National College of Ireland

AI-Driven Automated Cyber Risk Assessment Pipeline for GRC Intelligence – A Tripartite Framework

MSc Research Project
Data Analytics

Kaviya Maniyan
Student ID: x23377879

School of Computing
National College of Ireland

Supervisor: Prof. Arjun Chikkankod

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	KAVIYA MANIYAN
Student ID:	X23377879@student.ncirl.ie
Programme:	M.Sc. Data Analytics **Year:** 2025-2026
Module:	Research Practicum
Supervisor:	Prof. Arjun Chikkankod
Submission Due Date:	28-01-2026
Project Title:	AI-Driven Automated Cyber Risk Assessment Pipeline for GRC Intelligence – A Tripartite Framework
Word Count:	6602 **Page Count** 18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Kaviya Maniyan

Date: 28/01/2026

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI-Driven Automated Cyber Risk Assessment Pipeline for GRC Intelligence – A Tripartite Framework

Kaviya Maniyan

x23377879

Abstract

In this digital era, cybersecurity risk management became a crucial challenge that should be addressed as soon as possible to avoid more dangerous effects. Every year thousands of new vulnerabilities are released, yet organizations struggle to interpret, disclose and understand how these threats relate to specific attack behaviors and compliance controls. Most of the studies were dependent on small sampling, CVSS metrics and rule-based approaches. This research proposes a novel AI-driven tri-partite (CVE→ MITRE → NIST) automation framework by developing hybrid machine learning and deep learning models to classify CVE vulnerabilities as well as rule-free embeddings. Sentence-BERT was used to embed descriptions (text) of all three datasets and to train a hybrid MLP that achieved ~82% accuracy, ~0.72 macro F1 across the long NVD test cases. Cosine similarity has been generated for CVE → MITRE, MITRE → NIST, CVE → NIST mapping to rank top k exploitation and mitigation knowledge. A visual tri-partite knowledge graph using NetworkX was created and an interactive assistant was trained, which inputs both CVE IDs and free-text vulnerability description that maps them with top k NIST and MITRE frameworks it also provides standard NIST controls (top 3) to each attack technique. Therefore, this proposed system transforms raw information into GRC intelligence in seconds rather than traditional methods.

1 Introduction

1.1 Background and Context of the Problem

In recent years, threats like cybersecurity vulnerabilities are increasing, attacks are becoming more common and dangerous because everything is interconnected with each other. This leads to financial, operational and reputational risks, so handling them with appropriate methods becomes challenging for all organizations. Thousands of new Common vulnerabilities and Exposures are reported in National Vulnerability Database (NVD) – a public repository of vulnerability entries (Grigorescu et al., 2022). Even in this digital era, organizations still struggle to understand which is the most severe vulnerability, what are the possible attack techniques that can be used for exploitation, and what are the necessary defensive controls that can be implemented to avoid risk as well as lacks in automation procedures (Ali et al., 2025). Standards like NIST SP 800-53 Rev.5 and databases that contains adversarial knowledge – MITRE ATT&CK plays a crucial role in GRC framework which contributes to real-world mechanisms by connecting exploitation methods to policies. It has different structures, format and meaning. Recent existing studies rely heavily on

manual processes, expert knowledge and time-consuming documentation studies which make risk assessment even more challenging.

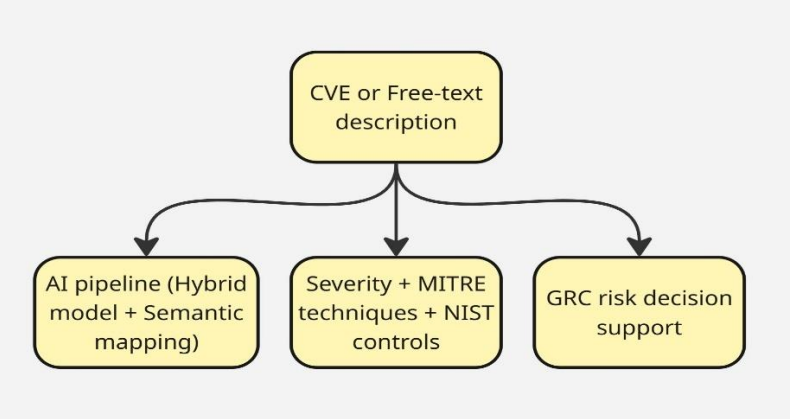

Fig1: Overview of the entire framework

1.2 Research Gap

Most of the studies have attempted to predict vulnerability severity through machine learning methods and treat them as a pure task without building a knowledge of connecting predictive outcomes to GRC frameworks (Kaur et al., 2025). And existing studies solely dependent on either structured or textual information which fails to capture the meaning and translate vulnerability outcomes into actionable guidance. This makes the security GRC teams more challenging to understand vulnerabilities and map them to attack and defensive paths.

Research Question

"To what extent does an AI-driven tri-partite CVE → MITRE ATT&CK → NIST SP 800-53 Rev.5 framework automate, improve cyber risk assessment and support GRC decision-making?"

