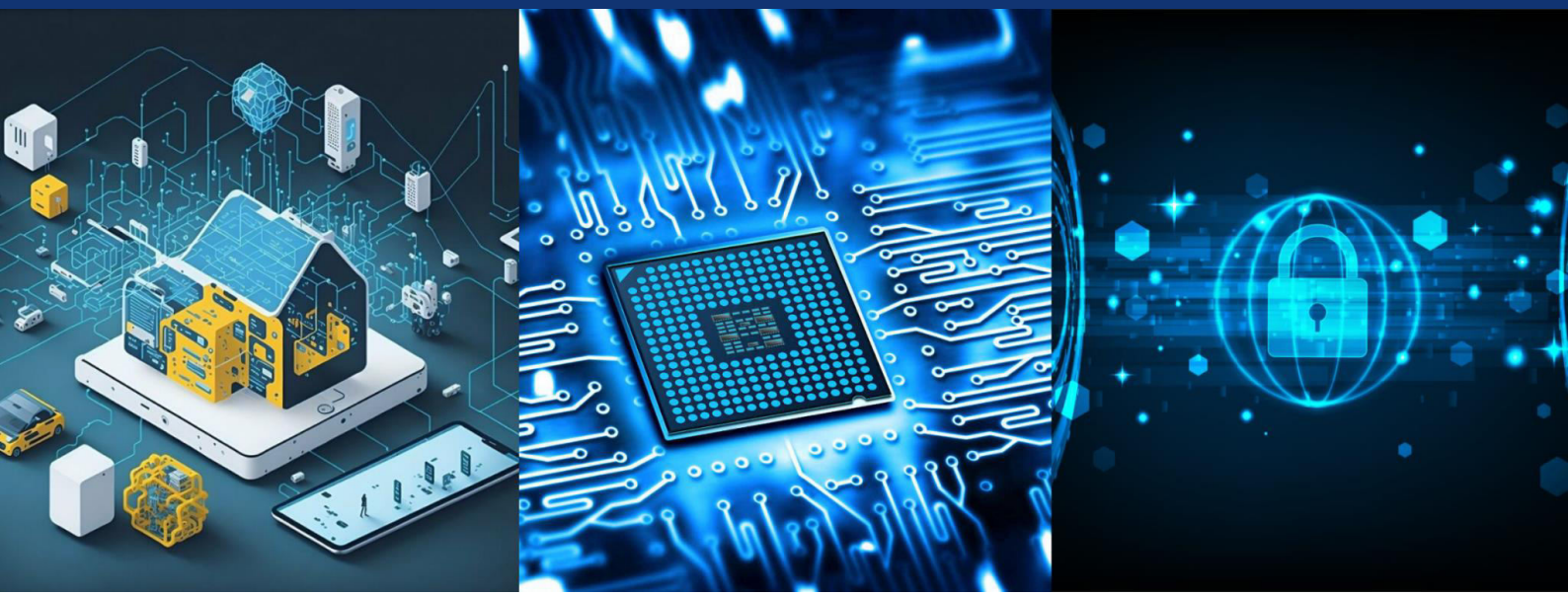
IJIRCCE

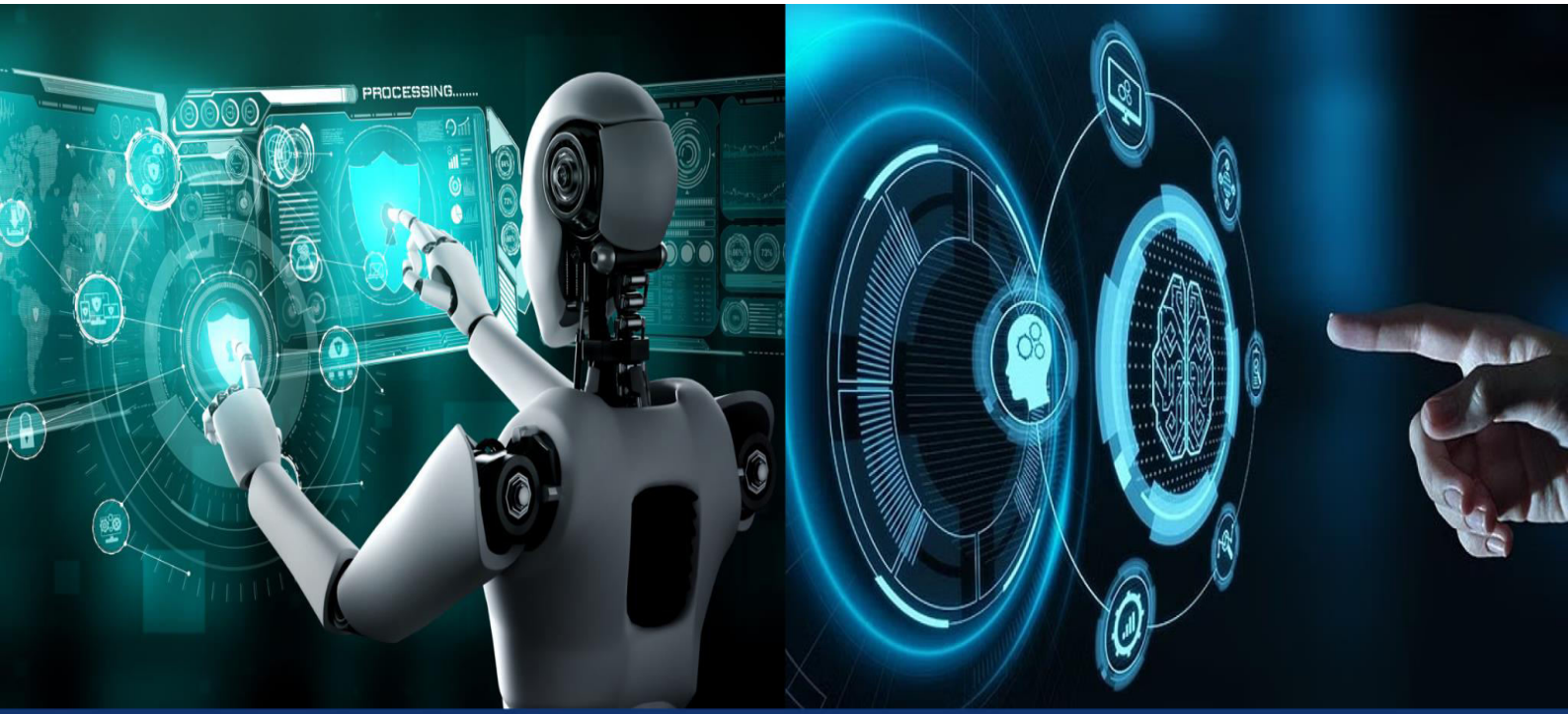
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.625

