ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

Preparing for Unknown Cyber Threats: A Comprehensive Review of Framework for Speculative Threat Intelligence Using Cross-Domain Indicators

Adeyemi Afolayan Adesola[1]

[1]Computer Science Department, Stephen F. Austin State University, Nacogdoches, Texas, USA, 75965

ORCID: 0009-0004-4325-5641

Publication Date: 2025/05/16

Abstract: The cybersecurity landscape is changing so fast. We need advanced threat intelligence frameworks. They should predict, detect, and prevent emerging risks in various domains. Thus, this review aimed to examine frameworks for cyber environments. These include cyber-physical systems (CPS), IoT networks, blockchain platforms, and cloud infrastructures. We aimed to evaluate their effectiveness and find gaps. Then, we would propose ways to improve cybersecurity resilience. Our study used a systematic review of the literature. It analyzed frameworks that use technologies like AI, ML, and automation. We found some strengths in the existing frameworks. They include real-time threat detection, adaptive defenses, and cross-domain collaboration via unified taxonomies. The key limitations, however, were high implementation costs, technical complexity, and scalability challenges. We thus concluded that while current frameworks have noteworthy capabilities, their adoption is generally limited by resource and technical barriers. We recommend that simplifying deployment processes, fostering interdisciplinary collaborations, and leveraging emerging technologies can help create scalable and effective cybersecurity solutions. To address the gaps identified, we proposed a hypothetical Adaptive Multimodal Threat Intelligence Framework (AMTIF), aimed at mitigating the laxities of existing frameworks. AMTIF combines data standardization, predictive analytics, behavioral simulations, and secure cross-domain data sharing. Using emerging technologies, such as blockchain, quantum computing, and self-supervised learning, we expect AMTIF to advance speculative threat intelligence.

Keywords: *Cyber-Physical Systems, Predictive Analytics, Cross-Domain Collaboration, Machine Learning, Adaptive Defenses, IoT Security, Blockchain Threat Intelligence*.

How to Cite: Adeyemi Afolayan Adesola. (2025). Preparing for Unknown Cyber Threats: A Comprehensive Review of Framework for Speculative Threat Intelligence Using Cross-Domain Indicators. *International Journal of Innovative Science and Research Technology*, 10(4), 3939-3958. https://doi.org/10.38124/ijisrt/25apr2255.

I. INTRODUCTION

We are currently in a world where everything is becoming digitalized day by day and due to this, we are more prone to cyberattacks[1, 2]. Due to the fact that almost everything is being digitalized, cyberattacks have now become more complicated. Most of the time, these threats include things like advanced threats, new security flaws, and highly targeted ransomware attacks. Interestingly, and maybe annoyingly, new technologies such as artificial intelligence (AI) and smart devices (IoT), have provided more ways and tools for hackers to attack. Chakraborty et al.[3] referred to this new wave of threats brought on by AI and IoT as “intelligent threats”. In addition, geopolitical conflicts and cyberwarfare have made cyber threats much harder to predict and due to this, we need better and more advanced ways to defend against these threats[4].

Hence, preparing for threats, predicting or preempting them is very important so as not to be caught unaware and this helps in maintaining organizational and national cybersecurity resilience[5]. These kinds of threats are referred to as "unknown-unknowns" by experts. Even though Heinonen et al.[6] described these unknown unknowns as being a potentially measurable threat themselves, it has been proven over time that reacting to attacks after they happen is not enough because using traditional approaches only focuses on known threats and patterns[7]. Hence, proactive measures need to be taken to stay ahead of these evolving dangers. One way to do this is by being able to forecast potential vulnerabilities

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

and integrate advanced intelligence into defense mechanisms so as to strengthen it[8].

Speculative threat intelligence can be referred to as the use of predictive analytics, scenario planning, and heuristic methods to anticipate potential cyber threats before they can even become threatening[9-11]. That is, they are used to predict cyber threats before they happen. This approach uses tools like data analysis to plan for different attack scenarios, and also smart ways of solving cyber problems. It involves analyzing a combination of data from many sources like past events, users' behavior, and unusual system activities[9]. This information is then sifted for similarity in patterns so as to find hidden risks that older methods might miss[12]. For example, data from fields like finance or healthcare can help find weaknesses that could affect other industries too.

- *Hence, the objectives of the systematic literature review were to:*

- Identify current research on speculative threat intelligence and cross-domain indicators.
- Identify gaps in existing frameworks for addressing unknown cybersecurity threats.
- Propose a comprehensive, interdisciplinary approach to enhance threat intelligence methodologies.

II. METHODOLOGY

A. Keywords and Search Terms

We searched the literature. We focused on peer-reviewed journals, conference papers, and trusted books in the ACM Digital Library. The search aimed to fully cover the topic of cybersecurity threats and methods related to it. We used a couple of search algorithms with specific terms and filters to find relevant literature. The first search algorithm focused on the terms "unknown," "cybersecurity," and "threat."

We applied a filter for e-publication dates within the past five years. This search yielded a total of 73 results, and from these, we selected 44 articles for further review. The second search algorithm employed the terms "cyber threat," "intelligence," and "methodologies." Once again, we filtered the results to include only those published in the past five years. This search produced 23 results, from which we chose 11 articles to include in our analysis.

From the 55 articles identified through the two search algorithms, 46 were selected for systematic analysis. The remaining nine articles were excluded because they were of low relevance to the main topic and objectives of our study. All the 46 articles included were full-text journal publications, published within the past five years.

B. Inclusion and Exclusion Criteria

To ensure the relevance of our research, we included studies published between 2019 and 2025. We focused exclusively on peer-reviewed articles and conference papers that explicitly discuss speculative intelligence, cross-domain indicators, or their applications within the field of cybersecurity. Furthermore, we restricted our selection to publications in the English language. We also exclude certain types of documents from our review. This included review articles and non-peer-reviewed pieces such as blog posts and opinion articles. Additionally, studies that concentrate solely on retrospective threat analysis without incorporating predictive methodologies were not considered. Finally, any research that was not available in full text was also excluded from our analysis.

C. Data Extraction

The studies included in the review were organized into several key themes. A key theme was emerging threat intelligence frameworks. They highlighted the latest strategies and methods in the field. Also, we looked at case studies. They showed how different sectors can share and use threat intelligence. They can do this through cross-domain indicators. Lastly, the review found gaps in addressing unknown cyber threats. It emphasized the need for more research to improve cyber resilience.

For effective data management, we used Endnote. Endnote is an excellent tool for managing references. It helped us organize the bibliographic data efficiently. Additionally, we used Excel to track search results and filter studies based on their relevance. We used these tools to make data management easier and boost productivity.

D. Analysis Approach

Thematic analysis was carried out to identify common patterns in methodologies that were focused on how the integration of data from different fields and artificial intelligence is used in speculative intelligence. Alongside this, we also combined studies to create a clear story of how speculative intelligence works and how it can be applied in different areas. This combination of thematic coding and narrative synthesis creates a complete and easy-to-understand view of the subject.

III. CONCEPTUAL FOUNDATIONS

A. Speculative Threat Intelligence

Speculative Threat Intelligence (STI) refers to the identification of possible cyber threats before they manifest through predictive and heuristic methodologies. STI does not operate like traditional threat intelligence, whose primary focus is on known and past threats. Instead, it looks for "unknown-unknowns" by spotting trends, combining data from different fields, and also leveraging advanced computer models[13]. The key distinguishing features include:

- **Predictive Analytics**: Using statistical modelling and machine learning to predict possible weak spots.
- **Heuristic Techniques**: Creating hypothetical scenarios to explore how attacks might happen.
- **Interdisciplinary Data Integration**: Bringing in knowledge from areas like psychology and logistics to build a wider view of threats.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

The concept of STI has evolved just as much as cyber threats have grown in sophistication. Speculative Threat Intelligence initially started in defense and military intelligence but became popular in commercial and governmental sectors in the 2000s[14, 15]. With the rise of AI and big data, the STI tools of today can detect problems in real time, predict threats using diverse data, and allow teams to share intelligence[12].

Current trends in STI include the use of AI-powered forecasting tools and a shift towards planning by imagining and preempting possible threat scenarios. For example, Lin et al.[16] used a scenario-prompt generator, the ICARUS matrix, to predict and simulate potential space cyber attacks with the idea that this is a step in the right direction toward speculative threat intelligence.

B. Cross-Domain Indicators

Cross-domain indicators (CDIs) are data points gotten from different domains such that when they are combined and analyzed, cyber threats can be predicted. These indicators may include:

- **Behavioural Data**: How people interact on digital platforms.
- **Economic Signals**: Strange ffinancial activity such as sudden changes in cryptocurrency transactions.
- **Logistical Metrics**: Problem in supply chain operations.
- **Social Trends**: What people are saying on social media about certain issues.

For instance, a sudden spike in certain financial transactions during a geopolitical event could mean a ransomware operation is happening[17].

➢ *The application of CDIs Enhances Cybersecurity by Enabling:*

- **Early Warning Systems**: Spotting unusual activity early to detect threats in various areas before they grow.
- **Improved Risk Assessment**: It gives a complete and perfect picture of where vulnerabilities might exist.
- **Interdisciplinary Collaboration**: They bring together experts from different areas, like finance and cybersecurity, to solve problems.

CDIs have been particularly impactful in areas such as healthcare, where patient data, supply chains, and IT systems overlap, creating opportunities to spot threats more effectively.

C. The Need for Frameworks

Despite advances in threat intelligence, most of the current methods of dealing with cyber threats mostly react after an attack happens. These are traditional methods that depend on outdated defense models that do not adapt well to modern threats[8]. Most importantly, a lot of organizations do not have the required tools to process and synthesize large datasets effectively. This makes them work in isolated teams with limited awareness. Cross-domain indicators however provide a pathway to overcome these limitations by:

- **Expanding the Scope of Data Analysis**: CDIs allow organizations to move beyond traditional IT-centric data, by adding insights from areas like finance, social media, and the environment.
- **Facilitating Dynamic Risk Modeling**: CDIs allow organizations to create systems that adjust quickly to new threats.
- **Enhancing Collaboration**: It encourages teamwork between disparate sectors, fostering a collective defense model.

For example, studies found that ransomware attacks use crypto for illegal transactions. They looked at financial data and social trends[18]. Hence, future frameworks can fix gaps and prepare for unknown cyber threats. That is the reason for this analysis. It should combine speculative threat intelligence and cross-domain indicators. The former is forward-looking. The latter is integrative.

IV. RESULTS

A. Summary of Reviewed Frameworks

The majority of the reviewed frameworks aimed to predict threats before they happened. They also focused on system resilience, collaboration across domains, and advanced security tech. They include models for CPS, IoT networks, blockchain, and cloud systems. These frameworks use machine learning, artificial intelligence, and automation. They help us detect and manage threats better.