1.3 Research Objectives

i) To evaluate vulnerable severity classification, build hybrid machine learning models using Sentence-BERT embedding and by integrating both structured CVSS attributes and textual descriptions (Carello et al., 2025).
ii) To link vulnerabilities outcomes with appropriate attack techniques and defensive security control, design an AI-based semantic embedding pipeline to map top k ranking across all three frameworks.
iii) Build an automated assistant that inputs free-text vulnerable descriptions and CVE identifiers to support real-world risk management.

1.4 Research Contribution and Justification

Building an automated tri-partite mapping across three different cybersecurity taxonomies that can convert raw vulnerability to control level mapping through rule-free Sentence-BERT semantic embeddings, and this outperforms in generalization and scalability unlike existing isolated classification and traditional manual based studies – a primary contribution of this research that fills a longstanding gap between vulnerabilities and GRC decisions with cybersecurity operations which is critical need of organizations. Existing studies fail to emerge threats and zero-day vulnerabilities by relying on some number of manual mappings, isolated analysis and constant expert contribution (Bhosale et al., 2024). The proposed framework is generalizable across unseen cases and the hybrid ML models achieved approximately 83% in accuracy and ~0.72 to ~0.74 macro F1-score and propose a production ready assistant that enables security teams to critically analyze vulnerabilities and its mapping relationships within seconds which contributes in GRC automation.

2 Related Work

This section is a literature survey conducted on recent studies to find the gap and to understand how primary studies are using different methods like manual approaches, developing machine learning models and automation pipelines to provide scalable solutions to mitigate vulnerabilities, identify threats and risks, globally as well as specifically.

2.1 Mapping Vulnerabilities Using NLP-Based Approaches with Controls

A conference study by Carello et al. (2025) proposed a semi-automatic approach between vulnerability descriptions and security controls with two distinct NLP models: Sentence-BERT, SECBERT which captures semantic similarities. This paper used 39 ENISA cloud vulnerabilities, 197 CSA Cloud controls and 399 CWE weaknesses (software development) to 52 MITRE ATT&CKS. SBET covered 90 percent of cloud vulnerabilities, SECBERT showed 64 percent accuracy. The Jaccard similarity metrics have a semantic score between 0.4 to 0.5 range which is a promising result. Elmarkez et al. (2024) provides an automation methodology using techniques like TF-IDF, Doc2vec and BERT for mapping public cybersecurity textual repositories like CAPEC, CWE and MITRE ATT&CK with NIST SP 800-53. Compared to other approach TF-IDF achieved a promising performance of 90 percent recall. To address the limitations of TF-IDF, the authors did a novel keyword boosting algorithm which improves average classification accuracy to all datasets up to 7 percent. This paper addresses a single relationship that is mapping security mitigations to control families which is a simple flat classification. Both studies lack generalization because Carello used only 39 vulnerabilities and Elmarkez approach relies on three smaller datasets (42 MITRE ATT&CK ICS, 24 CAPEC and 42 MITRE Defend mitigation entries) which shows the necessity of tri-partite contribution for a globally wide GRC compliance.

2.2 Severity and Vulnerability Classification/Prediction: ML - Based

Mapping Common Vulnerabilities and Exposures to MITRE ATT&CK yet existing approaches need manual efforts. Grigorescu et al. (2022) initiated CVE to ATT&CK also did manual expert annotations initially to map CVE to MITRE techniques which is used as a training set for BERT-based multi-label classification with 1813 CVEs and 31 ATT&CKs. This shows a result of 47.8 percent F1-score, due to insufficient training samples, nearly nine techniques are 0% F1-score. Even though the model was trained under subjective expert mappings still it leads to classification errors, also distinguishing identical or closely related attacks are way more challenging. As it is a supervised semantic similarity-based approach when it expands beyond 31 ATT&CKS the model won't be scalable for large datasets, creates a bottleneck for currency maintenance across organizations for extending manual expert findings/mappings. Lasantha et al. (2025) proposed a hybrid approach for vulnerability detection in AWS EC2 by integrating NIST and MITRE ATT&CK databases. This process is exclusively within cloud infrastructure to classify a binary classification (yes/no) on real time, lacks in detail multiple risk levels and semantic depth while integrating MITRE ATT&CK which are very important in governance, risk, and compliance. Used rule-based matching from API responses, this focus on AWS EC2 for practical value but generalizability to common vulnerabilities is absent. Kaur et al. (2025) is a literature survey of NVD vulnerabilities prediction using ML and DL, after surveying twenty papers where all the algorithms ranging from decision tress to neural network including BERT, GPT-2 and so on. It reveals Cross-Site Scripting is the most prevalent vulnerability from 2020-2025. Basically, this is a review paper where there is no practical experiments, but this work critically exposed that all surveyed papers/work mostly focus on binary classification and severity prediction without addressing how vulnerabilities can change into actionable insight for GRC.