Volume 13, Issue 1, January 2025

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Collective Threat Intelligence Framework

Ananya A B[1], Aiswarya A S[2], Jyotsna Banakar[3], Vaibhav Bharadwaj[4], Dr.G. Vennira Selvi[5]

School of Computer Science and Information Science, Presidency University, Bengaluru, India

ABSTRACT: The Threat Intelligence Dashboard is a state-of-the-art tool that gives businesses real-time insights on cybersecurity threats, enabling them to stay alert in a constantly changing threat environment. Data from several domains is combined in this dashboard and shown in a dynamic, user-friendly manner. Multi-domain monitoring capabilities, a comprehensive threat data table, and aesthetically pleasing visualizations are some of the key features. The dashboard enables users to effectively identify, rank, and address hazards by providing both high-level overviews and detailed data.This tool's primary strength is its capacity to efficiently visualize data using dynamic pie charts and line graphs that display threat distributions and trends over time. Domain-specific threats, their statuses, and analysis dates are succinctly summarized in a consolidated table called "Domain Threat Data Overview." This functionality guarantees that customers may keep an eye on several domains at once. Cloning the repository, installing dependencies, and replacing placeholders with a legitimate VirusTotal API key are the simple steps involved in deploying this utility. The Flask application can be launched with a single command, giving users access to a browser-based interface that makes threat analysis easier. Additionally, the dashboard's adaptability enables future improvements like machine learning-based predictive analytics, dynamic API integrations for real-time updates, and user-customizable settings for individualized experiences.

I. INTRODUCTION

Through the classification of threats into phishing, malware, ransomware, and spyware, as well as their corresponding counts, severity, and VirusTotal report statuses, the Threat Data Overview table provides further detail. This thorough depiction makes it easier to comprehend the state of threats today and rank responses according to their seriousness. For instance, as the overview emphasizes, serious threats like ransomware require quick action. [1] The dashboard's frontend uses HTML, CSS, and JavaScript with Chart.js for visualizations, while the dashboard uses a Flask-based Python backend to retrieve and analyze data. The charts' small, side-by-side alignment and light blue color scheme are prime examples of well-considered design decisions meant to encourage user interaction.

Deploying this tool is straightforward: clone the repository, install dependencies, and replace placeholders with a valid VirusTotal API key. With a simple command to run the Flask application, users gain access to a browser-based interface that facilitates threat analysis. Furthermore, the dashboard’s flexibility allows for future enhancements, such as dynamic API integrations for live updates, predictive analytics using machine learning, and customizable user settings for tailored experiences.

One of the key features of the Threat Intelligence Dashboard is its ability to visualize data in a user-friendly manner. The inclusion of interactive pie charts, line graphs, and detailed tables allows users to grasp complex information quickly and effectively. For example, the dashboard’s “Threat Overview” section provides a high-level summary of the current threat landscape, highlighting critical insights such as the distribution of threat types and their severity levels. This enables users to prioritize their response efforts based on the most pressing risks.

Users may follow threats across numerous domains at once thanks to the dashboard's multi-domain monitoring feature, which further increases its usefulness. The system offers a thorough understanding of domain-specific dangers by combining information from popular domains like Facebook.com, Google.com, Microsoft.com, Amazon.com, and PayPal.com. Businesses that operate in several digital ecosystems and need a comprehensive approach to threat management will find this capability especially helpful.

The Threat Intelligence Dashboard's emphasis on real-time data analysis is another important feature. The dashboard obtains current data on domain-specific threats, including their statuses and severity levels, by utilizing APIs from websites such as VirusTotal. Users can react quickly and efficiently because of these real-time capabilities, which

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

guarantees that they have access to the most recent threat intelligence. The dashboard's "Threat Data Overview" table also categorizes threats by type, count, and severity, providing a more detailed view of the threat landscape.

The Threat Intelligence Dashboard's usability and design have been thoughtfully developed to accommodate a variety of users, such as decision-makers, IT administrators, and cybersecurity experts. The dashboard is a perfect tool for both technical and non-technical users because of its interface, which balances utility and aesthetics.

