IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER ATTACKS MONITORING AND ANALYSIS USING POWER BI

[1]Prof. Asha, [2]Vaishnavi S, [3]Pallavi, [4]Rajeshree, [5]S Ashitha

[1]Professor, [2]Student, [3]Student, [4]Student, [5]Student

Department of Computer Science & Engineering,

Guru Nanak Dev Engineering College Bidar

Visvesvaraya Technological University, Belgavi, Karnataka, India

Abstract: Cyber attacks are getting more common these days with all the digital stuff growing so fast, networks everywhere, and services online all the time. It is kind of scary how they can mess up organizations, steal data, or just cause big problems for security. For this project, we built a system that monitors and analyses cyber attacks in real time, and we hooked it up with Power BI to make the visuals and analytics better. Since real cyber security data is super sensitive and not easy to get because of restrictions, I had to make a synthetic dataset instead. That way, it simulates real scenarios like DDoS attacks, SQL injection, cross-site scripting, brute force stuff, and port scanning. It feels realistic enough to test things out without actual risks. The dashboard uses HTML, CSS, and JavaScript, so it is interactive, and it simulates attacks dynamically. Then, the data gets processed and goes into Power BI for more advanced stuff. Dashboards there show trends, how severe attacks are, frequency, all that. It helps spot high-risk sources or vulnerable spots, and patterns that keep coming back. Some people might think real-time is enough, but mixing it with historical analytics makes it stronger for decisions. The system is meant to scale up if needed, run efficiently, and teach people about attacks. Cyber security analysts, students like me, researchers, they can use it to study behaviours, get aware of situations, and make better choices. Overall, it shows visualization and BI tools together can really help understand threats, even in a simulated setup.

Keywords: Cyber security, Cyber Attack Monitoring, Power BI, Real-Time Visualization, Data Analytics, Network Security, Threat Analysis, Dashboard Analytics

INTRODUCTION

In today's rapidly evolving digital ecosystem, cyber security has become an indispensable aspect of modern information technology infrastructure. The exponential growth of online transactions, cloud computing, and IoT-based devices has exposed organizations and individuals to a wide range of cysber threats. These threats are not limited to large corporations but extend to small businesses, government agencies, and personal systems as well. Common types of attacks such as Distributed Denial of Service (DDoS), SQL Injection, Cross-Site Scripting (XSS), Ransom ware, and Brute Force attacks cause significant damage by disrupting operations, stealing sensitive information, and undermining system integrity. The increasing sophistication and frequency of such attacks highlight the urgent need for effective monitoring, detection, and3 visualization tools. Traditional security systems and firewalls generate large amounts of raw log data, which are difficult to interpret manually and often delay response time. To overcome these limitations, data analytics and visualization technologies are now being leveraged to gain insights into network behaviour

and potential threats in real time. This project, titled "Cyber Attacks Monitoring and Analysis Using Power BI", focuses on developing a real-time visualization system that enables users to monitor and analyse cyber threats efficiently. The proposed system combines web technologies such as HTML, CSS, and JavaScript with Power BI analytics to create an interactive dashboard that dynamically displays simulated cyber-attack data. Through visual representation of attack frequency, type, source, and severity, the system enhances understanding and enables faster decision-making. This integration of data analytics with cyber security monitoring demonstrates how visualization tools can transform raw data into actionable intelligence, thereby strengthening an organization's overall defence mechanism.

LITERATURE REVIEW

The literature reviewed in this project shows a steady and increasing focus on cyber security monitoring, visualization, and data analytics. Over the years, researchers have worked to build smart systems that can quickly detect, analyse, and visualize cyber threats in real time. Redino et al. (2022) proposed a new deep-learning approach for detecting zero-day threats using graph and flow-based telemetry. Their dual-auto encoder model achieved near real-time detection with high accuracy and low false positives, demonstrating how artificial intelligence can improve traditional security systems. Similarly, Milajerdi et al. (2018) introduced HOLMES, a real-time system designed to identify Advanced Persistent Threats (APTs) by correlating suspicious information flows. Their framework created interpretable graphs that helped analysts understand the stages, sequence, and potential impact of attacks, making cyber security analysis more visual and actionable.

In 2018, Böhm, Menges, and Pernul stressed the value of graph-based visual analytics for converting complex cyber threat intelligence into interactive visual formats. Their study highlighted how visual tools enhance understanding, pattern recognition, and anomaly detection. Karasavvas et al. (2021) later introduced VizAttack, an open-source visualization framework for cyber attacks that supports various data types and visual metaphors, improving real-time interpretation for analysts. Ibrahim et al. (2020) concentrated on attack graph visualization for cyber-physical systems, allowing organizations to track attack paths and pinpoint system weaknesses. Their visual analytics model simplified the identification and mitigation of vulnerabilities. In related work, Chen (2013) used a semi-Markov process for real-time network security assessment, providing a statistical model for predicting attack transitions and visualizing changing threat states.

