IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13358

Cyber Insurance Risk Assessment Tool

Prithivi Raaj P[1], Dr. P. Menaka[2]

Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore[1]

Associate Professor, Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore[2]

Abstract: This project presents a Cyber Insurance Risk Assessment Tool designed to evaluate the cybersecurity risk level of organizations and support cyber-insurance decision-making. The system collects information related to security practices, vulnerabilities, incident history, and organizational assets through a structured assessment process. Based on the collected data, the tool computes an overall cyber risk score and classifies the risk level as low, medium, or high. The application provides a user-friendly dashboard that visualizes risk scores, risk trends, and estimated financial impact of cyber incidents. It also recommends suitable insurance coverage ranges and generates detailed assessment reports for organizations and insurers. By combining risk scoring techniques and optional machine learning-based predictions, the tool helps organizations understand their cyber risk posture and assists insurers in making data-driven premium and coverage decisions. The proposed system improves transparency, accuracy, and efficiency in cyber risk evaluation and cyber insurance assessment.

Keywords: Cyber Insurance, Cyber Risk Assessment, Cybersecurity, Risk Scoring, Risk Management

I. INTRODUCTION

With the rapid growth of digital technologies, organizations increasingly depend on computer networks and online systems to store and process sensitive information. This has led to a significant rise in cyber threats such as data breaches, phishing attacks, ransomware, and system intrusions. These cyber incidents can cause serious financial losses, legal issues, and damage to an organization's reputation.

Cyber insurance has emerged as an important solution to help organizations manage the financial impact of cyber attacks. However, assessing cyber risk accurately is a major challenge for both organizations and insurance providers. Many current methods rely on manual evaluation and general checklists, which may be time-consuming, inconsistent, and subjective.

The **Cyber Insurance Risk Assessment Tool** aims to provide an automated and systematic approach to evaluate an organization's cybersecurity risk level. The system collects security- related information, analyzes risk factors, calculates a cyber risk score, and presents the results through a user-friendly dashboard. It also generates detailed reports and suggests suitable insurance coverage based on the assessed risk level. This project helps organizations understand their cyber risk posture and supports insurers in making data-driven decisions for cyber insurance coverage.

II. LITERATURE REVIEW

Cyber risk assessment and cyber insurance have become critical research areas due to the growing number of cyber threats targeting organizations of all sizes. Many studies and frameworks focus on evaluating cybersecurity posture and identifying vulnerabilities:

[1]. Cyber risk framework:

Researchers and standard organizations such as the NIST Cybersecurity Framework and ISO/IEC 27005 describe structured approaches for identifying, analyzing, and evaluating risk in information systems. These frameworks provide guidelines for risk identification and mitigation but do not directly focus on insurance assessment.

[2]. Cyber insurance research:

Studies on cyber insurance explore the economic and actuarial aspects of cyber risk modeling. For example, work by Biener et al. (2015) and researchers in risk management journals discuss the challenges of quantifying cyber risk for pricing insurance premiums. These studies highlight the need for accurate data-driven risk quantification to support insurers.

[3]. Automated Risk Tools:

Various software tools and academic projects implement automated cybersecurity assessment engines using vulnerability assessment, threat modeling, and risk scoring. Tools often use metrics or machine learning models to identify potential weaknesses and compute risk ratings. However, many of these focus primarily on technical risk scores

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13358

(based on system vulnerabilities) and not on translating those scores into insurance decision-making metrics.

Overall, literature in this domain emphasizes risk quantification, technical cybersecurity assessment, and theoretical insurance models, but a comprehensive tool combining all these elements into a practical **insurance assessment interface** remains less explored.

Research gap: Existing cyber risk assessment methods mainly focus on technical vulnerabilities and do not directly support cyber insurance decision-making. Current systems are often manual, time-consuming, and lack standardized risk scoring linked to insurance coverage or premium estimation. There is limited integration of predictive analytics and visual dashboards tailored for insurers and organizations. Hence, an automated and insurance-focused cyber risk assessment tool is needed.

III. PROBLEM STATEMENT

Organizations face increasing cyber threats that can cause serious financial and operational losses. However, accurately assessing cyber risk for insurance purposes is difficult because current methods are often manual, inconsistent, and based on limited technical checklists. Insurers and organizations lack a standardized, automated system to evaluate cyber risk, predict potential impact, and generate clear reports for insurance decision-making. This results in inefficient risk evaluation and inaccurate insurance coverage planning.

IV. METHODOLOGY

[1]. User Registration & Authentication

Users (Organizations / Insurers / Admin) register and log in securely. Role-based access control ensures only authorized users can access specific features.