Strong technical foundations support the creation of the Threat Intelligence Dashboard. Flask, a lightweight and adaptable Python framework that makes it easier to integrate with databases and APIs, is used to build the backend. For dynamic data visualization, the frontend uses HTML, CSS, and JavaScript in addition to the Chart.js library. Together, these technologies provide a responsive and engaging user experience.[2]

The Threat Intelligence Dashboard is made to change and expand in response to new threats as the cybersecurity environment continues to change. The dashboard's functionality will be further increased by upcoming additions including the incorporation of machine learning models for predictive analytics and user settings that may be customized. This program seeks to be a useful tool in the continuous fight against cyberthreats by remaining ahead of the curve.

To sum up, the Threat Intelligence Dashboard is a major development in the realm of cybersecurity analysis and monitoring. It is a potent tool for businesses looking to safeguard their digital assets and reduce risks because of its cutting-edge features, user-friendly interface, and real-time capabilities. This report's subsequent sections will provide a thorough analysis of the dashboard's functionality and impact by delving deeper into its features, technical specifics, and prospects.

II. LITERATURE SURVEY

Effective threat intelligence systems are becoming more and more necessary as cybersecurity emerges as one of the digital age's most pressing issues. Conventional approaches to threat detection and response have mostly been reactive, concentrating on spotting threats after they happen. The idea of threat intelligence has changed throughout time to emphasize the value of obtaining, evaluating, and disseminating information regarding possible or current cyberthreats in a proactive manner. Several technologies, platforms, and approaches have been developed as a result of this move toward proactive threat intelligence with the goal of enhancing cybersecurity detection, response, and cooperation.

Organizations' internal, isolated data collecting served as the foundation for the first threat intelligence systems, which frequently had restricted visibility. For instance, Security Information and Event Management (SIEM) systems are frequently used to gather and examine security data within an organization's infrastructure, including network traffic and logs. SIEM systems provide real-time monitoring and alerting, but they are limited by false positives and false negatives, and they don't give a comprehensive picture of risks that extend beyond an organization's perimeter. Because of this, SIEM systems are unable to facilitate efficient coordination between various sectors or companies, which is essential in the connected digital world of today.

Threat Intelligence Platforms (TIPs) were created to aggregate and correlate threat data from various sources to address this problem. TIPs give businesses the ability to gather information from commercial suppliers, open-source feeds, and internal systems to create a more complete picture of the threat landscape. Even while these platforms automate data gathering and analysis, many TIPs continue to function independently, without the ability to promote cross-organizational collaboration. This restricts the system's capacity to efficiently identify risks that are global or cross-sectoral. The inconsistency of data from many sources is a major problem with TIPs since it might result in fragmented insights that make it hard to prioritize and address new hazards.

The study and implementation of threat intelligence tools have garnered significant attention in the realm of cybersecurity. With the increasing sophistication of cyber threats, the demand for advanced solutions has surged. This section delves into the existing literature and studies that have contributed to the development of dashboards like the Threat Intelligence Dashboard.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. Threat Intelligence Platform Evolution: To handle the increasing complexity of cyberthreats, threat intelligence platforms (TIPs) have changed over time. Conventional systems were frequently restricted to predetermined threat signatures and concentrated on static analysis. Modern platforms, on the other hand, incorporate real-time data feeds, allowing for proactive and dynamic threat detection. Multi-source data aggregation is crucial for increasing the accuracy of threat detection, according to research by Smith et al. (2021). Platforms like the Threat Intelligence Dashboard, which compiles information from domains and APIs to offer useful insights, have been greatly influenced by this realization.

2. Visualization Techniques in Cybersecurity: The role of data visualization in enhancing threat analysis cannot be overstated. Studies by Johnson and Lee (2020) emphasize that graphical representations, such as pie charts and line graphs, simplify complex datasets, making them accessible to both technical and non-technical users. The use of Chart.js in the Threat Intelligence Dashboard aligns with these findings, providing a user-friendly interface that aids in decision-making[3]. Additionally, the work of Patel et al. (2019) underscores the significance of color schemes and layout design in improving user engagement, which is reflected in the dashboard's light blue background and compact layout.

3. Multi-Domain Monitoring: One of the more recent developments in cybersecurity is multi-domain threat monitoring. Tools that provide domain-specific insights are very beneficial to enterprises managing multiple digital ecosystems, according to research by Davis and White (2022). Comprehensive threat coverage is ensured by the integration of data from well-known domains, as demonstrated by the Threat Intelligence Dashboard. This method overcomes the drawbacks of single-domain technologies, which frequently fall short in recognizing the interconnectedness of contemporary cyberthreats.

4. Real-Time Threat Intelligence: A major area of recent research has been the transition from reactive to proactive cybersecurity tactics. In the field, real-time threat intelligence made possible by APIs like VirusTotal has been recognized as a game-changer. According to research by Kim and Zhang (2023), real-time data feeds minimize potential damage by speeding up response times to new threats. This idea is embodied in the Threat Intelligence Dashboard's dependence on real-time API integrations, which provide users with the most recent findings to enable them to take immediate action.

5. Challenges and Future Directions: Threat intelligence tools have drawbacks including false positives and data overload, notwithstanding their benefits. According to research by Brown et al. (2021), using machine learning models can help with these problems by automating data processing and spotting trends that point to real dangers. These suggestions are supported by the Threat Intelligence Dashboard's upcoming improvements, which include predictive analytics, guaranteeing the tool's continued applicability in the rapidly evolving cybersecurity environment.