2.3 An Assessment of Risks and Frameworks Integrations

By using ML algorithms like Random Forest, SVM plus two more Karimi and Mendez Mena (2025) provides a framework for IT/OT cyber risks by mapping VCDB's 10,000+ breaches covered by 160 attributes with 168 MITRE ATT&CK techniques. Highlights 28 high risk techniques by using Lasso regularization which informs 68 mitigation processes. Rather than pre-breach vulnerability analysis, this paper focused on post-breach metadata financial analysis without semantic embedding techniques. Therefore, this is a reactive breach framework rather than proactive vulnerability management. This shows the importance of semantic methodology and the operation on vulnerability datasets. Kryukova et al. (2024) highlights the heterogeneous system's information and the challenges of its evolution making the security asses more challenging. By systematically projecting the events with attack stages and to include an attack-based model into the infrastructure, here the authors positioned their work. By integrating both NVD vulnerability with MITRE ATT&CK tactics and techniques, the authors constructed a hierarchical attack-graph model then mapped the SIEM-detected incidents to this graph and used Targeted Attack Analyzer rules. This automatically helps to match each incident with specific ATT&CK by matching the

incident against IOA (Indicators of Attack) rule set. On top of that the paper developed a multi-level attack graph which combines attack with vulnerabilities. However, this is highly relied on rule sets: if a rule exists for a given technique, this system cannot map an incident.

2.4 The Security of both OT (Operational Technology) and ICS (Industrial Control Systems)

Bhosale et al. (2024) conducted a manual expert analysis on ICS data where this paper used Nessus scanning to map ICS control vulnerability system to MITRE ATT&CK tactics. Also constructed BBN to identify attacker's paths, calculated risk quantification for safety security purpose of OT environments. This paper maps 16 vulnerabilities to 12 ICS tactics. Fundamental limitations are manual expert analysis, absence of automation and scalability, lacks in dealing with large datasets which leads to an organization lacking in necessary detailed mitigation process and a wide range of GRC requirements for both IT and OT environments. Lopez et al. (2025) is a systematic literature survey that contributes to ICS (Industrial Control System) security by employing Shodan search engine. There are six phases including web application analysis, IP discovery, risk analysis by mapping CVSSv3 to ISO 27001 and CIS controls version 8 etc. with a Japanese ICS case study where 17 vulnerabilities were identified with an attack surface of 5.81 and risk score of 2.27 and so on. This paper reviewed nearly 64 studies from 2014 to 2024 and reveals that most research focuses on internal risk analysis and cybersecurity testing. However this study focused on internet facing ICS security on real time but did manual testing by Nmap, Telnet which lacks in automation, identifying the entire historical corpus and model development as well where all these limitations are used for risk-based decision making across various environments like IT/OT. Rotibi et al. (2025) classified 12 different cyber risk tools for ICS system and categorized them then evaluated each tool for threat, vulnerability and so on. The authors assessed alignment based on the IEC 62443, NIST SP 800-82 and ISO 27001 standards. The findings revealed that seven tools address only operational technology, and the remaining five are systematic tools which cover all architectural points and identify threats. This paper lacks in developing models for automation, integrating natural language techniques, this mainly focused on operational risk identification tools evaluation and comparison.

2.5 An Analysis of Threats and ATT&CKs

The importance of MITER ATT&CK framework has expanded to categorize threats and identify vulnerabilities in recent years. Ekisa et al (2024) mapped cyberattacks from ICS testbed with Enterprise and ICS variants. From this, the study identified 26 techniques: 15 Enterprise and 11 ICS. This highlights how different modern attacks targeting both IT and OT domains. This study gives an understanding about attack methodologies, but the mapping process is manual and qualitative within the controlled environment. It also lacks in addressing variety of attacks and challenges faced by security officers. This shows the need for scalability, automation and data-driven approach. Sada et al. (2023) showed the richness of ATT&CK knowledge by analyzing ATT&CK entries, to prevent the attacks, capture relationships of tactics, and high-level patterns to

make security patterns in a precise way. This paper quantifies and visualizes attack techniques, did correlation and clustering analysis and then identified common attack behaviors. This technique relies mostly on ATT&CK layers, structured entries and statistical work rather than sentences/texts which is a limitation for automated GRC, doesn't integrate large data and no mapping with ATT&CK techniques. Ali et al. (2025) extract tactics, techniques and procedures from threat reports by an automated process. Then submit all CTI into tools and evaluate performance which includes accuracy, freshness, relevance and completeness. By evaluating 600 IoCs the performance showed inconsistency, after adding weights VirusTotal tool showed premium performance in freshness evaluation. This paper is an evaluation of intelligence and performance of different tools, it is limited in manual reports from specific vendors, lacks in automating from low-level to high-level security.

2.6 Specialized Frameworks for Emerging Techniques

The importance of security frameworks for vulnerability threat management is increasing day by day. Karim et al. (2025) provides a framework for securing LLM's workloads within IoRT (Internet of Robotic Things) systems by applying NIST AI Risk management to map AI-threats with systematic governance functions. Numeric risk models help to assess vulnerabilities in agriculture robotics and reduce risk. Identified gaps in current NIST AI RMF, then mapped IoRT attacks to MITRE ATLAS. However, this work did manual expert analysis which limits scalability in diverse organizational context. Yulianto and Caronongan (2024) conducted a study of cybersecurity practices across organizations in Philippine. They used both quantitative & qualitative surveys and interviews. This study shows uneven security practices globally where Penetration Testins are used 80%, Bug Bounty 20%, which is limited, Vulnerability Disclosure methods carry 30%, the least position and underrated practice is Red Teaming, which is an advanced practice, but it covers only 10% across the world because of its complexity, high resource requirements and limited expertise. This study only focuses on organizational practices particularly in Philippines not globally evaluating large-scale datasets/databases, no models have been developed, lacks in natural language processing and automation. So, the unsupervised approach eliminates manual work, improves automation.

