults.

Proactive Defense: By predicting capacity threats and mastering from beyond incidents, CTI enables instructional institutions to stay one step in advance.

In short, CTI enables colleges to put together and save them from cyberattacks, making safer virtual environments for college kids and personnel.

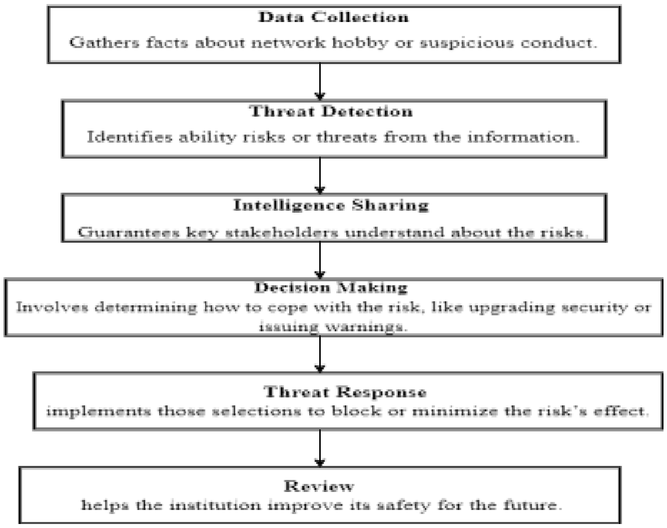

Data Collection
Gathers facts about network hobby or suspicious conduct.
Threat Detection
Identifies ability risks or threats from the information.
Intelligence Sharing
Guarantees key stakeholders understand about the risks.
Decision Making
Involves determining how to cope with the risk, like upgrading security or issuing warnings.
Threat Response
implements those selections to block or minimize the risk's effect.
Review
helps the institution improve its safety for the future.

Fig.3: Flowchart of CTI in education sector

3.1 Case Study on CTI in Education Sector

A huge university with over 30k students is dealing with a rise in cyber attacks, along with phishing scams, ransom ware, and information breaches. Sensitive data and research facts have been at danger, prompting the university to undertake a Cyber Threat Intelligence (CTI) system to live ahead of those threats.

Problem: The University struggled with:

Phishing Attacks: Fake emails tricking workforce and college students into giving up login credentials. **Ransomware:** Attackers targeting critical research statistics and administrative structures. **Data Breaches:** Personal and educational facts being compromised.

Objective: The intention turned into to detect and respond to threats early, minimize damage from attacks, and strengthen the institution's normal cyber security.

Solution: CTI Implementation

Data Collection: The college facts from network logs, login interest, and outside hazard feeds.

Threat Detection: AI gear analyzed these records to identify uncommon conduct, which include failed login attempts or phishing emails.

Threat Sharing: The CTI group shared actual-time intelligence with IT personnel to quick block attacks and alert customers.

Response: Immediate moves like enabling two-thing authentication (2FA) and schooling team of workers on phishing decreased assault achievement fees.

Learning: After preventing a ransom ware attack, the university great-tuned its defense techniques.

IV. RESULTS

In a case like this, results can be provided in diverse approaches to efficiently speak of the impact of the Cyber Threat Intelligence (CTI) implementation. Here are some not unusual strategies:

1. Quantitative Metrics

Before-and-After Comparisons: Show percent discounts in phishing tries, hit attacks, and fact breaches.

Cost Savings: Highlight monetary financial savings from keeping off ransom bills or decreasing healing fees.

Response Times: Illustrate improvements in how quick threats are detected and addressed.

Eg: **Phishing Success Rate:** Decreased through 40% after education and cognizance applications. **Ransomware Prevention:** Saved the college $500,000 by means of stopping an ability attack**.** **Data Breaches:** Reduced by using 50% in the first year.