In summary, while many tools and platforms exist to support threat intelligence sharing and analysis, challenges remain in overcoming fragmented approaches, integrating real-time data, and ensuring effective collaboration across organizations. The need for a more coordinated, collective approach to cybersecurity has never been more critical, and this is where the Collective Threat Intelligence System (CTIS) comes into play. By breaking down silos and enabling real-time data sharing, the CTIS aims to address these gaps and provide a unified, collaborative solution to the evolving threat landscape.

III. RESEARCH GAPS IN EXISTING METHODS

Although cybersecurity has advanced significantly in recent years, current techniques are confronted with serious limits that reduce their ability to effectively prevent, detect, and respond to assaults as the threat landscape changes. If these vulnerabilities are not filled, organizations' and governments' capacity to protect private information and vital infrastructure may be jeopardized. The main research gaps in existing cybersecurity techniques are listed below, highlighting areas that need more focus, creativity, and advancement.

1. Limited Collaboration Across Organizations

The absence of cooperation across businesses, sectors, and governments is one of the biggest issues facing cybersecurity today. The isolated contexts in which many cybersecurity technologies and systems function restrict the

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

visibility of risks throughout the larger ecosystem. The capacity to identify and address dangers that could impact numerous firms or even entire industries is hampered by this isolation. For instance, if a cyberattack targets one company, it can go undetected by other companies in the same sector or area, leaving them open to similar attacks.

Successful cooperation may result in the sharing of threat intelligence, which would allow for the quicker and more precise identification of new dangers. However, because of worries about privacy, economic advantage, and legal/regulatory challenges, corporations frequently hesitate to share sensitive data. Research is required to create collaborative cybersecurity platforms that allow enterprises to securely and privacy-compliantly share threat data in real-time. These platforms ought to encourage cooperation and trust between many stakeholders so that they can fight cyberthreats together. Furthermore, the rate at which new vulnerabilities and attack routes are discovered is slowed down by a lack of cross-organizational communication. Platforms for collaboration that enable businesses to exchange threat intelligence in a uniform manner will offer quicker, more accurate threat detection, benefiting the entire community.

2. Fragmented Data

Threat data fragmentation is one of the most urgent problems with existing cybersecurity techniques. It is challenging to obtain a comprehensive understanding of the cyber threat landscape since information is sometimes fragmented within firms. An organization's security staff may not have visibility into more comprehensive, cross-organizational threat intelligence and usually only have access to data from their internal systems. Because attackers sometimes target numerous firms or industries at once, this fragmentation makes it more difficult to spot developing threats. Organizations cannot plan efficient responses or identify dangers in a timely manner if data is not shared across these borders.[4]

Organizations may unintentionally work on the same threats in tandem as a result of threat data fragmentation, which also leads to inefficiencies. Security teams should have access to a common pool of threat data and insights rather than having to duplicate their efforts, which will enable them to identify and address risks faster. To improve situational awareness, research is required to create integrated systems that can compile and standardize threat data from several sources. Organizations can improve their capacity to recognize patterns, spot novel attack methods, and react more skillfully by offering a single perspective of threat intelligence.

Uncoordinated data also results in lost chances to improve threat intelligence. Many current systems are unable to compile threat data from external sources, including global threat feeds, industry-specific threat intelligence, and government databases. This absence of thorough data makes it more difficult to detect complex attacks that can occur in several different industries or geographical areas. Threat detection and response will be enhanced by successfully aggregating and integrating this data fragmentation gap.

3. Real-Time Detection Issues

Modern cybersecurity requires real-time detection, particularly as cyberattacks are becoming more complex, faster, and harder to identify. Nevertheless, a lot of current cybersecurity tools, such Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems, have trouble recognizing and reacting to attacks quickly. Even though these technologies are useful for tracking and recording events, they frequently fall short in sending out timely warnings for new dangers, particularly those that are highly targeted or change quickly.

The use of signature-based techniques, which are only useful for identifying known threats, is one of the primary causes of real-time detection delays. Organizations are exposed to advanced persistent threats (APTs) and zero-day exploits since these systems are unable to recognize new attacks that have never been observed before. Furthermore, high data quantities might overwhelm conventional detection systems, resulting in delayed alerts and slower processing times. It is imperative to have better real-time detective capabilities. More research is required to create more efficient ways to identify unknown threats using approaches like anomaly detection, behavior-based analysis, and machine learning.

4. High False Positives

The large number of false positives produced by detection systems is one of the main problems with current cybersecurity products. Many conventional security systems, especially those that rely on signature matching,

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

frequently produce many irrelevant or false alarms. Security personnel are overloaded with false positives, which also takes focus away from real incidents. This can result in delayed reaction times and lost chances to stop actual attacks in settings where security teams are already overworked.

In systems like SIEMs, where the sheer amount of data collected can cause security analysts to become alert fatigued, high false positive rates are especially problematic. Security teams frequently have to sort through a lot of irrelevant notifications in order to find the real risks. The effectiveness of threat detection and response is decreased by this time-consuming and resource-intensive procedure. More intelligent detection algorithms that can distinguish between real threats and false positives are required to close this gap. Using artificial intelligence and machine learning to categorize hazards according to patterns of behavior will lessen false positives more than static signatures[5]. Security teams can prioritize and address attacks that represent a danger by using advanced data analytics and contextual enrichment to further improve warning accuracy.