Patel (2021) studied multi-stage network attack visualization, introducing algorithms that examine attack paths, vulnerabilities, and future risk probabilities. His method used clustering and prediction techniques to spot potential attack trends. More recent research has looked at integrating business intelligence (BI) tools and AI-driven visualization. Dilpak and Kadam (2024) published a survey on cybercrime analysis using Power BI and Generative AI, offering insights into how BI can visualize threat data and reveal regional differences in cybercrime. Sufi et al. (2025) created a GPT-driven framework using Power BI for global threat forecasting, incorporating time-series models like ARIMA for predicting trends. Practical implementations have also played a significant role. Wonder Mahembe's project featured a Power BI-based cyber attack monitoring dashboard built with MySQL and Power Query, showing how real-world data can become actionable insights. Sharma and Jain (2023) developed an AI-based cyber threat visualization system combining machine learning algorithms like Random Forest with Power BI to present real-time intrusion detection results. Gupta et al. (2022) introduced a hybrid intrusion detection system that merged ML models with visualization tools such as Kibana and Power BI for a clearer understanding of attack vectors. Mehta et al. (2020) applied big data analytics and BI tools for efficiently managing large-scale cyber threat data. Kumar et al. (2021) proposed a deep learning prediction framework that used LSTM networks for proactive cyber attack forecasting, visualized through Power BI dashboards. Finally, Das et al. (2024) created a cloud-integrated Power BI visualization model that gathered data from Azure SQL and AWS RDS to analyse enterprise-level attacks.

Overall, these studies suggest that the future of cyber security relies on combining artificial intelligence, data analytics, and business intelligence visualization. By merging automated detection systems with interactive dashboards, organizations can achieve real-time awareness and respond quickly to threats. These insights provide the foundation for the current project, which aims to develop an interactive web-based system that can simulate, analyse, and visualize cyber attacks using Power BI integration for better monitoring and decision-making.

3. PROPOSED SYSTEM

The proposed system monitors and analyzes cyber attack data using Power BI dashboards. Security datasets such as network logs, intrusion records, and attack reports are collected and preprocessed. The cleaned data is imported into Power BI, where interactive dashboards are designed to display attack types, attack frequency, affected systems, and time-based trends.

4. METHODOLOGY

This project uses a structured method that combines web development, data simulation, and analytical visualization to build a real-time cyberattack monitoring system. The main goal is to create an application that simulates, records, and visualizes different types of cyberattacks through a user-friendly web interface integrated with Power BI for detailed analysis.

The system aims to tackle significant challenges in interpreting cybersecurity data, such as large data volumes, difficulties in spotting patterns, and the lack of visualization in standard tools. By merging front-end web technologies, like HTML, CSS, and JavaScript, with analytical visualization tools, the system effectively turns raw network data into useful insights.

The development process follows the Waterfall Model and includes these stages:

Requirement Analysis:

The project starts by identifying functional and non-functional requirements, such as attack simulation, data logging, and visualization needs. At this stage, tools like Chart.js, Power BI, and modern browsers are chosen.

System Design:

The system architecture outlines the logical flow between data generation, processing, and visualization. The web interface is designed for real-time display while Power BI manages historical trend analysis and detailed visual insights.

Implementation:

The system is built using HTML, CSS, and JavaScript for front-end development. The application dynamically simulates attacks using JavaScript logic and updates the display in real time. The Power BI component is included for external data analysis and reporting.

Testing and Evaluation:

Various test cases are used to confirm that the system works as intended. The charts, dashboards, and data tables are checked for accuracy, responsiveness, and consistency.

Deployment:

The final project is run using VS Code and can operate with the Live Server extension or in a Node.js environment. The Power BI report can be linked online or integrated through an API.

This organized methodology guarantees smooth project execution, maintainability, and ease of future improvement.

4.2 EXISTING SYSTEM

In traditional cybersecurity monitoring environments, organizations mainly rely on manual log analysis, command-line tools, or commercial monitoring solutions to detect and respond to threats. These systems generate large amounts of unstructured data that security professionals must interpret. Consequently, incident response can be slow and prone to errors.

Existing systems, like traditional SIEM (Security Information and Event Management) platforms, gather event data but require costly infrastructure, licensing fees, and expert knowledge. Smaller organizations, educational institutions, and students often cannot afford or use these tools effectively.