B. Emerging Themes and Trends

➢ *Theme 1: The Growing Role of Artificial Intelligence and Machine Learning*

AI and ML are now key technologies in predictive cybersecurity. Our review found they are the basis of speculative intelligence. The works of Breve et al.[19] and Gajjar et al.[20] are examples of the notable advancements in this domain. Breve et al.[19] combined various AI methods to quickly identify and explain security risks. This approach makes it easy to spot vulnerabilities in fast-changing environments. Similarly, Gajjar et al.[20] focused on FPGA-accelerated ransomware detection. They showed that hardware-optimized ML models can quickly detect and respond to ransomware. The use of ML-enhanced security was furthered by Bridges et al.[21].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

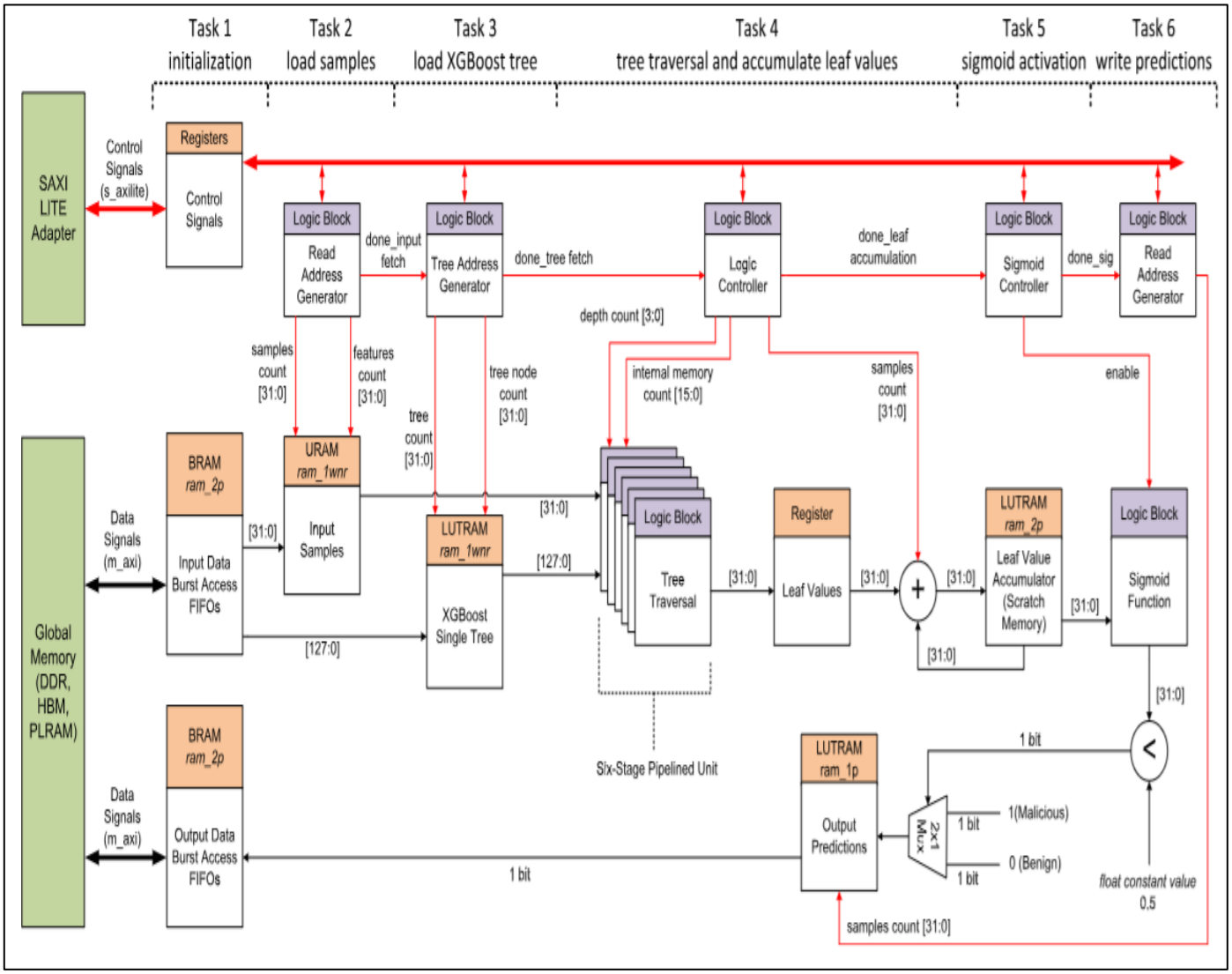

Fig 1: Experimental Evaluation of ML-based Malware Detectors[22]

Their experimental evaluation of ML-based malware detectors (Figure 1) showed the potential of such tools to reveal the presence of threats better than older, traditional systems. The FPGA-based system for XGBoost inference involved six key tasks. It started by initializing control signals via an AXI interface, then fetched input data from BRAM or URAM. XGBoost tree structures are loaded into LUTRAM. This is closely followed by tree traversal and accumulation of leaf values in a six-stage pipeline. A sigmoid function computes probabilities, and predictions (malicious or benign) are written back to memory based on a 0.5 threshold. The system maximizes efficiency through parallelization and specialized memory use. This prototype of Bridges et al.[21] improved predictions by using hardware performance counters, operating system calls, and network traffic together to reduce errors. It processed data faster than CPUs and GPUs, with lower delays. It is also more cost-effective and energy-efficient, saving up to 11 times the cost and using 643 times less energy compared to CPUs, and 3 times the cost and 16.8 times less energy compared to GPUs.

These works – Breve et al.[19], Gajjar et al.[20] and Bridges et al.[21] – showed a trend toward the growing use of AI at every stage of the cybersecurity lifecycle – from predicting the risk to stopping the threats in real-time.

Besides, the combination of different areas of expertise is another emerging trend in speculative intelligence. Samtani et al.[22] used dark web situational awareness to uncover hidden threats, showing the importance of data sources beyond regular IT systems. The dark web is a treasure trove of illegal transactions and sale of data obtained from hacking of several domains as shown in Figure 2 below. Table 1 further described how CTI can benefit from taking a deep dive into the wealth of information that the dark web has to offer. The table details various platforms and data sources that are essential to CTI, each providing unique insights. Together, these platforms enhance our understanding of cyber threats making it possible to pre-empt possible attacks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

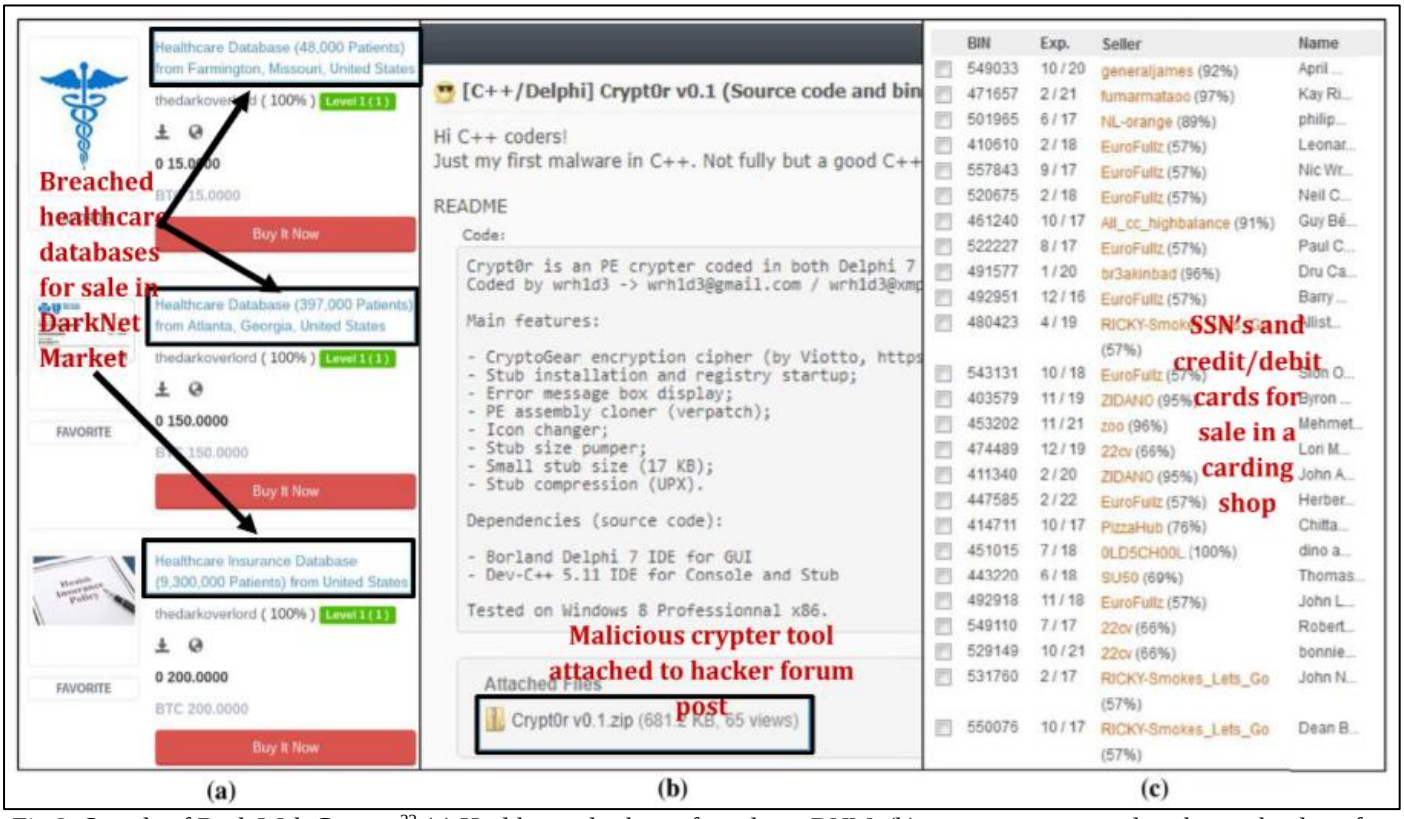

Fig 2: Sample of Dark Web Content[22] (a) Healthcare databases for sale on DNM; (b) a crypter source code, a key technology for ransomware shared on forums; (c) credit/debit cards and SSNs for sale in a carding shop.

Table 1: Overview and CTI Value of Dark Web Data Sources[22]

Platform	Data Sources	Description	Example Platforms	CTI Value
Hacker Forums	Leaked forums	Forums that have been leaked to the general public	Antichat, Blackhackerz, Blackhat World	-Discussions mentioning past and future attacks -Advertisements for hacking services (e.g., DDoS for hire) -Free hacking tutorials and exploits (e.g., SQLi, BlackPOS) -Identify key threat actors -Discover emerging hacking/threats
	Seized forums	Forums that have been shut down and seized by law enforcement	Darkode, shadowcrew, cardersmarket	
	Active forums	Active, accessible forums that have not been seized or are offline	OpenSC, Ashiyane, reverse4you, exelab	
Carding/Fullz Shops	Carding/Fullz shops	Shops selling stolen credit/debit cards and sensitive information (e.g., Social Security Numbers, drivers licenses, insurance cards)	cardershop, BESTVALID, rescatorccfullz, fullzshop	-Identify breached individuals and organizations -Discover trends of afflicted financial service industries
Internet-Relay-Chat	Active IRC Channels	Clear-text, instant messaging, communication that is not stored	Anonops, whyweprotest, anonet, opddosisis	-Preferred method of communication for hacktivist groups (e.g., Anonymous) -Since chats are not logged, hackers more freely share hacking knowledge and targets
DarkNet Markets	Grams	Search engine for identifying DNMs		-Identify markets to collect to generate CTI
	Active market website	Active marketplaces that have not been seized	Minerva, therealdeal, dream market	-Identify new, emerging exploits (0-days, ransomware) -Discover breached content (e.g., logins) -Early indicator for breached companies -Identify key sellers/buyers

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

This cross-domain intelligence is in line with the observations made by Bjurling and Raza[23], who suggested the use of analytic tradecraft to make CTI easier to understand and act upon. Similarly, the work of Albasir et al.[24] stands out for its focus on securing IoT and cyber-physical systems (CPS) through AI-enhanced methods, by combining traditional cybersecurity practices and new technologies. Banik et al.[25] also introduced adversary-in-the-loop defense planning, which included simulating adversaries to better predict and mitigate unknown threats.

We established earlier by the work of Samtani et al.[22] that advancements in cyber threats have necessitated the need for defense mechanisms to shift from reactive to proactive defense mechanisms. Happa et al.[26] studied the use of deception techniques, such as making network defenses unpredictable, to confuse attackers and delay their progress. This aligns with the work of Mundt and Baier[27], who similarly employed simulations to fight ransomware attacks. Both experiments show how speculative models can help in designing proactive defense strategies. Dubey et al.[28] also worked on protecting ML hardware against side-channel attacks, making AI-driven systems more resilient in tough situations. These studies demonstrate how proactive and deceptive approaches are becoming key parts of speculative intelligence frameworks.

Furthermore, Cyber-physical systems (CPS) have become a major focus for speculative intelligence due to their importance in modern infrastructure. Fu et al.[29] described methods for detecting anomalies and building resilient defenses in CPS to adapt to new threats (Figure 3). The method as illustrated in the diagram a secure control framework for a cyber-physical system (CPS). It employs an Anomaly Detector to monitor the CPS state and detect attacks. If an attack is detected, an Alarm triggers a Switching Strategy that dynamically transitions control between multiple controllers. Compromised controllers are isolated, normal controllers continue operation, and re-initialized controllers may replace attacked ones. This ensures continuous and secure system performance.