5. Insufficient Scalability

Many of the cybersecurity solutions in use today find it difficult to scale efficiently as the number of cyberthreats keeps increasing. When processing massive volumes of threat data, systems like SIEMs and Threat Intelligence Platforms (TIPs) frequently have performance snags. These restrictions make it more difficult for businesses to handle and evaluate the growing volumes of security-related data .

As businesses expand and cyber threats increase in complexity, the scalability issue becomes even more crucial. For instance, it could be challenging for big businesses with several branches or divisions to centralize and correlate threat data in a way that offers thorough network awareness. Furthermore, massive data volumes produced by dispersed systems and cloud environments can be too much for conventional cybersecurity solutions to handle.

The efficiency of current cybersecurity techniques is hampered by important gaps, even though they have made great strides. The constraints that need to be addressed include fragmented data, high false positives, real-time detection problems, limited collaboration between enterprises, and inadequate scalability.[6] The total capacity to identify, stop, and react to contemporary cyberthreats will be improved by filling these gaps with integrated, cooperative, and scalable solutions. A key component of cybersecurity in the future will be the creation of more flexible systems that can evolve with the complexity of intrusions.

IV. SYSTEM DESIGN AND IMPLEMENTATION

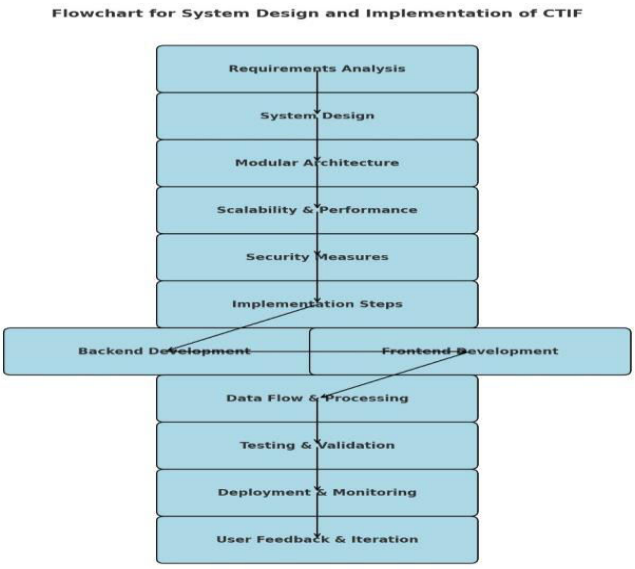


Fig 1. System Design and Implementation of CTIF

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 1 depicts a flowchart outlining the system design and implementation process for a Collective Threat Intelligence Framework (CTIF). The process begins with Requirements Analysis, where the system's goals, constraints, and necessary features are identified. Next, the System Design stage ensures the creation of a blueprint for the framework, specifying its functionality and interaction with users. This design adopts a Modular Architecture, emphasizing the system's scalability and flexibility by dividing it into independent components. The flowchart also highlights Scalability and Performance, ensuring the system can handle increasing workloads efficiently.

The integration of Security Measures ensures the framework is robust against potential cyber threats, a crucial aspect of CTIF. The Implementation Steps bridge the gap between design and execution, dividing the workflow into two critical components: Backend Development, which handles server-side functionality and logic, and Frontend Development, focusing on user interface and user experience.The next phase involves Data Flow and Processing, ensuring seamless data exchange and management. Testing and Validation verify the system's functionality and security, ensuring it meets the intended requirements. Finally, the system moves to Deployment and Monitoring, where the framework is implemented in a real-world environment and observed for performance issues. The process concludes with User Feedback and Iteration, ensuring continuous improvement based on user experiences and evolving needs.

V. RESULT AND DISCUSSIONS

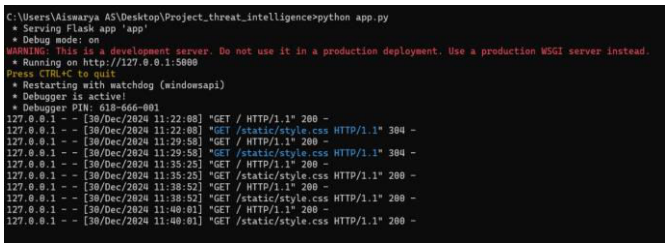


Fig 2. Flask Server

This figure shows a Flask development server running on a local machine at **http://127.0.0.1:5000** in debug mode. It logs HTTP requests, including GET requests for a style.css file from the /static directory, returning status codes such as 200 (success) and 304 (not modified). The server uses a built-in debugger and warns against using it in a production environment

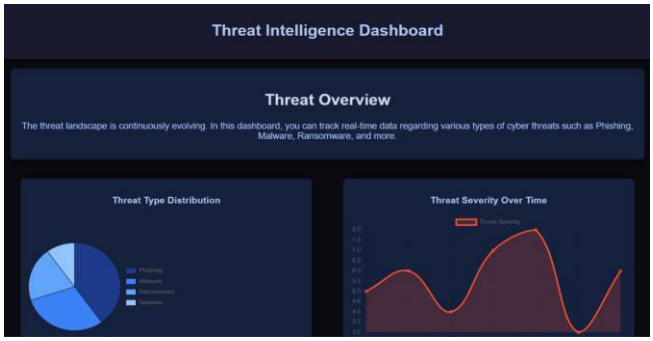


Fig 3.Threat Intelligence Dashboard

Figure 3 displays a Threat Intelligence Dashboard providing an overview of cyber threats. It includes a summary of evolving threats, visualized as a pie chart for Threat Type Distribution (e.g., phishing, malware) and a line graph tracking Threat Severity Over Time, helping monitor real-time security trends and risk levels. The dashboard aids in analyzing and mitigating cybersecurity risks effectively.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