[2]. Data Collection (Assessment Input)

The system collects structured inputs such as:

- Organization details (size, sector, assets)
- Security controls (firewalls, antivirus, backups, policies)
- Vulnerabilities and compliance status
- Past cyber incident history

[3]. Data Preprocessing & Validation

- Check for missing or incorrect inputs
- Normalize data into standard formats
- Convert questionnaire responses into numerical values for scoring

[4]. Risk Factor Analysis

- Analyze key factors: Threat likelihood, Vulnerability level, Asset criticality, and Potential impact
- Assign weights to each factor based on importance

[5]. Risk Scoring Algorithm

- Apply a weighted risk scoring formula to calculate overall cyber risk
- Classify risk into **Low / Medium / High** categories

[6]. Dashboard & Visualization

- Display risk scores, trends, and comparison charts
- Show estimated loss and recommended insurance coverage range

[7]. Report Generation & Recommendations

- Generate downloadable assessment reports
- Provide security improvement recommendations based on risk areas

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13358

[8]. Admin Monitoring & Management

- Admin manages users, assessment templates, and system data
- Monitor system usage and update risk scoring rules if needed

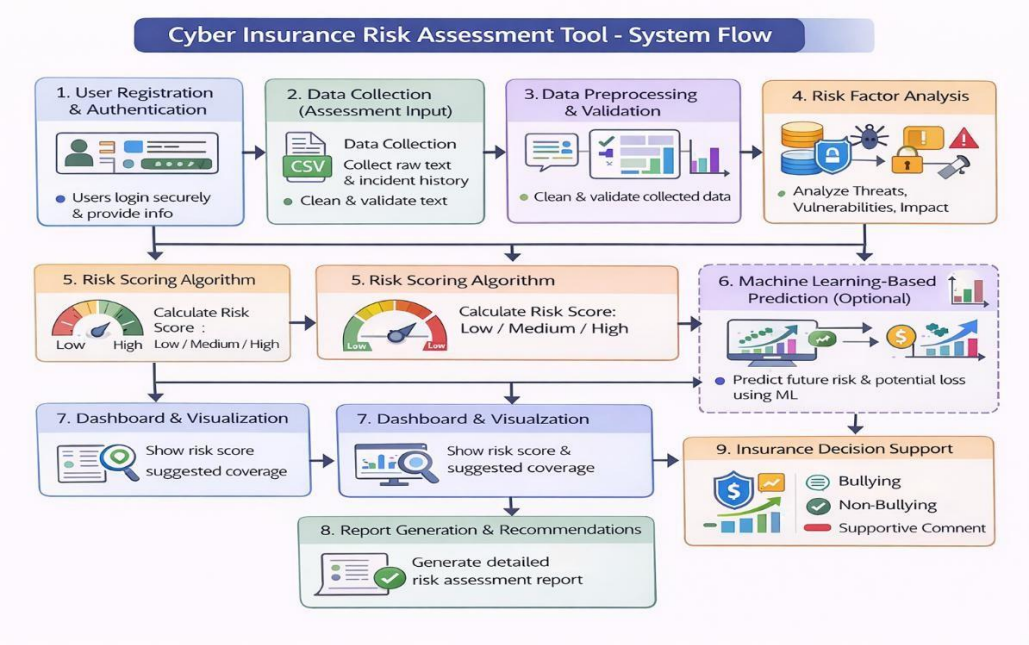

Fig:1.1: System Flow Diagram

V. PERFORMANCE AND EVALUATION

The performance of the Cyber Insurance Risk Assessment Tool is evaluated based on how accurately it analyzes security inputs, generates meaningful risk scores, and supports cyber insurance decisions. The evaluation focuses on correctness, consistency, speed, and usability of the system.

Evaluation Criteria

[1]. Risk Classification Accuracy

Checks whether organizations are correctly grouped into Low, Medium, or High risk.

[2]. Consistency of Risk Scores

Ensures similar security inputs produce similar risk scores, showing stable assessment behavior.

[3]. Processing Speed

Measures the time taken to calculate the risk score and display results on the dashboard.

[4]. System Reliability

Evaluates system stability during multiple user assessments without failures.