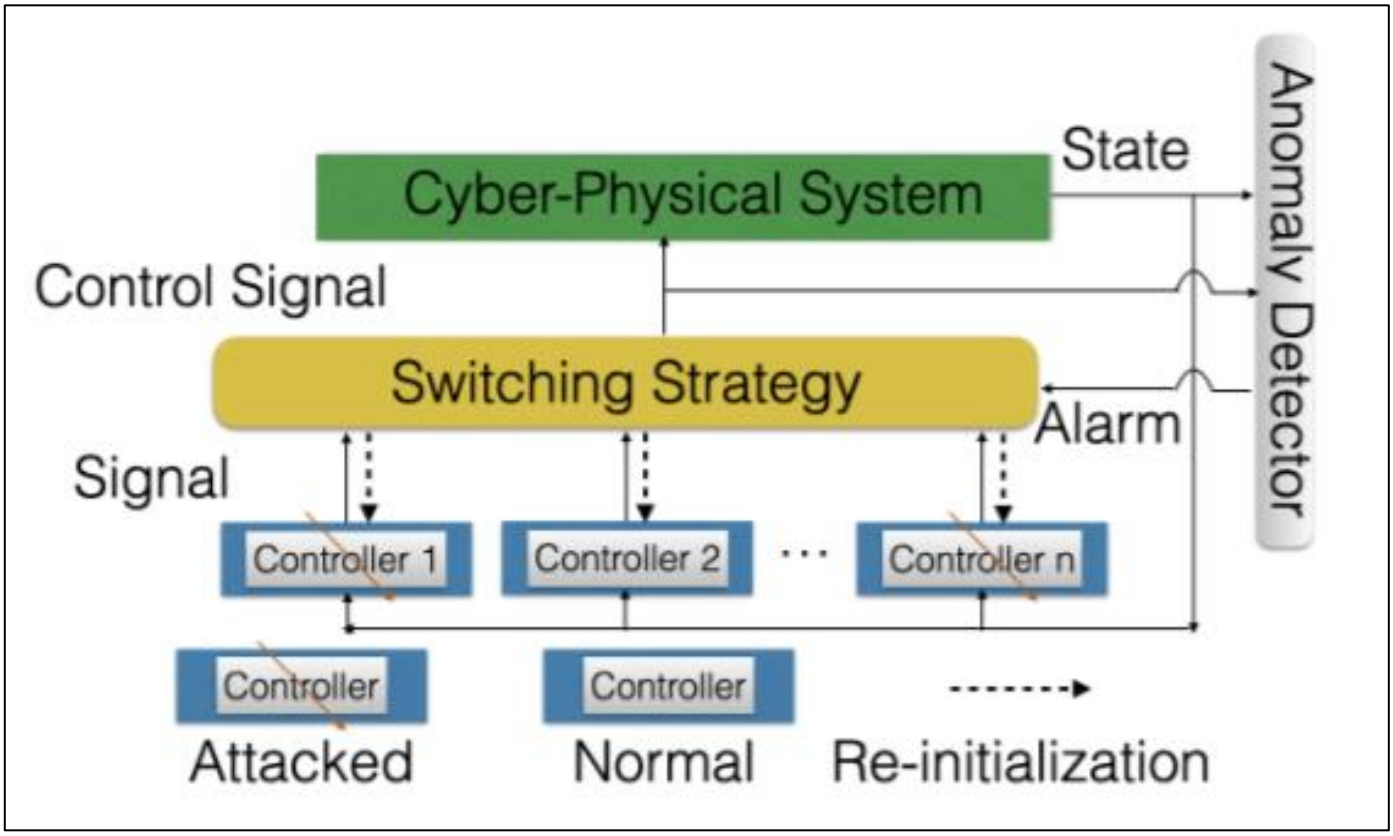

Fig 3: Re-Initialization, Anomaly Detection, and Switching Defense for the CPS Resiliency[29]

Similarly, Ou et al.[30] improved malware authorship verification using adversarial learning, helping to identify new attack methods that target CPS.

The combination of CPS security and adversary-centric testing is demonstrated by Staves et al.[31], who examined the utility of adversary-centric testing in IT/OT environments. These studies stress the trend toward predictive, adaptive, and experimental methodologies tailored to the unique vulnerabilities of CPS.

- *Emerging Trends in Speculative Intelligence*

✓ **Real-Time Adaptation in Speculative Intelligence:** One emerging trend in speculative intelligence is adapting in real-time to changing threats. Advances in FPGA-accelerated systems, as described by Gajjar et al.[20], is a worthy example of this shift. These systems capitalize on specialized hardware to detect ransomware as it begins infection. It shows that some technologies can handle urgent dangers. They do not rely on old threat models.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

This capability reflects a movement toward systems that not only predict but also adapt to threats as they unfold. This trend is complemented by adding anomaly detection to cyber-physical systems (CPS), as shown by Fu et al.[29]. Adaptive resilience mechanisms are vital. They must respond to unusual behaviors in networked systems. These systems help organizations to continuously update their defenses based on predictive analytics. This shows how flexible speculative intelligence can be.

- ✓ **Increasing Sophistication in Adversary-Centric Methodologies:** Adversary simulation and modeling are now part of speculative intelligence frameworks. The aim is to replicate the tactics, techniques, and procedures (TTPs) of potential attackers. Banik et al.[25] used adversary-in-the-loop methods. They show that simulating adversarial behavior in security systems can predict attack patterns. This method works well with the deception-based strategies by Happa et al.[26]. They introduced unpredictability to throw off attackers. Together, these approaches show a growing focus on understanding and predicting attacker behavior. This, in turn, informs complex and thorough defense strategies. Another notable development in adversary-centric methods is the use of adversarial machine learning, as seen in the work of Ou et al.[30]. This approach finds new malware and predicts how adversaries may adapt to bypass defenses. These studies show a trend. They seek to outpace attackers in cybersecurity by engaging with their evolving strategies.
- ✓ **Bridging Traditional and Non-Traditional Data Sources:** The incorporation of various data sources is another trend in improving threat detection. Traditional sources, like log files and network telemetry, are vital. But, non-traditional ones, like dark web monitoring, are gaining prominence. Samtani et al.[22] showed that dark web forums can provide insights. They can uncover hidden threats that traditional methods may miss. This mix of data sources is also backed by better analytic methods, as highlighted by Bjurling and Raza[23]. They stressed the need for actionable intelligence from integrated analytics. This reflects a demand for systems that combine data into clear threat models. This approach bridges the gap between technical cybersecurity methods and interdisciplinary insights.
- ✓ **Prioritizing Systemic Preparedness:** These studies share a theme. They focus on preparing systems as a whole, not on individual defenses. The work of Mundt and Baier[27] showed that simulation-based strategies for ransomware can model the effects of an attack. They help organizations understand its wide-ranging impacts. AI methods, such as those by Albasir et al.[24] highlight the need to blend speculative intelligence frameworks into systems. This is important for managing complex infrastructures, like IoT and CPS. This view includes proactive measures. For example, Bridges et al.[21] tested machine learning-based malware detection systems. The authors used these tools detect threats and forecast new ones. They ensure organizations can handle both current and future vulnerabilities.
- ✓ **Shifting Focus to Proactive, Automated Defense Mechanisms:** Automation continues to play a noteworthy role in speculative intelligence. The goal is to reduce human involvement in everyday security tasks. Breve et al.[19] showed that hybrid prompt learning can automate risk detection and handling. This saves time and resources in responding to threats. This reflects a shift in the industry. It is toward self-sustaining security systems. These systems use AI and machine learning to operate independently. They must also be very accurate. These automated defenses serve speculative intelligence. They let organizations focus on strategy, not operations. They also cut response times. This allows us to neutralize threats before they can fully materialize.

➢ *Theme 2: Cyber Risk and Threat Modelling*

As cyber threats evolve, proactive risk assessment is now vital to modern cybersecurity. In cyber-physical systems (CPS), Amro et al.[32] showed the ATT&CK Framework can help find and assess vulnerabilities. This study stressed the need to evaluate risk pathways. It aimed to use threat intelligence to predict attack vectors before they are exploited. Their method showed the value of scenario-based modelling. It also proved that proactive risk assessment can improve CPS security.

Similarly, Axon et al.[33] Their study used a predator-prey analogy. It assessed the effects of ransomware incidents across interconnected systems. They also found that systemic vulnerabilities often worsen ransomware attacks. They create ripple effects that weaken the entire organization's network. Systemic risk modelling. shows the links in modern cyber threats. Recent research has also aimed to create full response frameworks for ransomware attacks. Bajpai and Enbody[34] took this a step further with their proposed framework for ransomware response strategies (Figure 4).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

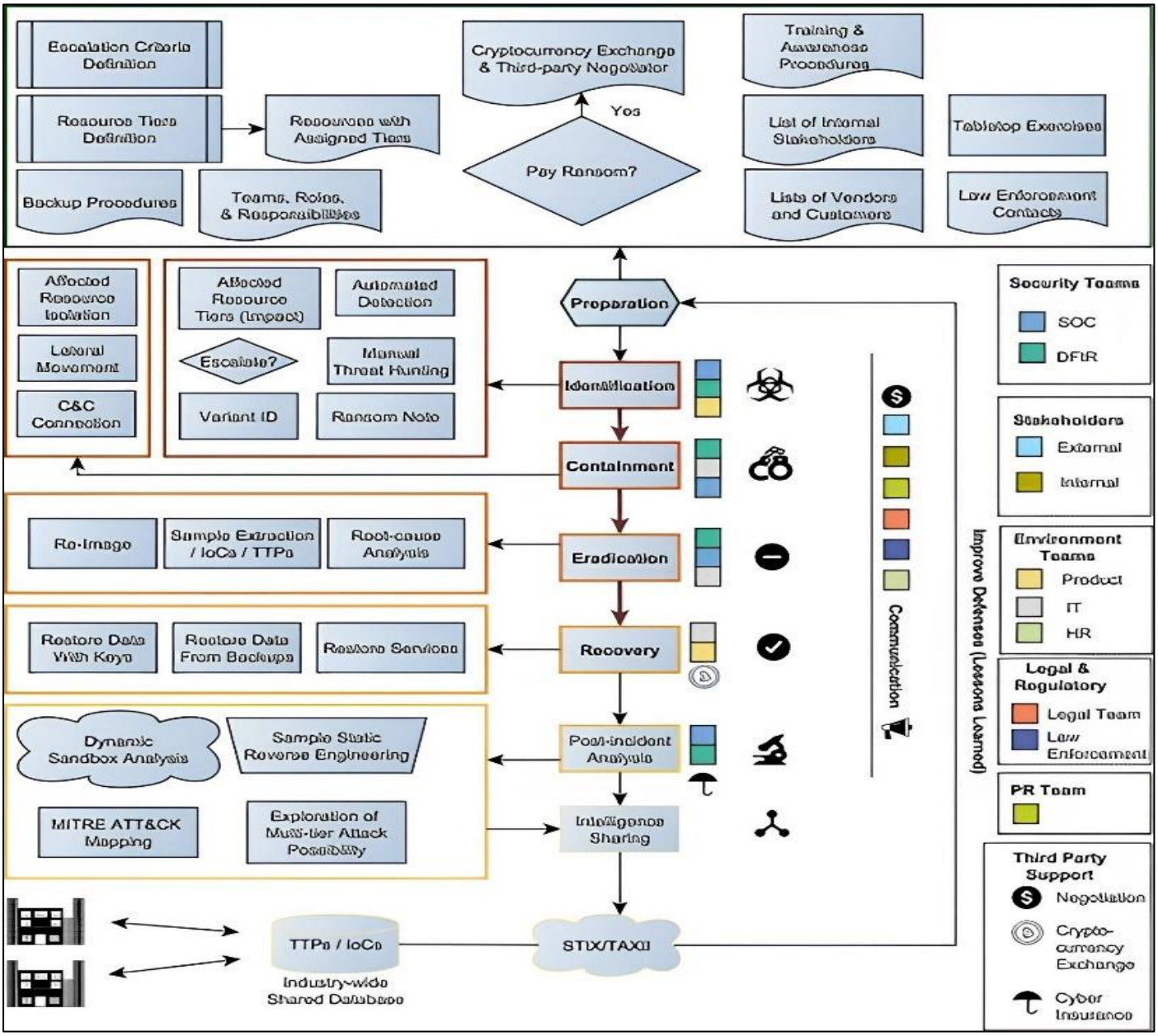

Fig 4: Bajpai and Enbody[34] proposed framework for Ransomware Response Strategies

Their study used predictive analytics and organizational readiness. It built a response model to reduce the impact of ransomware attacks, both short- and long-term. The framework emphasized combining technical, procedural, and human factors in the response strategy. They demonstrated that an effective ransomware defense requires a multifaceted approach. The framework's focus on preparedness reflects a trend in threat modelling. Organizations must prepare for unknown or emerging threats, not just respond to cyber incidents. This matches the speculative intelligence principles in earlier studies. They prioritize foresight and anticipation over traditional, reactive defenses.