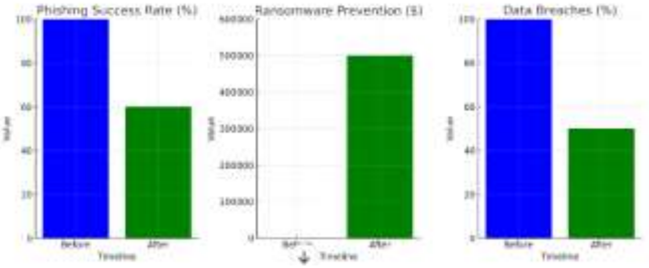


Fig.4: Flowchart of CTI in education sector

2. Graphs and Charts

Bar Graphs: Compare the quantity of assaults before and after CTI implementation.

Line Charts: Show trends over the years for incidents, along with reducing phishing tries.

Pie Charts: Visualize the distribution of different styles of threats encountered.

Eg: A bar graph showing the decline in phishing tries from 100 incidents/month to 60 incidents/month.

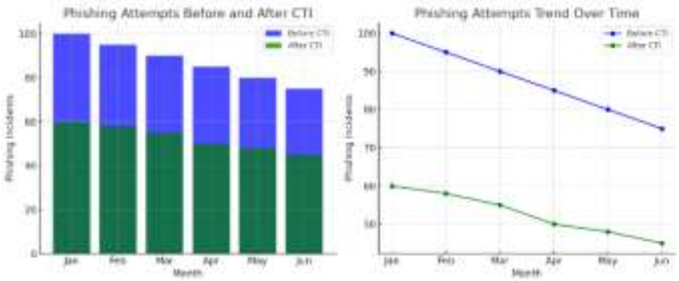


Fig.4: Graph showing before and after phishing CTI attempts

3. Case Highlights

Incident Summaries: Briefly describe particular incidents wherein CTI made a giant distinction, like thwarting a ransomware attack.

Testimonials: Include prices from IT groups of workers or directors about the effect of the CTI machine.

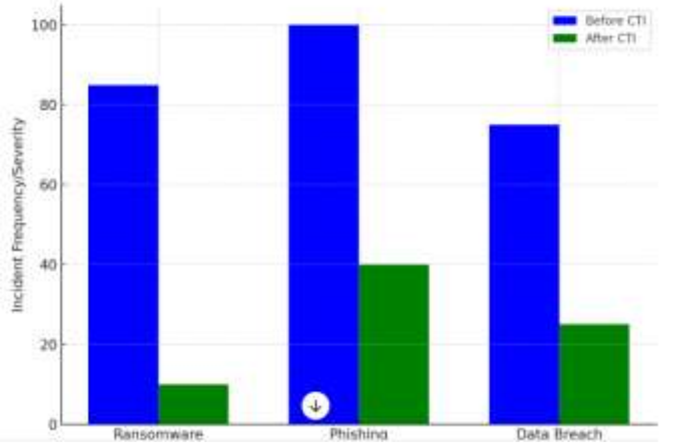


Fig.5: Graph showing before and after CTI

4. Narrative Summary

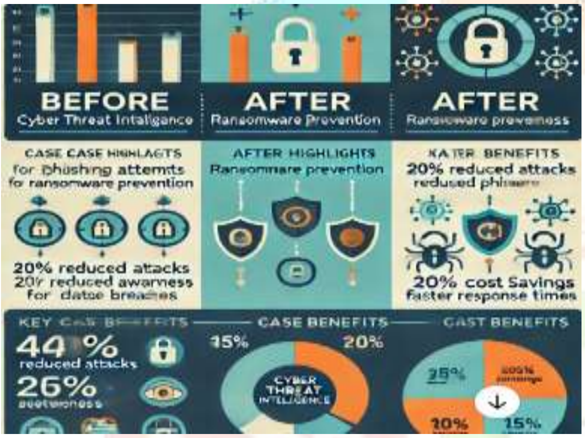
Key Takeaways: Summarise the overall advantages, consisting of stepped forward protection posture and more advantageous attention amongst the body of workers and college students.

Eg: The CTI implementation not handiest decreased the quantity of successful assaults but additionally fostered a lifestyle of cybersecurity focus in the university community.