Limitations of the Existing System:

- Lack of Real-Time Visualization: Most systems show static logs or delayed updates, making it hard to respond quickly to threats.
- Complex Interfaces: Security professionals need specialized training to operate SIEM tools.
- Limited Accessibility: Many tools are not easily deployable on web browsers or low-end systems.
- Poor Interpretability: Identifying attack patterns and event relationships is difficult without visualization.
- Cost and Scalability Issues: High licensing fees and system requirements make enterprise tools inaccessible for smaller users.

Due to these limitations, there is a need for a lightweight, real-time, visualization-driven system that helps users, including students and entry-level professionals, intuitively understand and monitor attack behavior.

4.3 PROPOSED SYSTEM

The proposed system, titled "Cyber Attacks Monitoring and Analysis Using Power BI," offers a modern, web-based visualization platform that can simulate and monitor cyberattacks in real time. It combines front-end web technologies (HTML, CSS, JavaScript) with data visualization tools (Chart.js and Power BI) to provide an interactive dashboard that updates continuously.

The project simulates various attack types, including DDoS, SQL Injection, Cross-Site Scripting (XSS), and Brute Force, to show how different cyber threats behave. These attacks are illustrated on line charts and data tables with corresponding timestamps, source IP addresses, and severity levels.

Features of the Proposed System:

- Real-Time Simulation: The system generates and updates simulated attack data every few seconds.
- Visualization Dashboard: Displays attack frequency, sources, and severity using line charts and tables.
- User Controls: Allows users to pause, reset, or adjust the speed of data generation.
- Power BI Integration: Provides a separate analytical layer for trend visualization and business intelligence.
- Accessibility: Works directly in web browsers without needing to install additional heavy software.
- Scalability: Can be expanded to integrate real-world data from APIs or log servers.

System Workflow:

- Attack Simulation: Random events are generated using JavaScript. Each event contains parameters like attack type, source IP, severity, and timestamp.
- Data Storage and Processing: The simulated data is temporarily stored in arrays and continuously updated.
- Visualization: Chart.js dynamically refreshes the visual charts based on the latest data.
- Power BI Dashboard: The Power BI report, when embedded, presents advanced analytics, including attack distribution and trends.

This proposed method improves situational awareness and helps train users to interpret attack data visually, making cyber security analytics more approachable and understandable.
The methodology can be understood in a following way:
Step 1: Collect cyber security datasets from logs or public sources.
Step 2: Clean and preprocess data using Excel or Python.
Step 3: Import processed data into Power BI.
Step 4: Create visualizations such as bar charts, line graphs, pie charts, and maps.
Step 5: Analyze dashboards to identify attack patterns and trends.
Step 6: Generate reports for decision-making.

5. IMPLEMENTATION

The system is implemented using Microsoft Power BI Desktop. Datasets are connected using CSV or Excel files. DAX functions are used for calculated measures and filtering. Dashboards include visuals for attack distribution, time-series analysis, and severity levels. The system was implemented using a modular approach. This ensured that each component, such as data simulation, visualization, Power BI integration, and reporting, was developed, tested, and verified individually before integrating them into the final setup. We used Visual Studio Code (VS Code) as the primary Integrated Development Environment (IDE) for the entire project.

The main technologies used in the system include:

- Front-End: HTML5, CSS3, JavaScript
- Data Handling & Visualization: Chart.js, Power BI Embedded Dashboard
- Backend / Database (optional for expansion): MongoDB or JSON files for data storage
- Visualization Tools: Microsoft Power BI
- Platform Used: Web browser-based environment

Each module serves a specific purpose, from generating simulated attack data to analyzing patterns through interactive dashboards. The Power BI component allows for improved visualization and analytical computation, while the front end ensures user interactivity and engagement.
Power BI integration is a key feature of this project. Once we generate and process the simulated data, we export it to a CSV or JSON file that connects to Power BI. This tool helps create interactive dashboards and reports, displaying:

- Total number of attacks by type
- Attack frequency by time
- Severity-level distribution
- High-risk IP addresses
- Time-series trends for attacks

To integrate Power BI with the web application, we used Power BI Embedded. We embedded the Power BI report link, generated after publishing the report to Power BI Service, into an <iframe> in the HTML code. This allows users to interact with the Power BI dashboard directly within the web interface without switching platforms. To ensure real-time up dates, we configured Power Query in Power BI to refresh data at intervals. This makes certain that the newly generated simulated data appears immediately in the analytical dashboards.