Likewise, Csikor et al.[35] highlighted the growing importance of attack analysis in CPS security. The researchers explored replay attacks on automotive CPS. They found critical vulnerabilities that can compromise vehicle safety and functionality. Their experiments showed that replayed signals could disrupt key tasks in autonomous and semi-autonomous vehicles. Their findings showed a need for strong authentication and anomaly detection systems to prevent such attacks. This focus on attack analysis reflects a trend in CPS security. It is vital to know the tactics and techniques of adversaries. This knowledge is key to developing proactive defenses.

Still, the complexity of CPS demands adaptive and resilient defense mechanisms capable of handling dynamic threats. Maruf et al.[36] met this need with their timing-based framework. This framework combined predictive threat detection and resilience strategies. Their research aimed to find time anomalies in CPS operations that could signal cyber intrusions (Figure 5).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

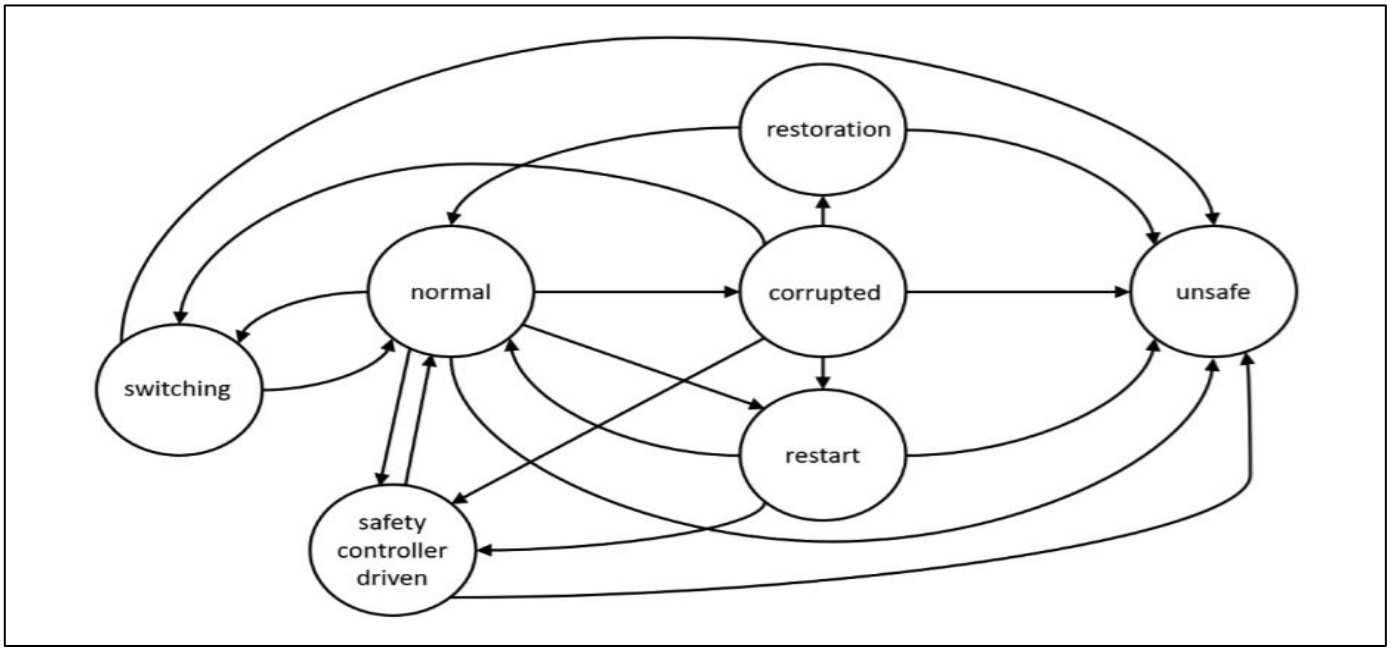

Fig 5: This Figure Presents the Hybrid System Model, H, with Statuses Shown as Circles and Transitions Represented by Arrows. It Shows How Resilient Architectures Evolved Cyber Statuses in CPS.

Maruf et al.[36] framework used predictive analytics and real-time monitoring. It let CPS stay functional, even under attack. A key contribution of this study is its emphasis on resilience as a core component of CPS security. Unlike traditional methods that defend the perimeter, this framework shifts focus. It aims to ensure system performance amid ongoing threats. This trend shows that keeping operations stable is as important as preventing breaches. Downtime can lead to serious problems. Rosso et al.[37] contributed by introducing SAIBERSOC. It's a tool for experimenting with Security Operations Centers in CPS environments (Figure 6). SAIBERSOC lets researchers and security teams test defenses. It simulates various attack scenarios in a controlled setting.

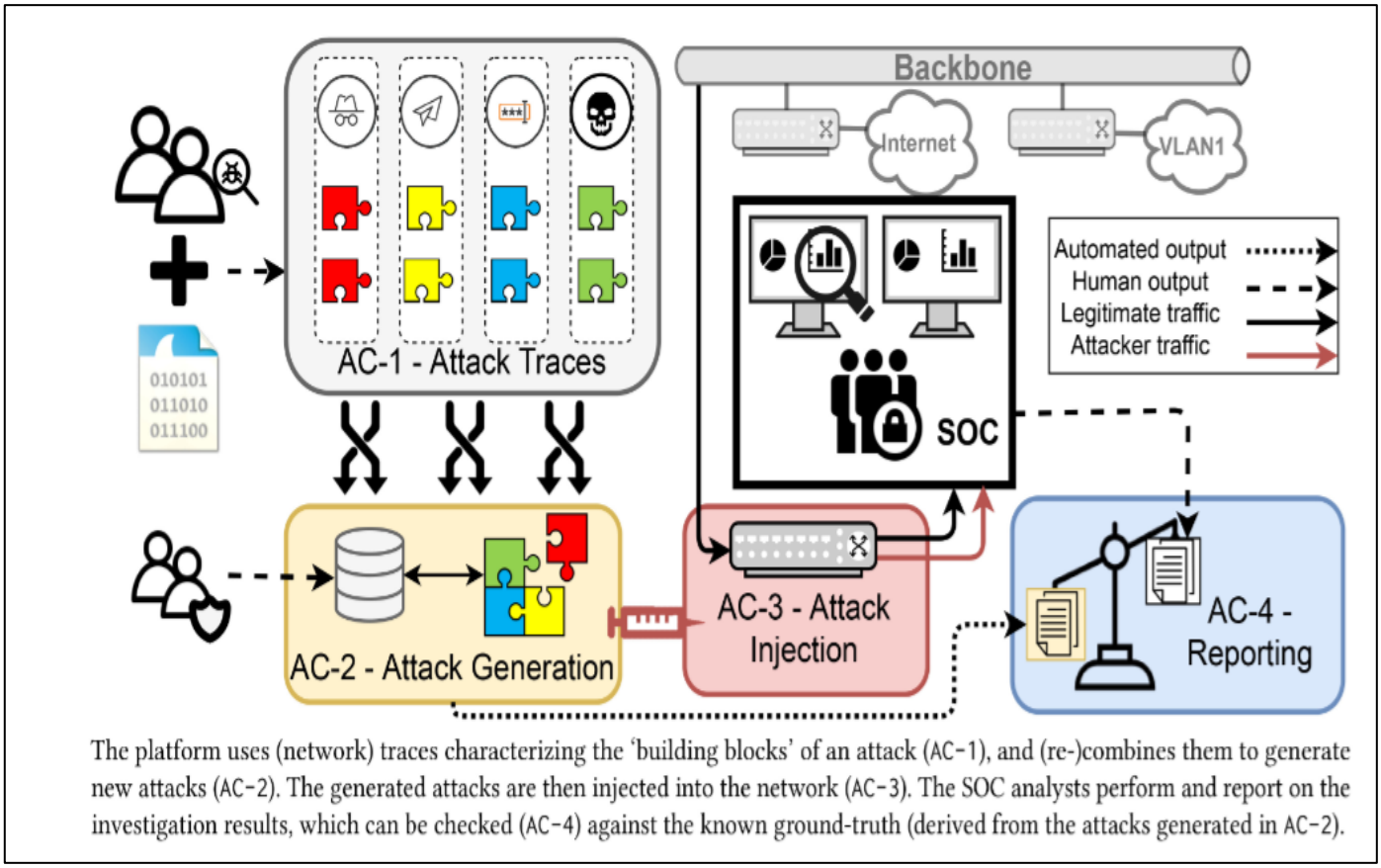

Fig 6: Proposed SAIBERSOC Tool by Rosso et al.[37]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

This tool deepens our understanding of CPS weaknesses. It also tests new defense strategies. The emphasis on SOC experimentation represents a significant trend in CPS security research. As cyber threats grow more complex, we must simulate real-world scenarios. This is crucial for training, analysis, and developing adaptive defenses. SAIBERSOC's app shows the need for tools that connect theory with practice.

A common theme is the growing reliance on threat intelligence. It aims to improve risk assessments and response strategies. Both Amro et al.[32] and Axon et al.[33] showed that adding actionable intelligence to risk modelling. can improve defense mechanisms. They become more accurate and adaptive. These studies stress the need for data-driven decisions in cybersecurity. The use of ATT&CK Framework to map CPS vulnerabilities and systemic risk modelling. to gauge ransomware's impact is indeed groundbreaking.

The systemic approach delineated by Axon et al.[33] was also about risk modelling. The researchers emphasized the interconnected nature of today's digital environments. They showed that a single point of failure can ripple through an organization or industry. This insight is valuable for building stronger, more adaptive cybersecurity frameworks.

Taken together, these studies point to the shift in CPS security toward proactive and resilient frameworks. The research highlights the need for adaptability in CPS. It shows this by examining specific attacks, like replay attacks, and developing timing-based and experimental methods. It also stresses the need for real-time monitoring. Also, the focus on experiments and simulations tests theories. This paves the way for practical applications.

- *Theme 3: Cross-Domain Indicators and Intelligence Integration*

The growing complexity of cyber threats has led to the need for unified taxonomies to organize and share threat intelligence. The study by Martins and Medeiros[38] exemplifies this trend. It proposed an OSINT-based framework that integrates a unified taxonomy for cyber threat intelligence. This approach makes data collection, categorization, and sharing uniform. It helps various cybersecurity tools work together more easily. The researchers showed that taxonomies improve the speed and accuracy of finding cross-domain threats in big, unstructured data. This focus on standardization showed that we must reduce redundancy and promote collaboration across cybersecurity teams and platforms. Aligning diverse datasets under a common framework can help organizations. It can reduce redundancy, improve collaboration, and build a stronger intelligence network to address evolving threats

Similarly, automating the sharing and analysis of threat intelligence is now a key focus in cybersecurity. Husák et al.[39] explored this through their work on automating the sharing of intrusion detection alerts. The researchers stressed the need for real-time data exchange. It can prevent attacks from spreading across interconnected systems. Their study introduced methods to automate alert dissemination. It kept data private and complied with the law. The outcomes of this research align with the growing reliance on automation in cybersecurity. Automated systems cut human input, speed up responses, and make intelligence actionable. This shift reflects a trend toward building agile defense systems capable of operating at the speed of modern cyber threats.

As smart cities grow, we must integrate cross-domain intelligence. It is key to managing the unique cybersecurity challenges of interconnected urban systems. Jarvis et al.[40] examined vulnerability intelligence in smart cities. They used data from transportation, utilities, and public safety to find risks. Their findings stressed the need to tailor threat intelligence for urban infrastructures. Their study found that cybersecurity frameworks must be both cross-domain and adaptable to specific sectors. This is essential. As smart cities become more complex, combining intelligence from various sources is critical. It ensures security and resilience.

Another trend in cross-domain intelligence is extracting insights from large datasets. Rani et al.[41] tackled this issue. They developed methods to extract actionable threat intelligence from cyber threat reports. Their approach aims to find tactics, techniques, and procedures (TTPs). It will then make actionable recommendations for organizations. Our study used NLP and machine learning. It showed that we can turn complex threat reports into user-friendly intelligence. This work aligns with the trend of prioritizing actionable insights over raw data. Organizations need tools to turn complex information into practical strategies. These strategies should enable proactive responses to emerging threats. These events highlight the need to blend tech innovation with usability in threat intelligence.