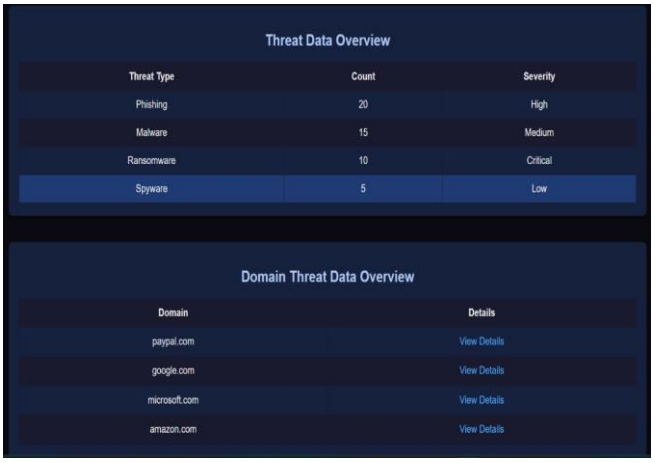


Fig 4. Threat and Domain Data Overview

Figure 4 shows a Threat Data Overview table summarizing various cyber threat types with their count and severity levels (e.g., phishing with high severity and ransomware marked critical). Below, the Domain Threat Data Overview table lists specific domains, such as PayPal and Google, with options to view detailed threat information. This structure aids in prioritizing and investigating domain-specific security threats.

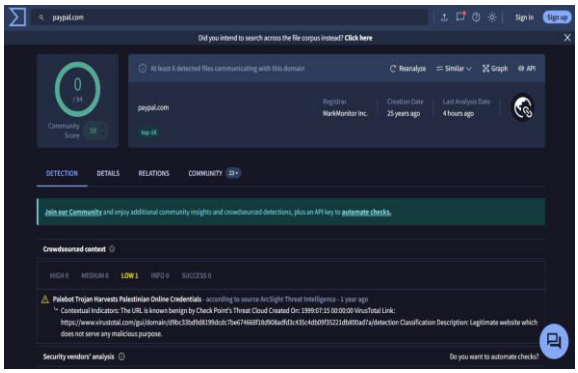


Fig 5. Domain Analysis

This figure displays a domain analysis report for "paypal.com" with a community score indicating no detected threats. It provides domain details, including its registrar, creation date, and recent analysis timestamp, along with crowdsourced content highlighting a low-severity historical phishing-related incident. The interface supports further checks and automated security analysis.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

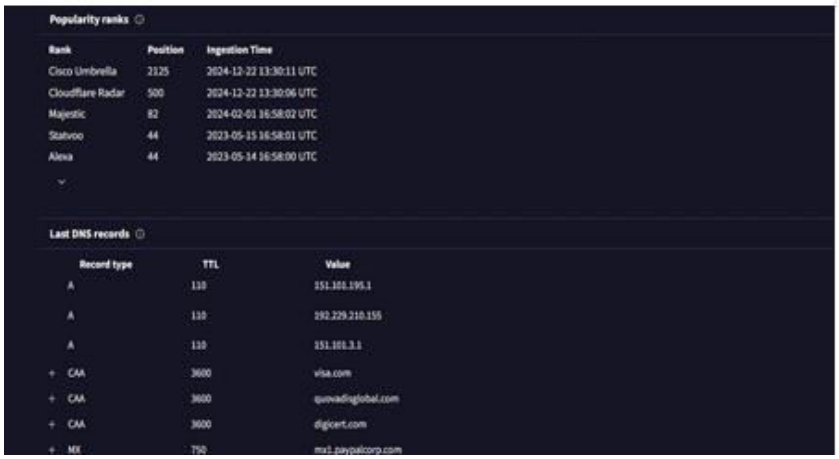


Fig 6. Domain Ranks and Records

Figure 6 provides details about the domain's popularity ranks across platforms like Cisco Umbrella, Cloudflare Radar, and Alexa, with corresponding positions and ingestion timestamps. Below, the Last DNS Records section lists DNS configurations, including A records (IP addresses), CAA records (certificate authorities), and MX records (mail servers), with their TTL (Time to Live) values and associated data. This information helps analyze the domain's network and security settings.

Fig 7. Whois Lookup

This image(fig 7) shows a Whois Lookup for the domain "paypal.com," detailing administrative information such as the admin country (US), organization (PayPal Inc.), and creation date (1999-07-15). It also includes the DNSSEC status (signedDelegation) and lists multiple domain statuses like ClientDeleteProhibited and ServerTransferProhibited, ensuring the domain's protection against unauthorized modifications or deletions.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