2.7 Analyzing the research gap

The literature survey shows yet existing research have not done tri-partite semantic mapping that unifies CVE vulnerabilities (NVD dataset) to MITRE ATT&CK techniques and tactics to NIST SP 800 – 53 controls along with severity predictions across NVD corpus. Some papers did pairwise map (Carello et al., 2025; Elmarkez et al., 2024), limited manual validations (Bhosale et al., 2024; Grigorescu et al., 2022), post-breach analysis (Karimi et al., 2025), implementing rule-based approaches (Kryukova et al., 2024; Lasantha et al., 2025), limitations on training data (Grigorescu et al., 2022), to fill these gap this work turns technical vulnerabilities into insightful information like aligning those to policy controls and attack techniques with an end-to-end pipeline using Sentence-BERT semantic embeddings for the tri-partite workflow (CVE -> MITRE ATT&CK ->

NIST) along with knowledge graph visualization, handled both structured and textual features individually as well as integrated those two and developed hybrid models to predict the severity. Also, an interactive assistant to look up each CVE IDs as well as free-text vulnerability analysis which supports organizations from reactive, manual and rule-based to proactive, automation, globally generalizable, scalable and GRC-aligned automation process which provides audit-ready component across environments regardless of size, sector or location – an important thing missed from all reviewed papers.

3 Research Methodology

3.1 Introduction and Methodology

This research proposes an integrated framework that is structured, comprehensive, iterative methodology that helps for implementation, development and evaluation of three cybersecurity domains and provides impact for governance, risks and compliance (GRC) decision-making process. The work began from structured NVD (National Vulnerability Database) that contain cybersecurity vulnerability entries to unstructured natural text information and then extended beyond mappings MITRE ATT&CK techniques and NIST SP 800-53 Rev.5 security controls families. The work focused on reproducibility and real-word applicability, so this study adopts Cross-Industry Standard Process for Data Mining (CRISP-DM) framework because it is more industry-aligned to solve problems To support GRC teams and organizations from risk to policy controls, this study aimed to build an automated scalable system which can classify vulnerability severity, generate cyber-attacks and policy mappings. This work includes data understanding, developing models, evaluation, deployment and often requires repeating this cycle before creating robust modelling which is particularly valuable in cybersecurity research so CRISP-DM perfectly suits. CRISP-DM distinguishes it from pure theoretical frameworks to operationally valuable and practical for security workflow integrations. This methodology implements a system capable of addressing real-world cybersecurity challenges and reaching the state-of-the-art through automated vulnerability and risk management as well as enabling researchers to extend, replicate or challenge the findings.

3.2 Understanding the scope of Business

Enterprises are facing real operational challenges in cyber risk assessment, where Business Understanding is the first phase of this. In section 2- Related work, two core deficiencies are framed and observed from existing GRC processes. Both Elmarkez et al. (2024) and Grigorescu et al. (2022) highlighted the major weakness is relying on manual rule-based methods of mapping vulnerabilities to attacks and controls which is time-consuming, not scalable enough and leads to inconsistency. The next weakness is the absence of automation when interpreting with both structured data and free-text descriptions a gap identified by Ali et al. (2025) – an evaluation of cyber threat tools. The business goal of this study is that organizations who handle or face cyberthreats should not always be dependent on manual rule-based methods, expert judgement and

inconsistent knowledge bases. The main objective is not only classifying vulnerabilities into LOW, MEDIUM, HIGH and CRITICAL severity cases through hybrid modelling but also using a systematic and automated way of mapping those relationships with semantically matched MITRE ATT&CK techniques and NIST SP 800-53 Rev.5 security controls. This phase directly addresses the limitations of Karim et al. (2025) – absence of automatic sematic linkage in IoRT systems by framing the research output into one unified decision-support tool that integrates model accuracy, score based semantic mapping and graph-based visualization. Stakeholders, system operation analysts, both vulnerability management and GRC teams, GRC officers and risk assessment professionals would benefit from this system who faces the challenge of triaging hundreds and thousands of newly disclosed CVEs (Common Vulnerabilities and Exposures). The AV-TEST institute registers approximately 450,000 new unwanted and malicious programs and applications daily which are overwhelming in volume and manual approaches cannot be processed within the timeframe and lead to unusual attacks and exploitations. Recent studies heavily rely on CVSS (Common Vulnerability Scoring System) scores provided by the NVD, it is a numeric value without any contextual information like what are the tactics and techniques can be used to exploit vulnerability, or which controls helps to mitigate the risk. There are two main parts one is severity classification from both structured and natural language description features (hybrid approach), and the other is automating the mapping process with attacks and controls where security analysts need to manually cross verify CVE datasets, MITRE ATT&CK techniques and proper NIST controls which were demonstrated by Ekisa et al. (2024) – even in controlled environments this work would consumes significant manual expert time. To advance the academic perspectives of cybersecurity this research proposed an operational pain point through semantic knowledge and machine learning methods by automating this entire process.