- *Theme 4: User-Centric and Niche Applications*

User authentication is key to cybersecurity. When flawed, attackers can invade indiscriminately. Maceiras et al.[42] study reveals a threat: account enumeration attacks. These exploit flaws in authentication to infer sensitive user info. The researchers used an empirical analysis. It showed that poor masking of error messages, or timing differences in login attempts, can compromise authentication protocols. This study highlights a key theme in user-centric cybersecurity. It is vital to have strong defenses that prioritize privacy and usability, without sacrificing security. It showed the need for strong authentication systems. They must resist inference attacks. The researchers suggested using error generalization and random response timing to reduce these risks. Their work shows a trend to balance security and user experience. This is to ensure that protective measures don't add complexity or hinder usability.

Also, blockchain technology has a decentralized structure and immutable ledgers. It is now vital for securing financial and transactional systems. However, cyber threats targeting blockchain environments have also become more advanced and sophisticated. Rabieinejad et al.[43] looked at generative adversarial networks (GANs) for threat hunting in Ethereum blockchains. They proposed a new way to find and fix anomalies (Figure 7).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

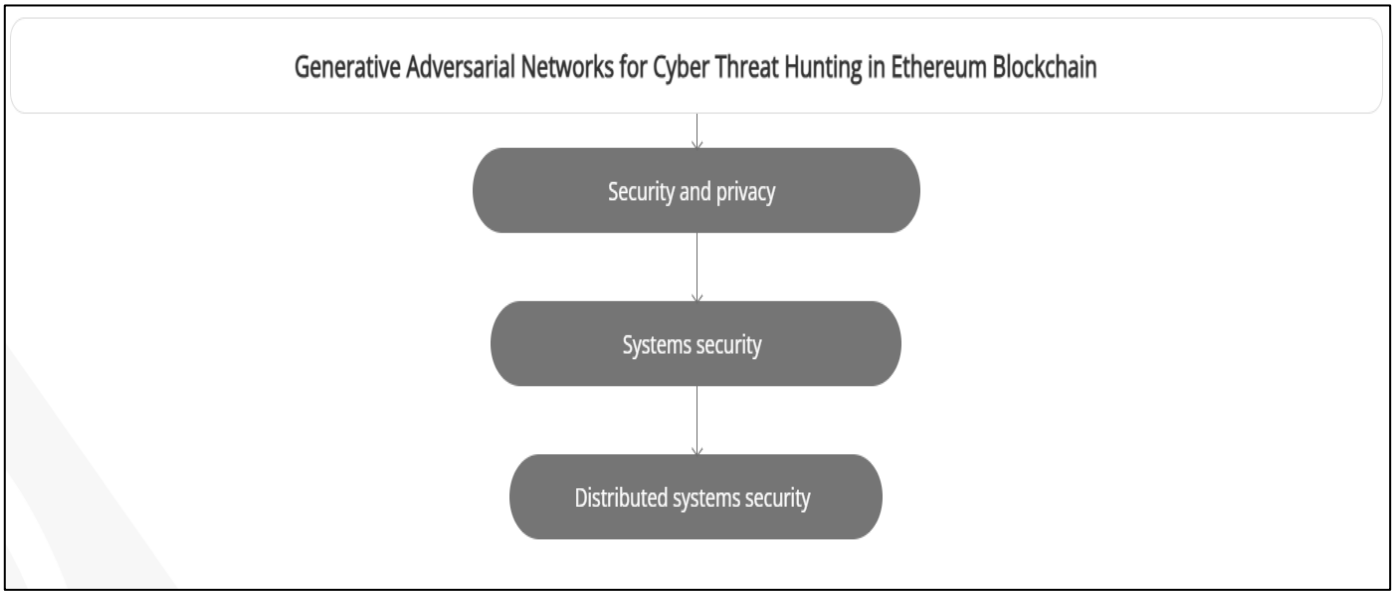

Fig 7: GANs for Threat Hunting in Ethereum Blockchain Environments[43]

GANs simulated potential attack scenarios. This helped find vulnerabilities in blockchain operations and smart contracts. Their research shows the niche but vital role of AI in blockchain security. Rabieinejad et al.[43] trained GANs to anticipate attacker behavior and exploit patterns. They showed that proactive modelling. can improve blockchain defenses. This approach aligns with the broader trend of using advanced machine-learning techniques to protect domain-specific applications. It also emphasizes the importance of integrating cutting-edge technologies into traditionally static security models to address emerging challenges.

Thus, both studies show us the growing trend in cybersecurity research: the targeted focus on specific vulnerabilities and environments to create specialized solutions. While Maceiras et al.[42] addressed a common concern in user-focused cybersecurity—authentication vulnerabilities—Rabieinejad et al.[43] focused on the highly specialized field of blockchain security. Both separate studies illustrate the importance of tailoring security measures to the unique characteristics of specific systems and use cases.

The common thread in these studies is a proactive identification and mitigation of risks. Whether addressing inference attacks in user authentication or simulating blockchain threats with GANs, these works show a move from reacting to problems to anticipating cybersecurity practices. This proactive approach not only strengthens defenses but also reduces potential disruptions by stopping attacks before they occur.

➢ *Theme 5: Advanced Threat Intelligence Frameworks*

We have established earlier that the growing complexity of cyber-physical systems (CPS) calls for smarter ways to detect threats. Hong et al.[44] addressed this challenge by developing advanced modelling. techniques tailored for multimodal CPS environments (Figure 8). Their approach combined hybrid models capable of analyzing data from sources ranging from sensor readings to network traffic logs, to detect unusual activity.

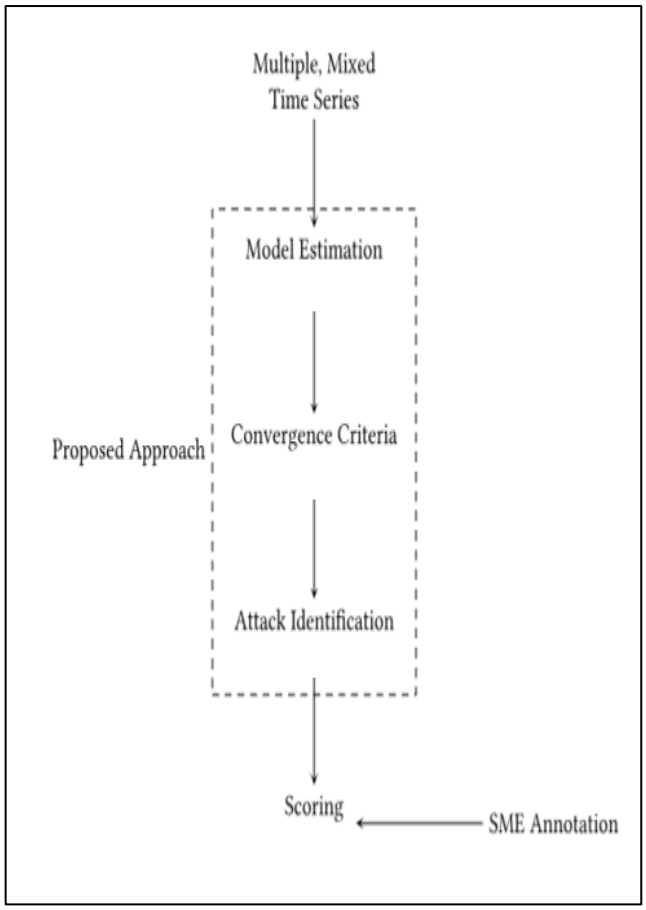

Fig 8: The Machine Learning Approach of Hong et al.[44]

This work addressed challenges in analyzing cyber-physical system logs with limited information and complex attack methods using a sticky Hierarchical Dirichlet Process Hidden Markov Model (sHDP-HMM). The researchers demonstrated its efficacy in attack detection on an avionics testbed and a consumer robot while comparing inference methods and accuracy metrics. They showed the importance of integrating temporal and spatial analysis to identify patterns indicative of cyberattacks. This work is another

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

indication of the growing trend in advanced threat intelligence frameworks: the shift toward holistic, multimodal systems capable of synthesizing data from various sources. The implication is that researchers and practitioners can address the vulnerabilities of CPS while reducing the risk of false alarms by adopting a unified approach.

Building on the theme of CPS security, López-Morales[45] proposed advanced threat intelligence methods. Their study introduced a detailed framework that combined real-time monitoring with predictive analytics to enhance situational awareness. A key feature of this research was its emphasis on adaptive defenses, which continuously adjust to evolving threat landscapes. The researchers did this by developing an Industrial Control System (ICS) threat taxonomy for Cyber Threat Intelligence (CTI) processing, a satellite honeypot for Cyber Threat Intelligence collection, and a Connected and Autonomous Vehicle (CAV) sandbox for simulating attacks and collecting Cyber Threat Intelligence. The findings from their research point to a growing reliance on dynamic threat intelligence in securing CPS. When potential vulnerabilities are proactively identified, it will be easier to adapt defenses accordingly. López-Morales' work shows the importance of blending real-time threat monitoring with forward-looking intelligence to create resilient systems capable of withstanding both current and emerging threats.

The application of automation and machine learning continues to transform the field of threat intelligence. Tunde-Onadele et al.[46] explored this by developing a self-supervised machine-learning framework for detecting attacks in containerized environments (Figure 9). Their study showed how containerization—a technology in modern cloud and software development—introduces unique security challenges.

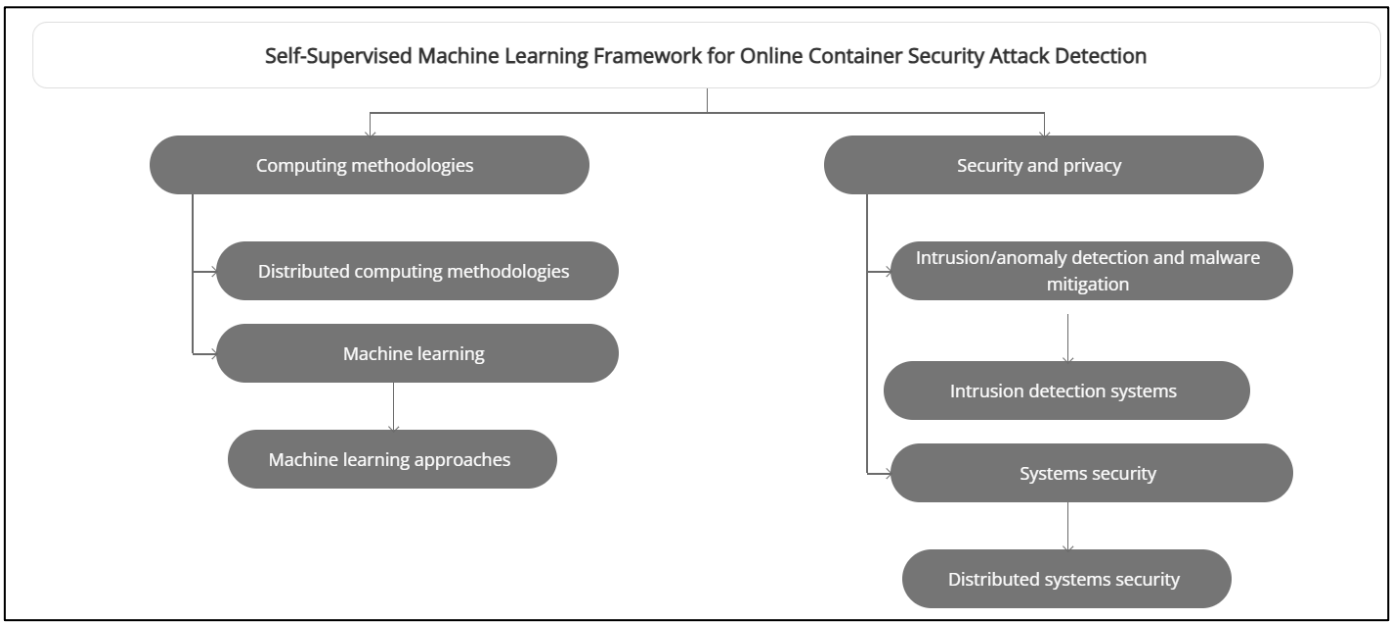

Fig 9: Self-supervised Machine Learning Framework by Tunde-Onadele et al.[46]

This study introduced a self-supervised hybrid learning (SHIL) framework for efficient online attack detection in containerized systems. It combined supervised and unsupervised learning without requiring manual data labeling and demonstrated a significant reduction in false alarms (33%-93%) with high detection accuracy across real-world attacks. These systems can adapt to new attack vectors more efficiently by reducing reliance on manual data labeling. The work of Tunde-Onadele et al.[46] shows that machine learning can solve complex, domain-specific problems. The way is thus paved for applications across diverse environments.