[5]. Usability & Decision Support

Checks ease of use of forms, dashboards, and usefulness of generated reports. The cyber risk score is calculated using key risk factors:

Risk Score = (Threat Level + Vulnerability Level + Impact Level) ÷ 3

Where:

- Threat Level → likelihood of cyber attacks
- Vulnerability Level → weaknesses in security controls
- Impact Level → potential damage if attack occurs

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13358

VI. RESULT AND DISCUSSION

Results

The Cyber Insurance Risk Assessment Tool was tested using different sample organizational profiles with varying security practices and risk factors. The system successfully collected user inputs, calculated cyber risk scores, and classified organizations into Low, Medium, and High risk levels. The dashboard displayed the results clearly, and assessment reports were generated correctly for each evaluation.The system produced consistent risk scores for similar inputs and completed the assessment process quickly. The visualization features such as charts and summaries helped users easily understand their cyber risk level and potential impact. The report generation feature provided structured outputs that can be used for cyber insurance planning and documentation.

Discussion

The results show that the proposed system provides a reliable and automated way to assess cyber risk compared to manual and checklist-based methods. It reduces human effort, improves consistency in risk evaluation, and helps organizations better understand their security posture for insurance purposes.However, the accuracy of the results depends on the correctness of the input data provided by users. Since the system is based on predefined scoring rules and weights, it may not capture real-time threat changes. The system can be further improved by adding real-time risk updates and more detailed assessment parameters in the future