3.3 Data Extraction and Data Understanding

The study used three different datasets from cybersecurity domains – NVD CVE data, MITRE ATT&CKs and NIST SP 800-52 Rev.5 controls. All three datasets are official and publicly available; due to different structural formats the extraction steps differ on each.

CVE data

This dataset was extracted from National Vulnerability Database (NVD) JSON feeds that includes features of key CVSS exploitability metrics – base score, attack complexity, privileges required, user interaction, base score and a textual description which captures exploitability characteristics of each vulnerability for both cross functional and semantic mapping.

MITRE ATT&CK data

This was officially sourced from *enterprise-attack.json* file and it was published by MITRE. Where this study intentionally retained only the core technique-level attributes such as technique identifiers, names, descriptions and platform coverage rather than mitigations, data sources and

others for high-level mapping. A proper python script was used to change the hierarchical STIX into a clean csv.

NIST SP 800-53 Rev.5 data

This data was extracted from the official OSCAL JSON catalog. The NIST SP 800-53 Rev.5 is also highly hierarchical with many families and sub controls. To handle this a python script was written to modify this into a structure csv that includes high-level security governance requirements and policy safeguards through family classification, titles, control ids and description where these supports regulatory frameworks to mitigate from risk and more feasible for computational power. Each dataset differs not only in structure but also in context and meaning or semantic purpose. This study utilizes all the above-mentioned datasets to build a tri-partite mapping between CVE vulnerabilities, MITRE techniques and NIST controls as well as understanding all three datasets even though it is inconsistent. During this phase EDA (Exploratory Data Analysis) process was conducted to analyze and fix missing values, duplicate entries inconsistent naming conventions, severity records and so on across CVE dataset which has a significant class imbalance on LOW case. The main analysis lay on textual descriptions, varying from length, clarity and details to different technical semantic vocabularies which informs the text-embedding methods to carefully bridge these divides by context.

3.4 Data Preparation and Modelling

The CVE dataset is cleaned, encoded and normalized for model-ready. Separated the dataset as structured-only analysis, text-only analysis and finally integrated both into one single predictive classification analysis using multi-model fusion (hybrid approach). TF-IDF representation has been used for text baselines, Sentence-BERT for hybrid modelling and similarity mapping. Generated cosine similarity for top-k ranking across all three datasets (CVE→MITRE→NIST). Class imbalances are handled through internal and external weights; early stopping was also conducted to prevent overfitting and for generalization purposes.

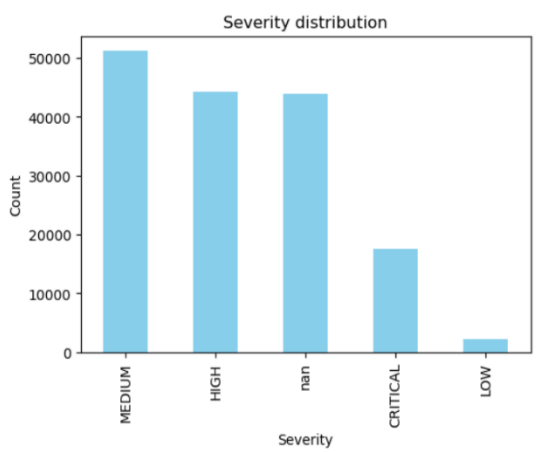

Fig2: Count of severity class imbalance

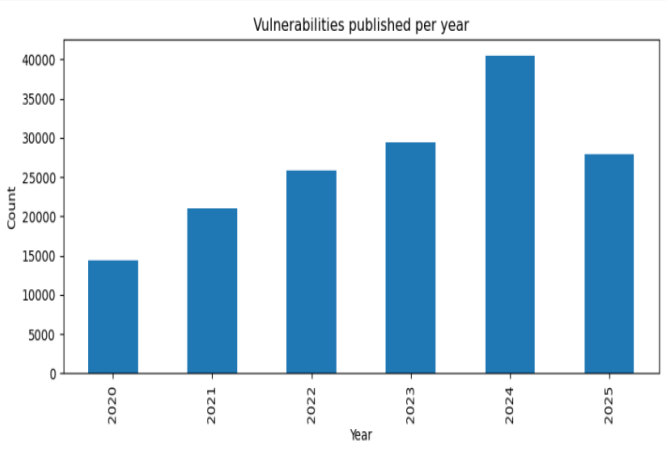

Fig3: New vulnerabilities records per year

4 Design Specification

The design of this cybersecurity knowledge system is a multi-layer architecture including data analytics, semantic embeddings and graph-based framework where all these are capable of automatically classifying severe vulnerabilities, identifying relevant techniques of MITRE and mapping to NIST controls also generalizes unseen vulnerability descriptions. The idea addresses the limitations in research – mostly rely on manual rule-based approaches and existing tools.