➢ *Theme 6: Other Relevant Emerging Technologies*

Apart from the articles that are closely related to Speculative Threat Intelligence, other emerging technologies are relevant to proactively combat cyber threats. They are:

- *Automation for Cloud-Based Security Assessments*

Cloud platforms like Amazon Web Services (AWS) are vital for modern businesses. However, their complexity creates unique security challenges. Engström et al.[47] focused on automated security assessments for AWS. They stressed the need for tools to evaluate configs, find vulnerabilities, and provide solutions, all without manual effort. Their findings showed that automated tools are effective. They improve response times. They are essential in environments where scalability is critical. As more firms adopt cloud services, automating security tasks helps. It maintains consistency and reduces human error. This will in turn enable organizations to better manage the growing complexity of their environments.

- *Hardware Security Through Obfuscation Techniques*

Hardware intellectual property (IP) security remains a major concern in high-value technology ecosystems. Rahman et al.[48] studied obfuscation techniques to protect hardware IP. They focused on methods that hide design logic to deter reverse engineering and tampering. Their findings showed that obfuscation could defend against advanced side-channel attacks. Though traditionally overlooked, hardware security is gaining traction. Adversaries are exploiting low-level

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

vulnerabilities. Obfuscation techniques show a shift to more proactive measures in protecting physical infrastructure.

- *Bridging Cyber-Risk Management in IT/OT Systems*

The merging of operational technology (OT) and information technology (IT) is creating a combined environment. It poses unique cybersecurity challenges. Pal et al.[49] tackled this by creating a cyber-risk management framework for IT/OT integration. Their approach identified key risks. It assessed their impact on interconnected systems. Then, it provided strategies to reduce these risks. The outcomes of this study emphasize the importance of adopting a holistic view of risk management. As IT and OT systems connect more, it's important to understand their links and possible weaknesses. This knowledge helps build strong and secure infrastructures.

- *Enhancing Resilience in Distributed Control Systems*

Distributed control systems (DCS) manage complex industrial processes. But, their reliance on networks makes them vulnerable to cyberattacks. Zhao et al.[50] proposed a framework for improving the resilience of DCS through multi-agent learning techniques. Their framework used adaptive, cooperative learning. It let systems detect and respond to anomalies while staying efficient. This work supports a trend of building resilience into industrial systems. It ensures they can withstand disruptions from cyber and physical threats. It also stresses the need to add machine learning to traditional control systems to boost their defenses.

- *The Evolution of IoT Security Architectures*

The Internet of Things (IoT) presents unique challenges due to its large scale and diverse devices. Ameer et al.[51] proposed a Zero-Trust architecture for IoT systems. It stresses continuous verification and strict access control to prevent breaches. Their framework showed that a trustless model could reduce the attack surface. It would also ensure secure device interactions. This study is part of research on Zero-Trust principles in cybersecurity. In it, trust is not granted by default. It must be continuously verified. These principles are key for IoT environments. The many connected devices raise the risk of lateral movement attacks.

- *Identifying Capability Gaps in IoT Cybersecurity*

Industrial IoT (IIoT) systems are vital to manufacturing and supply chains. But, their security often lags behind tech advances. Axon et al.[52] found gaps in IIoT cybersecurity. This is especially true for device authentication, data integrity, and threat detection. Their study proposed a roadmap to fix these issues. It aimed to improve the security of IIoT systems. This work highlights a problem with new technologies: there is a gap between their rapid adoption and robust security measures. Thus, we need both technical innovation and industry-wide collaboration to fix these gaps. We must establish best practices.

- *Language Models for Cybersecurity*

As cybersecurity data grows, it becomes more complex. So, NLP tools are being designed to improve data analysis and threat detection. Bayer et al.[53] introduced CySecBERT, a language model tailored for cybersecurity. The researchers proved its effectiveness by fine-tuning the model on domain-specific data. It can analyze cyber threat intelligence reports and find patterns. They showed that, by reducing analysts' cognitive load, such tools can speed up finding actionable insights in large datasets.

- *Domain-Specific Approaches to IoT Threat Mitigation*

Spoofing attacks continue to be a significant challenge in IoT environments. Madani et al.[54] explored random moving-target methods to detect and prevent MAC-layer spoofing. Their method used dynamic configurations to thwart attackers. It made it harder to exploit fixed vulnerabilities. Hence, researchers can develop more effective defenses against evolving threats by tailoring solutions to the unique characteristics of IoT systems. This research shows the importance of domain-specific solutions in addressing IoT security challenges.

C. Case Studies

➢ *Highlighting Examples of Frameworks in Action*

- **Multimodal Cyber-Physical Systems Threat Detection Frameworks:** The work of Hong et al.[44] showed how advanced modelling. techniques can help to detect attacks in multimodal CPS. This framework combines temporal and spatial data analysis to identify anomalies in CPS components. For instance, in a smart grid environment, the system detected irregularities in both network traffic and sensor data. This demonstrates its ability to address complex, multi-layered threats. This case study illustrates the importance of using a holistic approach in environments. Such environments enable related components to serve as targets and entry points for cyber threats if neglected.
- **Real-Time Resilience in Containerized Environments:** Tunde-Onadele et al.[46] explored self-supervised machine learning frameworks to detect attacks in enclosed environments. Examples are those used in cloud-based software deployments. This framework detected container-specific anomalies, with no need for extensive labeled datasets. Such container-specific anomalies include privilege escalation attempts. In practice, such an approach was used in a healthcare cloud infrastructure. It successfully detected and mitigated unauthorized attempts to access patient records. This case study is an example of the adaptability of self-supervised learning to evolving threats.
- **SAIBERSOC for SOC Experimentation:** Rosso et al.[37] introduced SAIBERSOC, a tool for SOC experimentation in CPS environments. This framework was tested in a simulated water treatment facility. It replicated various attack scenarios, including ransomware and insider threats. The experiments showed how cross-domain integration can improve the efficiency of threat detection and response. SAIBERSOC enabled security teams to refine their defense strategies and assess system vulnerabilities under real-world conditions. It provided a controlled environment for such testing to be done.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

➢ *Comparative Insights from Different Domains*

- **Finance:** The study by Engström et al.[47] focused on automated security assessments in AWS environments. This framework is particularly relevant to the financial sector. Cloud platforms are used in banking and fintech for their scalability and operational efficiency. However, these platforms are also high-value targets for cyberattacks. The framework highlighted vulnerabilities in mis-configured access controls and unpatched software. It shows automation is crucial for ensuring compliance and safeguarding sensitive financial data.
- **Healthcare:** The Zero-Trust architecture proposed by Ameer et al.[51] was tested in a healthcare system. It was tested in an IoT-based patient monitoring system. This architecture minimized the attack surface by continuously verifying device identities and enforcing strict access controls. Similarly, the work of Maruf et al.[36] on timing-based resilience frameworks were applied to a hospital's CPS. It ensured uninterrupted operation despite ongoing attack attempts in smart infusion pumps.
- **Critical Infrastructure:** For critical infrastructure, systemic risk modelling. and resilience frameworks are pivotal. Axon et al.[33] applied systemic risk modelling. to a power grid. The model used a predator-prey analogy to predict the cascading effects of ransomware attacks on interconnected systems. Similarly, Zhao et al.[50] developed a multi-agent learning framework for distributed control systems (DCS). This improved their resilience against anomalies.

In summary, these frameworks show into how disruptions in one component could affect the entire network. This emphasizes the importance of systemic preparedness in critical sectors.

➢ *Summary of Comparative Insights*

The frameworks reviewed from Themes 1 to 6 highlight the following comparative insights:

- **Cross-Domain Applicability**: While tailored for specific domains, many frameworks share common principles. This includes real-time monitoring, adaptive responses, and predictive analytics. For example, Zero-Trust principles from IoT in healthcare could be adapted for smart financial systems.
- **Emphasis on Automation**: Automated tools are increasingly reducing the need for human involvement in threat detection.
- **Resilience Through Adaptation**: Frameworks for multimodal CPS and DCS prioritize maintaining operational stability during attacks. This is a priority in critical and interconnected domains.
- **Simulated Testing for Preparedness**: Platforms like SAIBERSOC enable organizations to enhance their strategies and simulate real-world scenarios. This points to the benefits of proactive defense planning.

These case studies and comparisons show the evolving nature of cybersecurity frameworks. This emphasizes the need for adaptability, automation, and cross-domain learning. Each framework helps to build resilient, proactive defenses against a dynamic threat landscape.

V. DISCUSSION

A. Analysis of Findings

➢ *Strengths and Weaknesses of Existing Frameworks*

- *Strengths*

Existing cybersecurity frameworks provide structured ways for identifying and addressing threats. They use advanced technologies like artificial intelligence, machine learning, and automation. For example, frameworks like Zero-Trust in IoT systems focus on strict access control. It ensures that no device is trusted without continuous verification. Such frameworks are good at preventing unauthorized access and controlling data flow.

The integration of predictive analytics is another strength. Predictive tools in frameworks for CPS can analyze patterns to detect anomalies before they cause damage. Models used for multimodal CPS threat detection combine data from sensors and networks. They do that to provide better situational awareness. This makes it easier to identify attacks early.

Automation is also a major strength. Tools that automate tasks, like the AWS security assessment frameworks, reduce the time required for manual work. They can identify misconfiguration and vulnerabilities more consistently than human administrators. Additionally, self-supervised learning models reduce the need for labeled data. They are useful in dynamic environments like containerized systems.

Finally, frameworks like SAIBERSOC, which support experimentation help organizations simulate real-world attacks. These simulations allow teams to test their defenses and improve them without risking actual harm to their systems. These tools make frameworks more adaptable to threats by providing controlled testing environments.

- *Weaknesses*

While existing frameworks have strengths, they also have weaknesses. One major weakness is their reliance on specialized knowledge. Many frameworks need skilled professionals to operate them effectively. For example, setting up and managing a Zero-Trust architecture can be complex in large networks with many devices. Smaller organizations may not have the resources to hire such experts.

Another weakness is the high cost of implementation. Advanced frameworks often need investment in hardware, software, and training. This makes them harder to adopt for organizations with limited budgets.

Some frameworks also struggle with false positives. For example, multimodal CPS models can sometimes flag normal activities as suspicious. This creates extra work for analysts and can reduce trust in the system.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

Additionally, frameworks that rely on ML models may become outdated if they are not regularly updated with new data. This is because attackers are always finding new methods to attack and static models can fail to detect novel threats. In domains, like IoT and blockchain, rapid advancements often outpace the ability of existing frameworks to adapt.

➢ *Barriers to Implementation and Adoption*

- **Complexity of Deployment:** Many frameworks are difficult to deploy due to their complexity. Integrating cross-domain threat intelligence involves collecting and standardizing data from various sources. Hence, organizations may face technical challenges in ensuring that their systems can process and use this data. Also, these frameworks require coordination between different teams. This can be hard to achieve in large organizations.
- **Lack of Skilled Professionals:** A shortage of skilled cybersecurity experts is another shortfall. Advanced tools like GAN-based threat hunting in blockchain need trained operators. Without proper knowledge, these tools may not be used to their full potential, limiting their effectiveness.
- **High Costs:** Implementing these frameworks can be financially challenging, particularly for smaller organizations. Hardware-focused frameworks, such as those relying on FPGA technology, need expensive equipment. Similarly, frameworks requiring real-time monitoring and advanced analytics may require high-performance computing resources. This increases costs.
- **Organizational Resistance:** Resistance to change is another challenge. Organizations may be reluctant to adopt new frameworks if they feel that their existing systems are sufficient. There may also be concerns as to how new frameworks will fit into existing workflows or whether they will disrupt normal operations. For example, Zero-Trust models require major changes to how devices and users access networks, which can slow down adoption.
- **Legal and Compliance Issues:** Some frameworks are constrained by legal and regulatory challenges. For example, automated systems that share intrusion alerts must comply with data privacy laws. This can make organizations restrain from sharing sensitive information. Even with good intentions, they are restrained by fears of fines or reputational harm.
- **Scalability Issues:** Scalability poses a challenge for frameworks that excel in small-scale tests but falter in larger, real-world networks. For example, experimental frameworks like SAIBERSOC may be effective in simulated environments. However, it could require major adjustments to handle the complexity of real-world systems. Similarly, IoT frameworks can face challenges in managing the vast number of devices found in modern IoT networks.

Hence, while existing frameworks offer many strengths, they also face limitations. Their adoption is limited by technical, financial, and organizational barriers. Organizations can address this by streamlining deployment, enhancing accessibility, and ensuring frameworks evolve with emerging threats. These steps can help make cybersecurity frameworks more practical and effective for organizations.