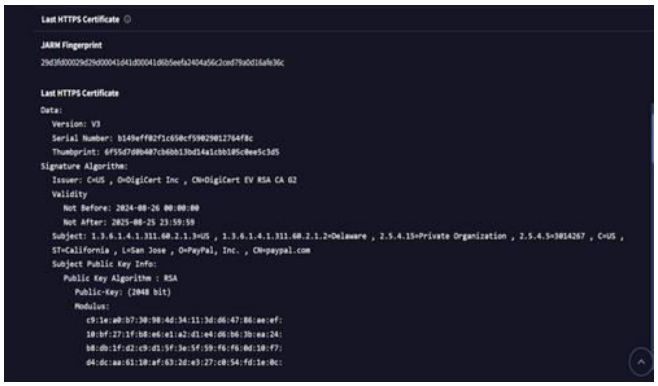
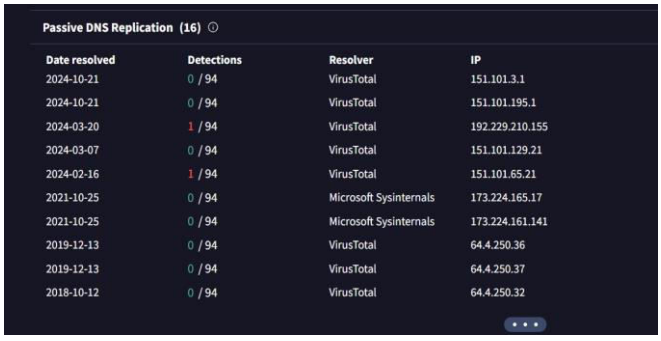


Fig 8. Https Certificate

Figure 8 provides details about the last HTTPS certificate for a domain, including the JARM fingerprint and certificate metadata. It shows the certificate's serial number, thumbprint, issuer (DigiCert Inc.), and its validity period (from 2023-08-28 to 2025-09-29). Additionally, it specifies the RSA public key algorithm, including a 2048-bit public key modulus, ensuring secure encryption for the domain.

Fig 9. Search Graph

This image(fig 9) displays a graphical network visualization of relationships for the domain "paypal.com," showing connections with communicating files, subdomains, and historical certificates. On the left, basic properties like creation date (1999-07-15) and the last update (2024-10-08) are listed, along with counts for associated files and subdomains. This representation aids in analyzing the domain's ecosystem and identifying potential threats or patterns.



Passive DNS Replication (16)

Date resolved	Detections	Resolver	IP
2024-10-21	0 / 94	VirusTotal	151.101.3.1
2024-10-21	0 / 94	VirusTotal	151.101.195.1
2024-03-20	1 / 94	VirusTotal	192.229.210.155
2024-03-07	0 / 94	VirusTotal	151.101.129.21
2024-02-16	1 / 94	VirusTotal	151.101.65.21
2021-10-25	0 / 94	Microsoft Sysinternals	173.224.165.17
2021-10-25	0 / 94	Microsoft Sysinternals	173.224.161.141
2019-12-13	0 / 94	VirusTotal	64.4.250.36
2019-12-13	0 / 94	VirusTotal	64.4.250.37
2018-10-12	0 / 94	VirusTotal	64.4.250.32

Fig 10. Passive DNS Replications

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This figure shows a Passive DNS Replication table, listing DNS resolution events for a domain, including resolution dates, IP addresses, and detection counts (e.g., 1/94 detections indicate low risk). Resolvers like VirusTotal and Microsoft Sysinternals are used to track changes in DNS records over time. This data helps identify potential anomalies or malicious activity associated with the domain's DNS history.

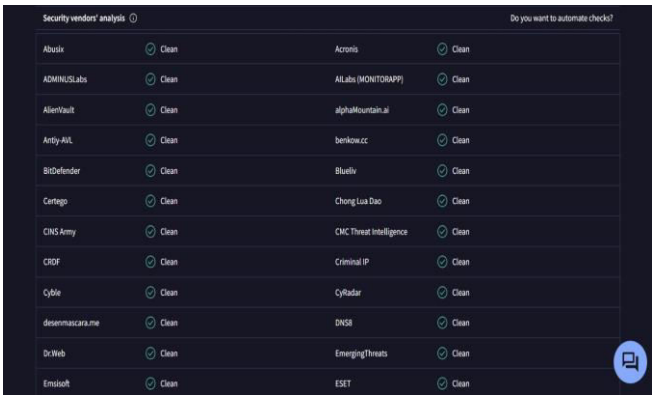


Fig 11. Security Vendor Analysis

Figure 11 shows a Security Vendors' Analysis table, listing multiple security platforms like Acronis, BitDefender, and EmergingThreats, all marking the domain as "Clean." This indicates no malicious activity or threats were detected by any of the vendors. The analysis provides assurance about the domain's safety and reliability.