4.1 System Architecture

The system architecture begins with extracting structured CVE data from National Vulnerability Database (NVD) which includes CVSS metrics, base score and severity labels. Then extracted publicly available two unstructured textual datasets - MITRE ATT&CK and NIST SP 800 53-Rev.5 controls. By incorporating narrative form descriptions to capture threats using Sentence-BERT embedding overcomes traditional risk assessment. Rather than limited to numerical scoring fields, the system recognizes severity of each threat, potentially identifies attack and security paths. The innovation of this system lies in the scope of changing vulnerability to GRC reasoning.

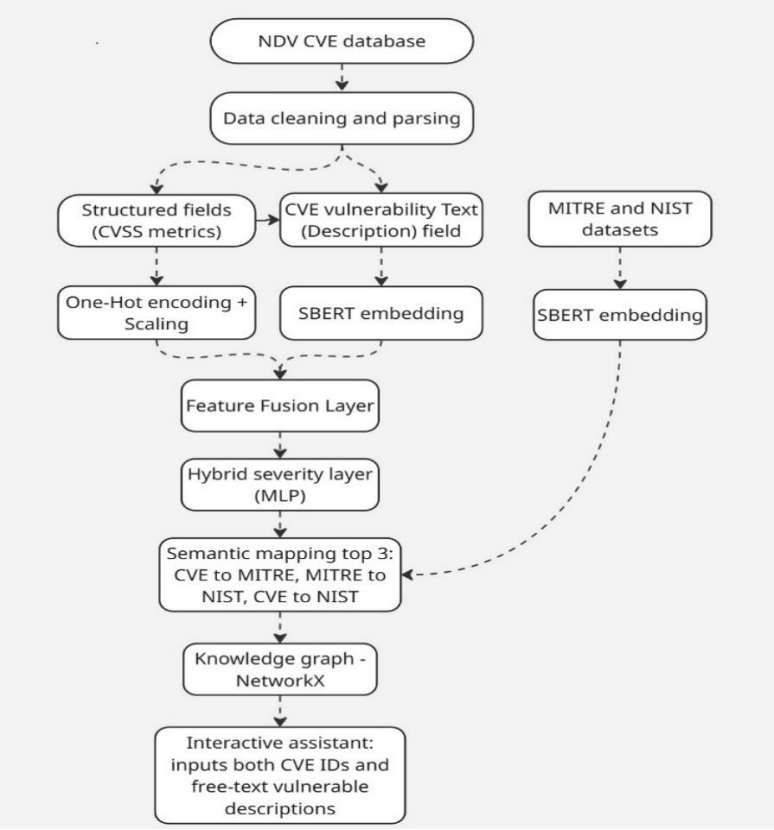

Fig4: System architecture workflow

4.2 Embedding Semantic Relationship Workflow and Knowledge Graph Representation

This embedding layer creates semantic space for each component such as CVE vulnerability descriptions, MITRE ATT&CK descriptions and control definitions of NIST. All textual information that matches with others lies close to each other in the vector space, generates separate embeddings and then transforms those textual sources into comparable embedding vectors and then compared those into cosine similarity scores. Therefore, semantic mapping can discover relationships between vulnerable actions, actions of attacks and security to defend those attack paths.

cosine similarity (CVE, MITRE ATT&CK)	Top-k techniques
cosine similarity (MITRE ATT&CK, NIST)	Top-k controls
cosine similarity (CVE, NIST)	Direct mapping

Fig5: Cosine similarity mapping to rank top-k matches

This fundamental mapping mechanism enables scalable previously unknown free-text vulnerability inputs. The next layer of architecture provides a visual tri-partite knowledge graph built with top-k mappings that connects all three frameworks into one single system. Nodes are: {CVEs, MITRE techniques, defensive NIST controls} with edges weighted by cosine similarity scores and the nodes are colored (red-CVE, blue-MITRE, green-NIST). This serves as a visual justification and understanding of relationships across three different datasets. Each fundamental component operates independently which enables future improvements and induvial component replacement much easier without touching or modifying the entire system such as adopting different modelling languages, further extensions in control frameworks and so on. The novelty and innovation lie in the tri-partite CVE to MITRE to NIST reasoning, builds a knowledge bridge of rule-free system that outperforms traditional methods.

5 Implementation

This section is all about the implementation process of final end-to-end pipeline, technical environments & components used and core implementations.

5.1 Environments and Libraries Used

The system was built in two different environments, one is Jupyter Notebook, and the other is Google Colab Pro due to computational power and time and was developed using Python. Where Jupyter Notebook was used for preprocessing the CVE data, do Exploratory Data Analysis (EDA), build models for structured only and text only features. Then effectively choose Google Colab Pro due to its superior computational GPU power and time efficiency for building hybrid machine learning models, generating semantic mapping of top 3 CSVs, NetworkX knowledge graph and

interactive assistants for both CVE IDs and free-text vulnerability descriptions. This study worked with libraries which are mature, supportive and suitable for large-scale text analysis - Pandas, NumPy, TensorFlow, scikit-learn, Sentence-BERT, PyTorch and NetworkX as well.