B. Implications for Practice and Policy

➢ *Recommendations for Improving Speculative Threat Intelligence Frameworks*

- Simplify Framework Deployment: Many speculative threat intelligence frameworks are complicated and hard to implement. Simplifying these frameworks can make them more accessible to smaller organizations. User-friendly interfaces and clear documentation are useful for tools like Zero-Trust architecture and AWS security assessments. This can help reduce the time and expertise needed for implementation. Organizations can also benefit from pre-configured solutions that require minimal customization.
- Invest in Automation: Automation is important for improving the efficiency of threat intelligence frameworks. Automated tools can help process large amounts of data and detect threats faster than humans. Frameworks that use machine learning models should include automation to handle repetitive tasks. Automating data collection, threat analysis, and reporting allows security teams to concentrate on decision-making and planning. Automation plays a key role in making threat intelligence frameworks more efficient.
- Focus on Scalability: Frameworks need to work well across different scales, from small businesses to large enterprises. For example, IoT security frameworks should handle networks with thousands of devices as easily as they handle small ones. Researchers and developers should test frameworks in diverse real-world environments to ensure scalability. Cloud-based solutions can help with this with no need for expensive hardware.
- Address False Positives: Frameworks should prioritize minimizing false positives. False positives can waste time and reduce trust in the system. Improving the accuracy of machine learning models is one way to address this issue. For example, CySecBERT can analyze cybersecurity data to differentiate normal and suspicious behavior. Regularly updating models with new data can also help reduce errors.
- Enhance Adaptability: Threat intelligence frameworks need to adapt to new and evolving threats. This is especially important because attackers are always developing new techniques. Frameworks like the timing-based resilience for CPS should be updated consistently. This will help the system to stay effective. Using AI and ML can help frameworks learn from past attacks and adjust their defenses automatically.

➢ *Suggestions for Cross-Domain Collaborations*

- **Share Data and Insights:** Cross-domain collaborations can help organizations share data and insights about emerging threats. Cybersecurity teams in the finance and healthcare sectors can collaborate to identify common attack patterns. Sharing information can help

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

organizations learn from each other and improve their defenses. Platforms like SAIBERSOC already provide a shared environment. This could be expanded to allow multiple sectors to test and improve their strategies in a

- **Develop Common Standards:** Collaborations among sectors should aim to establish common standards for threat intelligence. Martins & Medeiros[38]suggested using a unified taxonomy. This can help standardize how data is collected, analyzed, and shared. Common standards make it easier for organizations to integrate and compare their data. Thus, it will improve the overall effectiveness of threat intelligence frameworks.
- **Partner with Academic Institutions:** Collaborating with universities and research institutions can help industries access the latest knowledge and technologies. Academic researchers often develop new frameworks that can benefit multiple sectors. Partnerships can also create opportunities for testing frameworks in real-world scenarios. This improves their practical value.
- **Engage Policy Makers:** Governments and regulators should be part of cross-domain collaborations. They can help create policies that support cybersecurity efforts. Such policies can encourage information sharing while protecting sensitive data through privacy regulations. Policymakers can also ensure that frameworks comply with legal requirements. This in turn makes it easier for organizations to adopt them.
- **Encourage Public-Private Partnerships:** Public and private organizations can work together to develop and deploy threat intelligence frameworks. Governments can provide funding or resources to support the adoption of frameworks in industries. Private companies can share their expertise in developing technologies such as blockchain security. As such, a partnership will help smaller organizations access tools and knowledge that might otherwise be out of reach.
- **Build Cross-Domain Training Programs:** Bringing together experts from different sectors can improve the skills of cybersecurity teams. If healthcare and finance organizations collaborate, they can train their staff in using IoT frameworks or blockchain threat detection tools. It can also help create a shared understanding of emerging threats and best practices for addressing them.

C. Future Directions

➢ *Opportunities for Interdisciplinary Research*

Cybersecurity is becoming more complicated as technology connects different systems and areas. We believe this is an opportunity for interdisciplinary research to bring together expertise from various fields. Knowledge of computer science, engineering, behavioral science, and public policy can create better frameworks for threat intelligence. Hence, we developed a hypothetical framework, inspired by the studies reviewed in this research. This hypothetical framework combines predictive analytics, cross-domain data sharing, and adaptive learning.

➢ *Hypothetical Framework: Adaptive Multimodal Threat Intelligence Framework (AMTIF)*

- **Objective:** The AMTIF would enhance threat intelligence by integrating data from multiple sources, using real-time analysis and adaptive learning to detect and respond to threats (Figure 10).

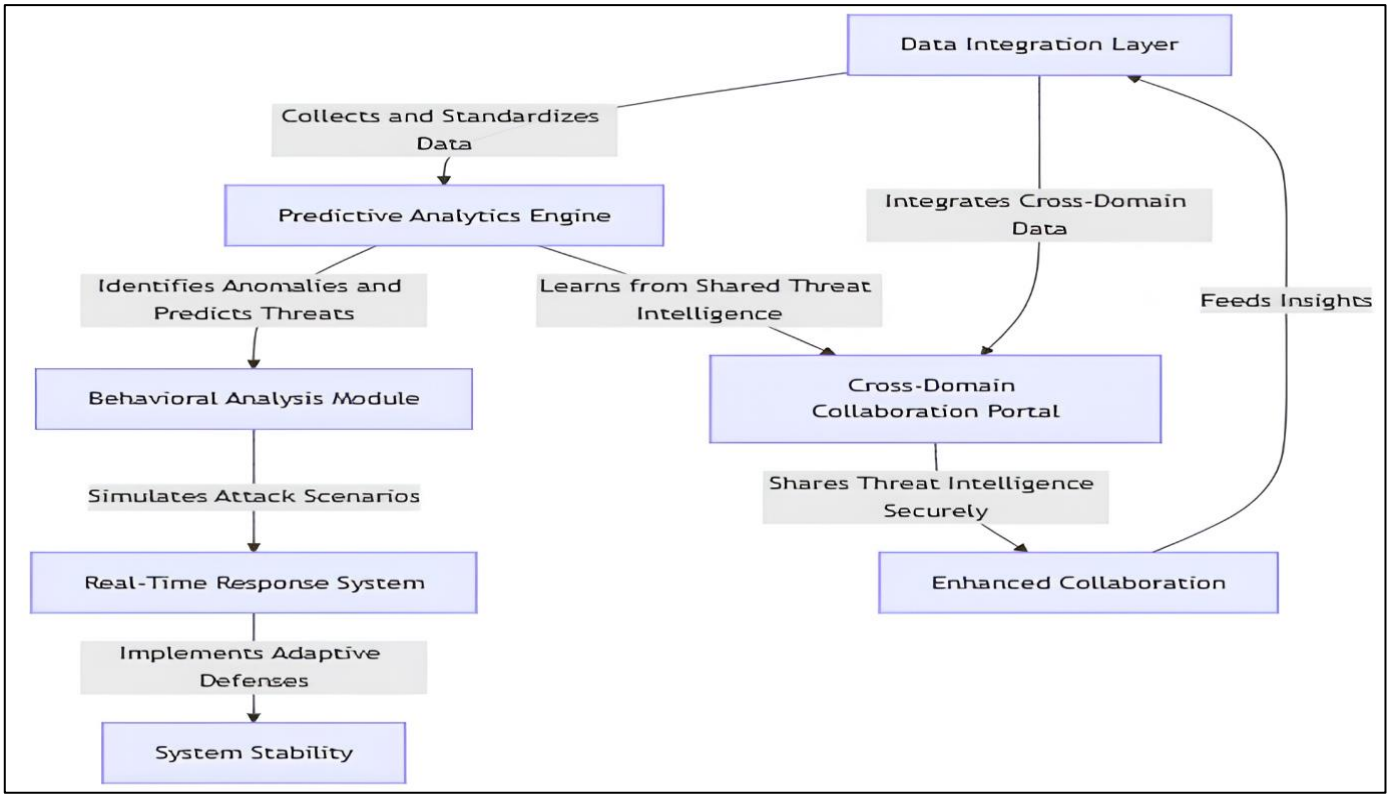

Fig 10: Proposed Adaptive Multimodal Threat Intelligence Framework (AMTIF)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

➢ *Components:*

- **Data Integration Layer**: This layer is expected to gather data from sources like IoT devices, cloud environments, and network traffic. It is similar to the unified taxonomy proposed by Martins and Medeiros[38]. This layer would standardize data collection to improve analysis.
- **Predictive Analytics Engine**: We borrow this idea from the machine learning models as applied by Fu et al.[29] and Gajjar et al.[20]. This engine would identify anomalies and predict potential threats. For instance, it could detect early signs of ransomware or insider threats.
- **Behavioral Analysis Module**: This is inspired by frameworks like those used in SAIBERSOC[37]. This module would simulate potential attack scenarios. Behavioral science could be integrated to understand how attackers might adapt their tactics.
- **Real-Time Response System**: We borrow ideas from the timing-based resilience in CPS by Maruf et al.[36]. This system would implement adaptive defenses to maintain system stability during attacks.
- **Cross-Domain Collaboration Portal**: This component would allow organizations to share threat intelligence securely. This method is similar to the automated alert sharing used by Husák et al.[39].

➢ *Functionality:*

- AMTIF would enable organizations in different sectors to work together by integrating their data and sharing insights.
- Its adaptive learning feature would continuously improve threat detection and response as new data is introduced.
- The framework would also help test defenses in simulated environments, providing insights for future improvements.

In practice, this framework should demonstrate how interdisciplinary research can address complex cybersecurity challenges.

➢ *Emerging Technologies and Their Potential to Enhance Threat Intelligence*

- **Artificial Intelligence and Machine Learning:** Artificial intelligence (AI) and machine learning (ML) are already improving threat intelligence. However, their potential has yet to be fully realized. Technologies like self-supervised learning[46], enable systems to adapt by learning from unlabeled data. AI can also improve the accuracy of threat detection and reduce false positives, making frameworks more reliable. Generative adversarial networks (GANs)[43] also show potential for simulating new attack methods. This will help organizations prepare for evolving threats. AI can also support natural language processing tools like CySecBERT[53], to analyze complex cybersecurity data more efficiently.
- **Blockchain Technology:** Smart contracts could automate data sharing between organizations while ensuring privacy and compliance. Frameworks for blockchain threat detection, like those studied by Rabieinejad et al.[43], could also be expanded to protect financial and supply chain systems from cyberattacks.
- **Internet of Things (IoT) Security Enhancements:** The IoT connects billions of devices, creating both opportunities and challenges for cybersecurity. As proposed by Ameer et al.[51], zero-trust architectures could be enhanced by new technologies like quantum encryption. This would provide stronger protection for IoT networks against threats like spoofing attacks[54].
- **Quantum Computing:** Quantum computing poses risks to traditional encryption methods. However, Sonko et al.[55] established that it offers opportunities for developing more advanced cryptographic systems. Quantum key distribution (QKD) could make data transmission in frameworks like CPS or IoT systems more secure. This could improve the resilience of critical infrastructure, which relies on secure communication to prevent disruptions.
- **Augmented Reality (AR) and Virtual Reality (VR):** AR and VR technologies could enhance cybersecurity professionals' training programs. For example, simulation tools like SAIBERSOC could integrate VR to provide immersive training environments for responding to cyberattacks. AR and VR can also help visualize complex threat data, making it easier for teams to analyze and act on intelligence.

It is thus safe to say that future research in speculative threat intelligence frameworks can benefit from interdisciplinary collaboration and emerging technologies. A hypothetical framework like AMTIF can show how to integrate data from different domains. Predictive analytics and adaptive learning create more resilient defenses. Emerging technologies such as AI, blockchain, and quantum computing can further enhance these frameworks by improving data security, detection capabilities, and collaboration. As threats continue to evolve, investing in these areas will be crucial for advancing the field of cybersecurity.

VI. CONCLUSION

The field of speculative threat intelligence is relatively new. It is advancing rapidly as cybersecurity threats grow in complexity and scope. This study explored frameworks and methodologies aimed at predicting, detecting, and preventing new threats. Environments studied include cyber-physical systems (CPS), Internet of Things (IoT) networks, blockchain platforms, and cloud-based infrastructures. We identified key strengths, limitations, and future directions in speculative threat intelligence.