The entire project was implemented and tested in **Visual Studio Code**, ensuring smooth execution and modular coding structure. Below is a simplified example of the code structure:

File Structure:

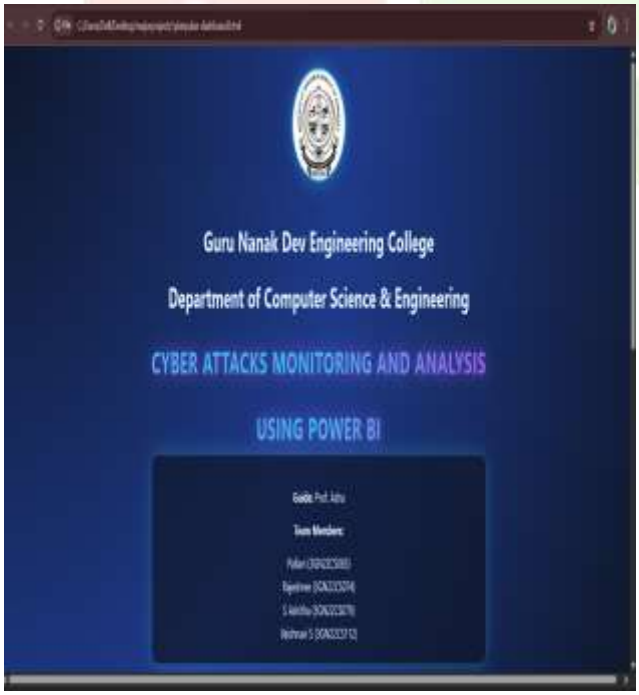
File Structure:

pgsql

```
/CyberAttackDashboard
|
├── index.html
├── style.css
├── script.js
├── data/
|   ├── attacks.json
|   └── processed.csv
└── assets/
    └── icons, images
```

6. RESULTS AND ANALYSIS

The Power BI dashboards provide clear insights into cyber attack trends. Results show frequent attack types, peak attack times, and vulnerable systems. Visual analysis helps security teams quickly identify anomalies and respond effectively. The system improves monitoring efficiency compared to traditional log-based analysis.



7. ADVANTAGES

- Real-time and interactive visualization
- Easy identification of attack trends
- Improved decision-making
- User-friendly dashboards
- Reduced analysis time

8. LIMITATIONS

- Depends on quality of input data
- Limited real-time capability without live data sources
- Requires Power BI expertise

9. FUTURE SCOPE

Future enhancements include real-time data streaming, integration with SIEM tools, machine learning-based attack prediction, and automated alert generation.

10. CONCLUSION

Cyber Attacks Monitoring and Analysis Using Power BI provide an effective approach to visualize and analyze cyber security data. The system enhances threat awareness, supports faster incident response, and strengthens organizational security. Power BI proves to be a powerful tool for cyber security analytics. The project “Cyber Attacks Monitoring and Analysis Using Power BI” achieved its goal of creating a real-time, interactive system for monitoring, simulating, and analyzing cyberattacks. By combining web development technologies like HTML, CSS, and JavaScript with analytical visualization tools such as Power BI, the system offered an efficient platform for live monitoring and thorough data analysis. The simulated environment generated various attack types, including DDoS, SQL Injection, XSS, Port Scanning, and Brute Force. Each attack was represented with parameters like timestamps, severity levels, and IP addresses. These attacks were visualized dynamically using Chart.js, which ensured real-time updates without delays or data loss. The integration with Power BI allowed users to gain insights through interactive dashboards, displaying attack frequency, distribution, and severity patterns over time. Graphs and metrics helped identify high-risk sources, detect recurring patterns, and assess overall vulnerabilities in the system. The project performed well during testing, confirming its ability to handle large amounts of data efficiently. In

conclusion, this project shows the strong connection between cybersecurity analytics and business intelligence tools. It provides a practical, educational, and research framework for understanding cyber threats. Additionally, it lays the groundwork for future improvements, such as adding machine learning models for predicting attacks, connecting with live intrusion detection systems, and deployment in security operation centers (SOCs) for real-world cybersecurity monitoring.

References

- Redino, C. et al. (2022). Zero Day Threat Detection Using Graph and Flow-Based Security Telemetry. arXiv Preprint.
- Böhm, F., Menges, F., & Pernul, G. (2018). Graph-based Visual Analytics for Cyber Threat Intelligence. SpringerOpen.
- Dilpak, V., & Kadam, A. J. (2024). A Survey on Cyber Crime Analysis System: Leveraging Power BI and Generative AI for Comprehensive Insights. IJARESM.
- Sufi, D. et al. (2025). Quantifying Temporal Dynamics in Global Cyber Threats: A GPT-Driven Framework for Risk Forecasting and Strategic Intelligence. MDPI.