5.2 Data Transformation and its Preprocessing Pipeline

This step begins in Jupyter Notebook with a complete transformation of CVE (National Vulnerability Database) dataset as it includes both structured and long textual description features. For each vulnerability this system generates high-quality numerical representations by cleaning, normalizing, scaling and encoding all the structured features and then embedded text field by using Sentence-BERT 'all-MiniLM-L6-v2' model. The output of this process includes embedding (.npy and .pt) files, preprocessed features and a reusable preprocessing end-to-end pipeline.

5.3 Hybrid Deep Learning Approach and its Implementation

The next phase was changing the environment to Google Colab Pro for computational power. Here the hybrid deep learning was built with batch normalization, prevent overfitting by early stopping steps, L2 for penalizing large errors and dropout regularization for generalization. The model infuses features of both structured and Sentence-BERT embeddings into an MLP (multi-layer perceptron) which was trained to classify vulnerability severities – HIGH, MEDIUM, LOW, CRITICAL and it was implemented in TensorFlow/Keras. This model stands as the initial work of system's pipeline.

5.4 Semantic Mapping and Relationships

This part was also done in Google Colab pro, with the use of three external cybersecurity sources such as MITRE ATT&CK techniques, NIST SP 800-53 Rev.5 control policies and CVE (NVD) vulnerabilities. Produced a tri-partite relationship using Sentence-BERT embeddings method between CVE → MITRE ATT&CK, MITRE ATT&CK → NIST and CVE → NIST, ranked top-k similarity scores across all three sources and created three comprehensive mapping csv files (datasets). These files open the knowledge of automated reasoning and work as a backbone of how a vulnerability can be exploited and what are all the possibilities to control it, or which controls help to mitigate it.

5.5 Representation of Unified Tri-partite Knowledge Graph

Based on the csv's top-k mappings, rather than the continuous operation this study constructed a unified representation of tri-partite visualization graph using NetworkX which was also implemented in Google Colab Pro. Where CVEs, MITRE techniques and NIST controls are the nodes of this explainable and traceable visualization. This shows the capacity of system that works for threats and risk mitigation strategies.

5.6 Interactive Notebook Assistant

The final output combines all three components into a one single interactive notebook-based assistant which either accepts CVE ID as a string or a free-world/text vulnerability description as an input, then runs the hybrid model to predict or determine or identify the severity, retrieves semantic mapping of top MITRE ATT&CKs and NIST controls. Specifically, along with that the system also provides description of the vulnerability, probability distribution of all the severity cases, top 3 MITRE techniques as well as both direct and indirect NIST controls. And finally produces a visual representation (graph) of all the above. In summary, this prototype produces a Governance, risk, and compliance (GRC) intelligence which is capable of producing raw information like CVE ID or vulnerable description into an actionable, automated, and evidence-based intelligence that addresses the business challenges discussed in methodology by producing all necessary artefacts.

6 Evaluation

The evaluation phase is analyzing the produced system which shows predictive performance, quality of semantic mapping, effective usefulness and valuable contribution for GRC. This helps to evaluate whether the hybrid deep learning model and semantic mapping improves automated cyber threat analysis more effectively than rule-based manual approaches.

6.1 Performance of Predictive Models

6.1.1 Model's performance on Structured-Only Features

Two models have been trained on the structured only attributes such as CVSS metrics and severity (target/exploitability) variable. Initially both XGBoost and LightGBM showed approximately identical results, proving that choosing different models does not improve learnings. Even after feature engineering and class weighting slightly improved the results but confusion matrix indicates overlaps and misclassification of most severe classes by highlighting low F1 and recall on LOW and high recall on CRITICAL, this shows the importance of contextual information and limitations of using structured only features.

6.1.2 Model's Performance on Text only Features

Trained Logistic Regression and XGB with TF-IDF representation on vulnerability description with 109492 x 3000 matrix. Compared to structured baseline this shows progressive improvement, proving the richness of contextual data. Confusion matrices revealed that XGB excelled in LOW class precision but dropped recall and limited with F1.

6.1.3 Evaluating the Performance of Hybrid Model

The hybrid modelling approach integrates both structured and textual features. By using TF-IDF representation XGB and LightGBM were trained and used Sentence-BERT representation on MLP

model. All three achieved slightly identical results but deeper architecture shows stability through enhancement with L2 regularization, early stopping and dropout methods. This method outperformed structured-only and text-only approaches proving the value of multimodal fusion. To prioritize GRC operational system, four complementary result metrics were selected. CVE dataset has severe class imbalance – 2% LOW class, 16% CRITICAL and the rest 82% are covered with HIGH & MEDIUM. Accuracy is the primary metric that captures overall correctness of classification, to avoid minority ignorance evaluated Macro F1-score, to capture the riskiest minority class and to avoid resource waste LOW F1 has been utilized because F1 is a single value-harmonic mean of precision and recall, to avoid breaches on severe class is the most important perspective of cyber risk and GRC, so CRITICAL recall is chosen rather than precision and F1 because catching real positives is more important than avoiding extra false alarm.