One strength of existing frameworks is their integration of advanced technologies. This includes artificial intelligence, machine learning, and automation. These technologies enable frameworks to analyze big data, detect anomalies, and predict potential threats with high efficiency and accuracy. Multimodal CPS and blockchain environments have been shown to have the potential to adapt to evolving threats. This ensures proactive and resilient defense systems. Additionally, frameworks such as Zero-Trust architectures

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

are important continuous verification and access control. They reduce vulnerabilities in increasingly connected ecosystems.

However, there are still challenges that remain. The complexity of using and maintaining these frameworks often limits their adoption. This is particularly felt in smaller organizations with limited resources. High implementation costs, a lack of skilled professionals, and scalability challenges further hinder their use. Moreover, barriers such as organizational resistance, legal compliance, and interoperability between systems continue to limit their application. Future opportunities lie in interdisciplinary collaboration and the adoption of emerging technologies. Our hypothetical Adaptive Multimodal Threat Intelligence Framework (AMTIF) is a step in this direction. AMTIF integrates predictive analytics, real-time monitoring, and cross-domain data sharing to improve threat detection and response. Emerging technologies like blockchain, quantum computing, and self-supervised machine learning also hold promise for evolving the capabilities of these frameworks.

We thus conclude that speculative threat intelligence frameworks are useful tools in the dynamic cybersecurity threat landscape. It is true that a lot of progress has been made. However, continued innovation, collaboration, and adaptation are required to overcome current challenges. It will also ensure the security and resilience of critical systems and infrastructures. The field of speculative threat intelligence focus on practical applications and leverage cutting-edge technologies. Thus, it can move closer to achieving its goal of proactive and effective cybersecurity.

- **Competing Interest:** There is no competing interest.

REFERENCES

[1]. A. . Juneja, S. Goswami, and S. Mondal, *Cyber security and digital economy: opportunities, growth and challenges.* Journal of technology innovations and energy, 2024. **3**: p. 1-22.

[2]. S.S. Goswami, et al., *The role of cyber security in advancing sustainable digitalization: Opportunities and challenges.* Journal of Decision Analytics and Intelligent Computing, 2023. **3**(1): p. 270-285.

[3]. A. Chakraborty, A. Biswas, and A.K. Khan, *Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation*, in *Artificial Intelligence for Societal Issues*, A. Biswas, V.B. Semwal, and D. Singh, Editors. 2023, Springer International Publishing: Cham. p. 3-25.

[4]. T. Stevens, J. Devanny, and A. Brantly, *Research Handbook on Cyberwarfare*. Chapter 7: Cyber intelligence: method or target? 2024: Edward Elgar Publishing. 98-114.

[5]. M. Zaydi, Y. Maleh, and Y. Khourdifi, *A new framework for agile cybersecurity risk management: Integrating continuous adaptation and real-time threat intelligence (ACSRM-ICTI)*, in *Agile Security in the Digital Era*. 2025, CRC Press. p. 19-47.

[6]. S. Heinonen, J. Karjalainen, and A. Taylor, *Landscapes of our uncertain Futures.* Towards mapping and understanding crisis-related concepts and definitions. Landscapes of our uncertain Futures. Towards mapping and understanding crisis-related concepts and definitions. FFRC eBOOKS, 2022. **7**: p. 2022.

[7]. P. Manandha, *Exploring Machine Learning and Big Data Techniques for Proactive Identification of Cybersecurity Vulnerabilities in Complex Networks.* Global Research Perspectives on Cybersecurity Governance, Policy, and Management, 2023. **7**(11): p. 1-11.

[8]. A. Marshall, et al., *Forecasting unknown-unknowns by boosting the risk radar within the risk intelligent organisation.* International Journal of Forecasting, 2019. **35**(2): p. 644-658.

[9]. J. Olusegun, *Utilizing Predictive Analytics for Threat Detection and Prevention in Cybersecurity.* 2024.

[10]. S. Ainslie, et al., *Cyber-threat intelligence for security decision-making: A review and research agenda for practice*. Computers & Security, 2023. **132**: p. 103352.

[11]. G. Cascavilla, D.A. Tamburri, and W.-J. Van Den Heuvel, *Cybercrime threat intelligence: A systematic multi-vocal literature review.* Computers & Security, 2021. **105**: p. 102258.

[12]. S.N. Sakib, *Cyber Threat Intelligence.* 2022.

[13]. M. Campfield, *The practical difference between known and unknown threats.* Computer Fraud & Security, 2021. **2021**(5): p. 6-9.

[14]. D. Schlette, *Cyber Threat Intelligence*, in *Encyclopedia of Cryptography, Security and Privacy*, S. Jajodia, P. Samarati, and M. Yung, Editors. 2019, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 1-3.

[15]. M. Conti, T. Dargahi, and A. Dehghantanha, *Cyber threat intelligence: challenges and opportunities*. 2018: Springer.

[16]. P. Lin, et al., *Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise.* arXiv preprint arXiv:2406.12041, 2024.

[17]. J. Matilainen, *Using cyber threat intelligence as a part of organisational cybersecurity*, in *Information Systems Science*. 2021.

[18]. P. Radanliev, et al., *Super-forecasting the 'technological singularity' risks from artificial intelligence*. Evolving Systems, 2022. **13**(5): p. 747-757.

[19]. B. Breve, G. Cimino, and V. Deufemia, *Hybrid Prompt Learning for Generating Justifications of Security Risks in Automation Rules.* ACM Trans. Intell. Syst. Technol., 2024. **15**(5): p. Article 103.

[20]. A. Gajjar, et al., *RD-FAXID: Ransomware Detection with FPGA-Accelerated XGBoost.* ACM Trans. Reconfigurable Technol. Syst., 2024. **17**(4): p. Article 56.

[21]. R.A. Bridges, et al., *Beyond the Hype: An Evaluation of Commercially Available Machine Learning–based Malware Detectors.* Digital Threats, 2023. **4**(2): p. Article 27.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

[22]. S. Samtani, et al., *Informing Cyber Threat Intelligence through Dark Web Situational Awareness: The AZSecure Hacker Assets Portal*. Digital Threats, 2021. **2**(4): p. Article 27.
[23]. B. Bjurling and S. Raza, *Cyber Threat Intelligence meets the Analytic Tradecraft*. ACM Trans. Priv. Secur., 2024. **28**(1): p. Article 6.
[24]. A. Albasir, K. Naik, and R. Manzano, *Toward Improving the Security of IoT and CPS Devices: An AI Approach.* Digital Threats, 2023. **4**(2): p. Article 22.
[25]. S. Banik, et al., *Automated Adversary-in-the-Loop Cyber-Physical Defense Planning.* ACM Trans. Cyber-Phys. Syst., 2023. **7**(3): p. Article 18.
[26]. J. Happa, et al., *Deception in Network Defences Using Unpredictability*. Digital Threats, 2021. **2**(4): p. Article 29.
[27]. M. Mundt and H. Baier, *Threat-Based Simulation of Data Exfiltration Toward Mitigating Multiple Ransomware Extortions.* Digital Threats, 2023. **4**(4): p. Article 54.
[28]. A. Dubey, et al., *Guarding Machine Learning Hardware Against Physical Side-channel Attacks.* J. Emerg. Technol. Comput. Syst., 2022. **18**(3): p. Article 56.
[29]. H. Fu, P. Krishnamurthy, and F. Khorrami, *Combining switching mechanism with re-initialization and anomaly detection for resiliency of cyber–physical systems.* Automatica, 2025. **172**: p. 111994.
[30]. W. Ou, et al., *VeriBin: A Malware Authorship Verification Approach for APT Tracking through Explainable and Functionality-Debiasing Adversarial Representation Learning.* ACM Trans. Priv. Secur., 2024. **27**(3): p. Article 26.
[31]. A. Staves, A. Gouglidis, and D. Hutchison, *An Analysis of Adversary-Centric Security Testing within Information and Operational Technology Environments.* Digital Threats, 2023. **4**(1): p. Article 14.
[32]. A. Amro, V. Gkioulos, and S. Katsikas, *Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework.* ACM Trans. Priv. Secur., 2023. **26**(2): p. Article 22.
[33]. L. Axon, et al., *Ransomware as a Predator: Modelling the Systemic Risk to Prey.* Digital Threats, 2023. **4**(4): p. Article 55.
[34]. P. Bajpai and R. Enbody, *Know Thy Ransomware Response: A Detailed Framework for Devising Effective Ransomware Response Strategies.* Digital Threats, 2023. **4**(4): p. Article 57.
[35]. L. Csikor, et al., *RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems.* ACM Trans. Cyber-Phys. Syst., 2024. **8**(1): p. Article 5.
[36]. A.A. Maruf, et al., *A Timing-Based Framework for Designing Resilient Cyber-Physical Systems under Safety Constraint.* ACM Trans. Cyber-Phys. Syst., 2023. **7**(3): p. Article 19.
[37]. M. Rosso, et al., *SAIBERSOC: A Methodology and Tool for Experimenting with Security Operation Centers.* Digital Threats, 2022. **3**(2): p. Article 14.
[38]. C. Martins and I. Medeiros, *Generating Quality Threat Intelligence Leveraging OSINT and a Cyber Threat Unified Taxonomy*. ACM Trans. Priv. Secur., 2022. **25**(3): p. Article 19.
[39]. M. Husák, et al., *Lessons Learned from Automated Sharing of Intrusion Detection Alerts: The Case of the SABU Platform.* Digital Threats, 2023. **4**(4): p. Article 48.
[40]. P.-D. Jarvis, et al., *Vulnerability Exposure Driven Intelligence in Smart, Circular Cities.* Digital Threats, 2022. **3**(4): p. Article 40.
[41]. N. Rani, et al., *TTPXHunter: Actionable Threat Intelligence Extraction as TTPs from Finished Cyber Threat Reports.* Digital Threats, 2024. **5**(4): p. Article 37.
[42]. M. Maceiras, et al., *Know their Customers: An Empirical Study of Online Account Enumeration Attacks.* ACM Trans. Web, 2024. **18**(3): p. Article 37.
[43]. E. Rabieinejad, et al., *Generative Adversarial Networks for Cyber Threat Hunting in Ethereum Blockchain.* Distrib. Ledger Technol., 2023. **2**(2): p. Article 9.
[44]. A.E. Hong, P.P. Malinovsky, and S.K. Damodaran, *Towards Attack Detection in Multimodal Cyber-Physical Systems with Sticky HDP-HMM based Time Series Analysis.* Digital Threats, 2024. **5**(1): p. Article 5.
[45]. E. López-Morales, *Securing Cyber-Physical Systems via Advanced Cyber Threat Intelligence Methods*, in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*. 2024, Association for Computing Machinery: Salt Lake City, UT, USA. p. 5119–5121.
[46]. O. Tunde-Onadele, et al., *Self-Supervised Machine Learning Framework for Online Container Security Attack Detection.* ACM Trans. Auton. Adapt. Syst., 2024. **19**(3): p. Article 16.
[47]. V. Engström, et al., *Automated Security Assessments of Amazon Web Services Environments.* ACM Trans. Priv. Secur., 2023. **26**(2): p. Article 20.
[48]. M.M. Rahman, et al., *Security Evaluation of State Space Obfuscation of Hardware IP through a Red Team-Blue Team Practice.* ACM Trans. Des. Autom. Electron. Syst., 2024. **29**(3): p. Article 50.
[49]. R. Pal, et al., *How Hard Is Cyber-risk Management in IT/OT Systems? A Theory to Classify and Conquer Hardness of Insuring ICSs.* ACM Trans. Cyber-Phys. Syst., 2023. **6**(4): p. Article 35.
[50]. Y. Zhao, C. Rieger, and Q. Zhu, *Multi-agent Learning for Resilient Distributed Control Systems*, in *Power Grid Resilience: Theory and Applications*, J. Wang, Editor. 2025, Springer Nature Switzerland: Cham. p. 425-458.
[51]. S. Ameer, et al., *ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model.* ACM Trans. Priv. Secur., 2024. **27**(3): p. Article 22.
[52]. L. Axon, et al., *Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda.* Digital Threats, 2022. **3**(4): p. Article 34.
[53]. M. Bayer, et al., *CySecBERT: A Domain-Adapted Language Model for the Cybersecurity Domain.* ACM Trans. Priv. Secur., 2024. **27**(2): p. Article 18.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr2255

[54]. P. Madani, N. Vlajic, and I. Maljevic, *Randomized Moving Target Approach for MAC-Layer Spoofing Detection and Prevention in IoT Systems.* Digital Threats, 2022. **3**(4): p. Article 35.

[55]. S. Sonko, et al., *Quantum cryptography and US digital security: a comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security.* Computer Science & IT Research Journal, 2024. **5**(2): p. 390-414.