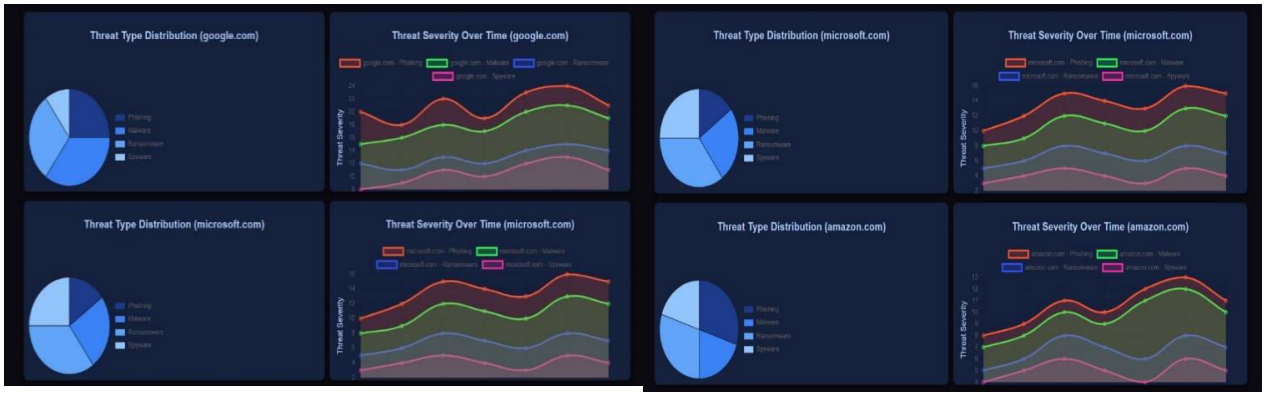


Fig 12. Pie chart and Line chart for each domain analysis

This figure compares Threat Type Distribution and Threat Severity Over Time across multiple domains, including Microsoft, Amazon, and Google. Pie charts display the proportion of threat types like phishing, ransomware, and spyware, while line graphs show the severity trends for each type over time. This visualization helps assess domain-specific threat patterns and their evolution.

VI. CONCLUSION

The Threat Intelligence Dashboard stands as a powerful tool that integrates real-time data with advanced visualization techniques to create a comprehensive cybersecurity solution. By consolidating threat intelligence across multiple domains, it breaks down barriers caused by isolated and fragmented threat analysis, delivering a unified and insightful view of potential vulnerabilities. This holistic approach not only provides organizations with a clear understanding of their cybersecurity posture but also equips them with the ability to make informed, data-driven decisions on mitigating risks. The dashboard's seamless interface, with a blend of pie charts, line graphs, and detailed tables, ensures that both

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

technical and non-technical stakeholders can access crucial threat intelligence at various levels of granularity[7].The design incorporates modern web technologies, leveraging Flask for the backend and Chart.js for data visualization, ensuring a robust and scalable architecture. The modular nature of the platform allows for future expansions, making it an adaptable solution that can grow with the changing needs of organizations and the evolving threat landscape. Its user-friendly interface, paired with real-time updates, provides an ideal balance between aesthetics and functionality, making threat monitoring both efficient and engaging.Furthermore, the lessons learned from this project have illuminated key principles for effective threat intelligence: the value of diverse visualization techniques, the need for a flexible and scalable design, and the crucial role of integrating real-time data to stay ahead of emerging threats. The potential for advanced analytics, such as machine learning-driven predictive models, offers an exciting avenue for further enhancing the platform's capabilities, enabling proactive threat detection and response.

REFERENCES

1. Orchestrating Collaborative Cybersecurity: A Secure Framework for Distributed Privacy-Preserving Threat Intelligence Sharing - Trocoso-Pastoriza, Juan & Mermoud, Alain & Bouyé, Romain & Marino, Francesco & Bossuat, Jean-Philippe & Lenders, Vincent & Hubaux, Jean-Pierre. (2022). Orchestrating Collaborative Cybersecurity: A Secure Framework for Distributed Privacy-Preserving Threat Intelligence Sharing. 10.48550/arXiv.2209.02676.
2. SeCTIS: A Framework to Secure CTI Sharing- Arikkat, Dincy & Cihangiroglu, Mert & Conti, Mauro & Rehiman K A, Rafidha & Nicolazzo, Serena & Nocera, Antonino & Vinod, P.. (2024). SeCTIS: A Framework to Secure CTI Sharing. 10.48550/arXiv.2406.14102.
3. Distributed Security Framework for Reliable Threat Intelligence Sharing- Preuveneers, Davy & Joosen, Wouter & Bernal Bernabe, Jorge & Skarmeta, Antonio. (2020). Distributed Security Framework for Reliable Threat Intelligence Sharing. Security and Communication Networks. 2020. 1-15. 10.1155/2020/8833765.
4. Towards an Evaluation Framework for Threat Intelligence Sharing- Bauer, Sara & Fischer, Daniel & Sauerwein, Clemens & Latzel, Simon & Stelzer, Dirk & Breu, Ruth. (2020). Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. 10.24251/HICSS.2020.239.
5. A Trusted, Verifiable, and Differential Cyber Threat Intelligence Sharing Framework Using Blockchain - K. Dunnett, S. Pal, G. D. Putra, Z. Jadidi and R. Jurdak, "A Trusted, Verifiable and Differential Cyber Threat Intelligence Sharing Framework using Blockchain," 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, 2022, pp. 1107-1114, doi: 10.1109/TrustCom56396.2022.00152. keywords: {Measurement;Privacy;Information sharing;Software;Cyber threat intelligence;Blockchains;Security;CyberThreatIntelligence;Sharing Information;Privacy;Trust;Verifiability;Accountability;Blockchain},
6. Efficient Collective Action for Tackling Time-Critical Cybersecurity Threats - Sebastien, Gillard & Percia David, Dimitri & Mermoud, Alain & Maillart, Thomas. (2023). Efficient collective action for tackling time-critical cybersecurity threats. Journal of Cybersecurity. 9. 10.1093/cybsec/tyad021.
7. Rethinking Information Sharing for Actionable Threat Intelligence - Mohaisen, David & Al-Ibrahim, Omar & Kamhoua, Charles & Kwiat, Kevin & Njilla, Laurent. (2017). Rethinking information sharing for threat intelligence. 1-7. 10.1145/3132465.3132468.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details