5. Infographics

Create a visual illustration combining metrics, case highlights, and summaries to engage readers efficiently.

By the use of these techniques, the outcomes of the CTI implementation may be surely and correctly communicated to stakeholders.



V. CONCLUSION

By adopting a CTI device, the university received a proactive protection against cyber threats, minimizing disruptions and protecting both students and studies. This method significantly advanced cyber security and reduced the number of hit attacks.

VI. REFERENCES

[1] Libin Yang, Menghan Wang , Wei Lou, "An Automated Dynamic Quality Assessment Method for Cyber Threat Intelligence", Published by Elsevier Ltd, (http://creativecommons.org/licenses/by-nc-nd/4.0/), August 28, 2024.

[2] Poopak Alaeifar , Shantanu Pal , Zahra Jadidi , Mukhtar Hussain , Ernest Foo, "Current approaches and future directions for Cyber Threat Intelligence sharing", Journal of Information Security and Applications 83 (2024) 103786, https://doi.org/10.1016/j.jisa.2024.103786, 17 May 2024.

[3] Burak Gulbay , Mehmet Demirci ,"APT-scope: A novel framework to predict advanced persistent threat groups from enriched heterogeneous information network of cyber threat intelligence", Elsevier, Engineering Science and Technology, an International Journal 57 (2024) 101791, https://doi.org/10.1016/j.jestch.2024.101791, 17 August 2024.

[4] Kealan Dunnett , Shantanu Pal , Zahra Jadidi , Volkan Dedeoglu , Raja Jurdak, "Priv-Share: A privacy-preserving framework for differential and trustless delegation of cyber threat intelligence using blockchain", Elsevier, Computer Networks 252 (2024) 110686, https://doi.org/10.1016/j.comnet.2024. 110686 , Accepted 30 July 2024.

[5] Mario Angelelli , Serena Arima , Christian Catalano , Enrico Ciavolino, "A robust statistical framework for cyber-vulnerability prioritisation under partial information in threat intelligence", Elsevier, Expert Systems With Applications 255 (2024) 124572, https://doi.org/10.1016/j.eswa.2024.124572 , Accepted 20 June 2024.

[6] Hang Thanh Bui, Hamed Aboutorab, Arash Mahboubi, Yansong Gao, ,Nazatul Haque Sultan , Aufeef Chauhan , Mohammad Zavid Parvez , Michael Bewong ,Rafiqul Islam , Zahid Islam , Seyit A. Camtepe , Praveen Gauravaram , Dineshkumar Singh , M. Ali Babar , Shihao Yan,"Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems", Elsevier, Computers & Security 140 (2024) 103754, https://doi.org/10.1016/j.cose.2024.103754, Accepted 6 February 2024.

[7] Fahim Sufi , "A global cyber-threat intelligence system with artificial intelligence and convolutional neural network", Elsevier, Decision Analytics Journal 9 (2023) 100364, https://doi.org/10.1016/j.dajour.2023.100364 , Accepted 10 November 2023 .

[8] Ehtsham Irshad , Abdul Basit Siddiqui, "Cyber threat attribution using unstructured reports in cyber threat intelligence", Elsevier, Egyptian Informatics Journal 24 (2023) 43–59, https://doi.org/10.1016/j.eij.2022.11.001, Accepted 30 November 2022.

[9] Paolo Zucca, “Four cognitive-ecological biases that reduce integration between medical and cyber intelligence and represent a threat to cybersecurity”, Elsevier, Forensic Science International: Animals and Environments 2 (2022) 100046, https://doi.org/10.1016/j.fsiae.2022.100046 , Accepted 25 March 2022.

[10] Libin Yang, Menghan Wang, Wei Lou, “An Automated Dynamic Quality Assessment Method for Cyber Threat Intelligence”, Elsevier, Computers & Security (2024), https://doi.org/10.1016/j.cose.2024.104079 , 23 August 2024.