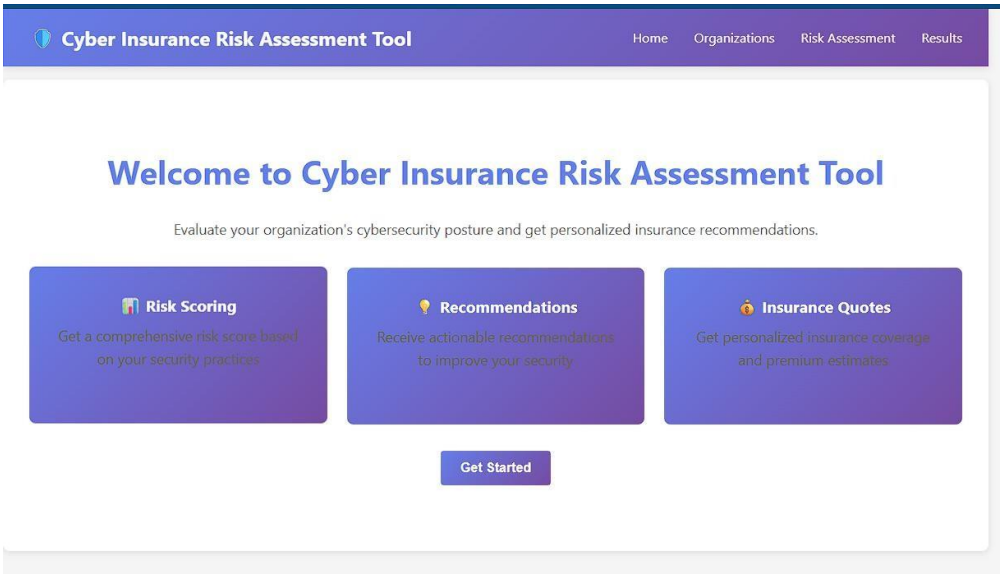

Fig 1.2: Home Page

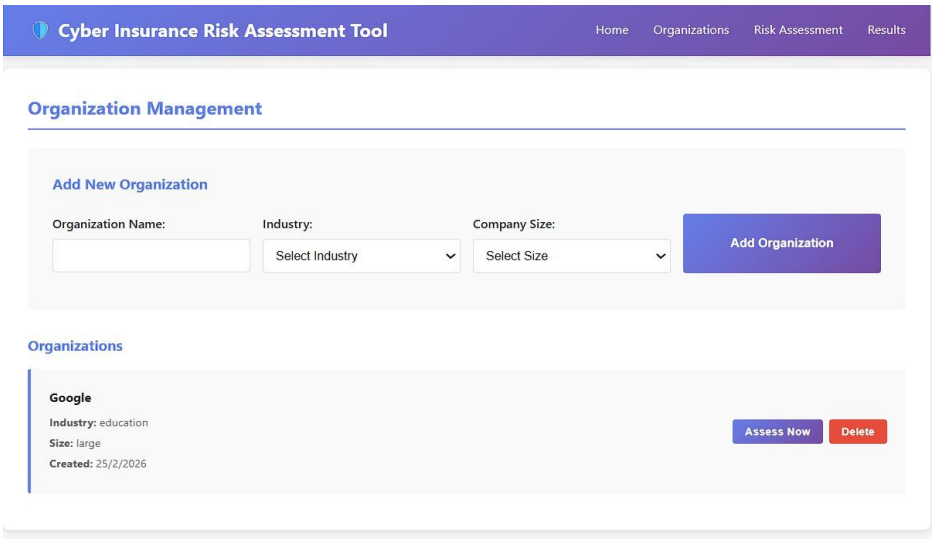

Fig 1.3: Organization Management

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13358

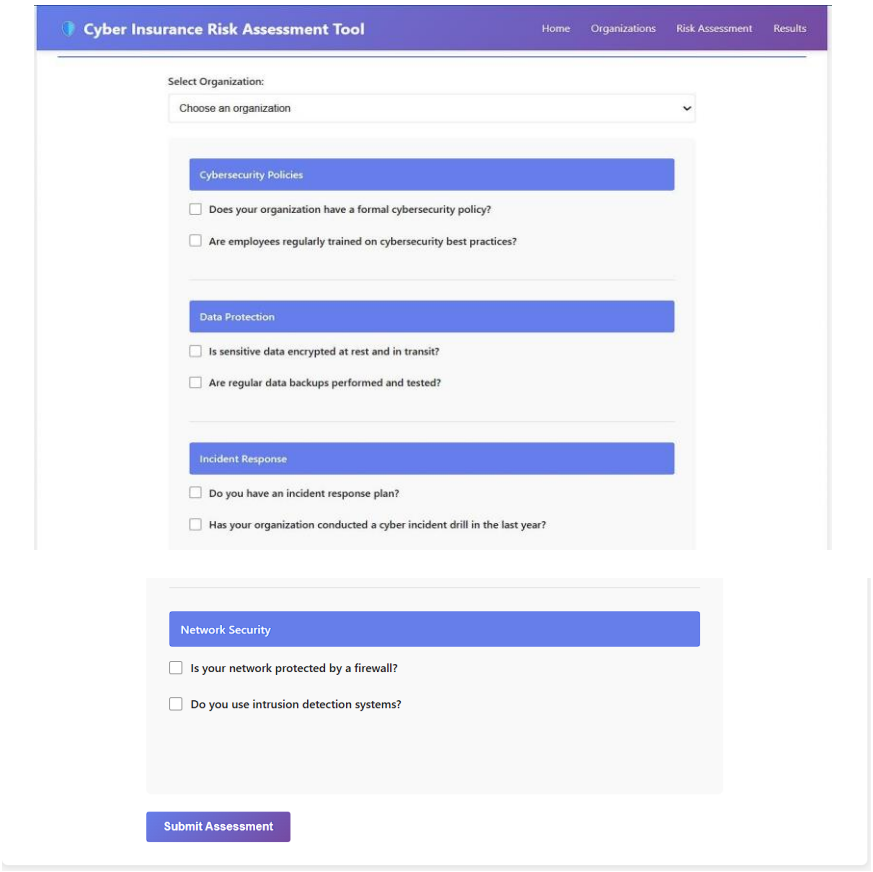

Fig 1.4: Risk assessment

VII. FUTURE WORK

In the future, the Cyber Insurance Risk Assessment Tool can be enhanced by integrating real-time cyber threat information to provide more up-to-date risk scores. Additional risk factors such as cloud security, network configuration, and third-party risks can be included to improve the accuracy of assessment. The system can be connected with existing security tools to automatically collect security data instead of relying only on manual inputs. Further improvements may include providing more detailed and customizable insurance recommendations, adding mobile application support for easier access, and improving report formats with comparison and export features for better analysis and decision-making.

VIII. CONCLUSION

The Cyber Insurance Risk Assessment Tool provides an effective and automated way to evaluate the cyber risk level of organizations. By collecting security-related inputs and applying structured risk scoring methods, the system helps classify organizations into low, medium, or high risk categories. The user-friendly dashboard and report generation features make it easier for organizations and insurers to understand cyber risk and support insurance decision-making. Overall, the project reduces manual effort, improves consistency in risk assessment, and offers a practical solution for cyber risk evaluation in the context of cyber insurance.

REFERENCES

[1]. National Institute of Standards and Technology
NIST Cybersecurity Framework — Year: 2018 (v1.1) Pages: Framework document (no fixed page numbers for citation)

[2]. International Organization for Standardization
ISO/IEC 27005: Information Security Risk Management — Year: 2018 Pages: Standard document (page numbers vary by edition)

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13358

[3]. OWASP
OWASP Top 10 – Web Application Security Risks — Year: 2021 Pages: Online report (no fixed page numbers)
[4]. ENISA
Cybersecurity Risk Management Guidelines — Year: 2016–2023 (various reports) Pages: Report-based (no fixed page numbers)
[5]. SANS Institute
Cybersecurity Best Practices — Year: Ongoing publications Pages: Whitepapers/articles (no fixed page numbers)
[6]. Verizon
Data Breach Investigations Report (DBIR) — Year: Annual (e.g., 2023) Pages: Report-based (no fixed page numbers)