- Accuracy = TP + TN / TP + TN+FP + FN
- Macro F1 = 1/n Σ F1(class_i), F1 = 2 x (precision x recall) / (precision + recall)
- LOW F1-score = 2 x (LOW precision x LOW recall) / (LOW precision + LOW recall)
- CRITICAL recall = TP_CRITICAL / (TP_CRITICAL + FN_CRITICAL)

Approach	Accuracy	Macro F1-score	LOW F1	CRITICAL Recall
Structured-only XGBoost	~0.61	~0.52	~0.23	~0.97
Structured-only LightGBM	~0.60	~0.52	~0.23	~0.97
Text-only Logistic Regression (TF-IDF)	~0.68	~0.57	~0.23	~0.69
Text-only XGBoost (TF-IDF)	~0.74	~0.61	~0.28	~0.60
Hybrid: TF-IDF + structured →XGBoost	~0.82	~0.72	~0.39	~0.93
Hybrid: TF-IDF + structured →LightGBM	~0.83	~0.74	~0.44	~0.91
Hybrid: Sentence-BERT + structured→LightGBM	~0.82	~0.72	~0.43	~0.89

Fig6: Comparison table of predictive models

The above table summarizes that LightGBM achieved the highest macro F1-score while MLP learns and understands the vulnerabilities with robust semantic relationships and hybrid modelling effectively enhance severity classification.

6.2 Analyzing Semantic Relationships and Performance

Instead of relying on manual mappings and defined rules the second evaluation captures sentence-level embeddings with cosine similarity scores ranging from 0.3 to 0.7 which is moderate but

meaningful as explicitly highlighted by Carello et al. (2025) and these scores are used for ranking top-k techniques and controls relevant to each vulnerability across three directions – CVE to MITRE, MITRE to NIST, CVE to NIST. For instance, if a vulnerability that describes local privilege escalation, then the system maps to credential abuse and process injection (MITRE ATT&CK) and further move to NIST controls related to system integrity and authentication to secure the vulnerability from exploitation. This process was done within few seconds that helps security analysts to save time - waiting for an expert advice or manually searching detailed documents where the possibility of risk can increase and exploitation can happen at any time during manual/time-consuming process. By providing CVE identifiers and free-text descriptions, the system correctly identifies severity classification with CVSS metrics and logically outputs consistent MITRE and NIST mappings, additionally for each MITRE attack techniques the system generates top 3 NIST controls, showing all the possible security framework should be implemented – a practical usefulness. This proves that the mapping generalizes beyond the known information from the dataset (not limited to historical records) that enables scalable GRC architecture.

6.3 Graph Based Analysis Explanation

A knowledge graph was developed using NetworkX which shows a visualized representation of mappings – how a vulnerability connects to multiple attacks and controls. The full graph was constructed with all three embedded CSVs – CVE to MITRE, MITRE to NIST, CVE to NIST with color type and edges are weighted by similarity scores. Due to the complexity of graph and dataset size, creating a subgraph with 150-nodes - provides reasonable explanation. This visualization can be used in security workflows, compliance discussion and contributes for both academic and practitioner purposes. It also serves as evidence of how similarity in text connects cybersecurity.

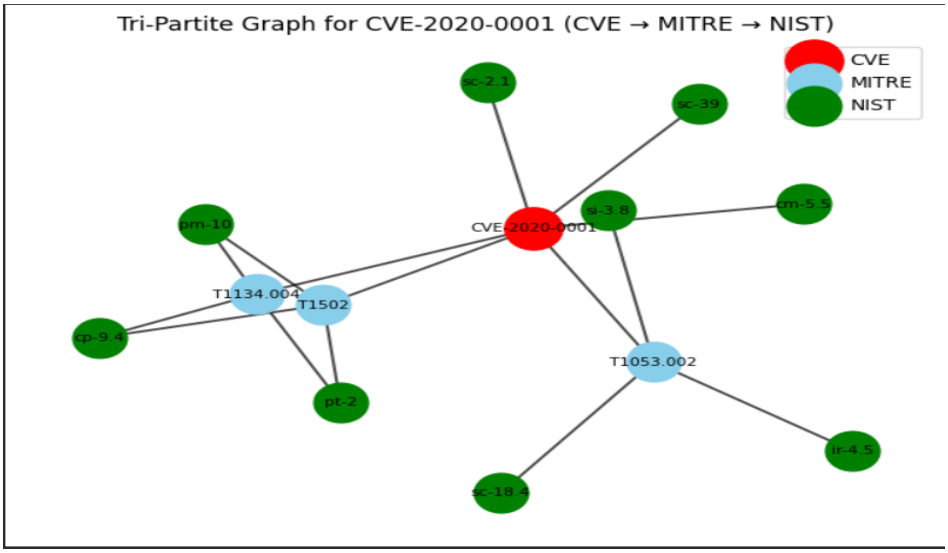

Fig7: An example subgraph of CVE-2020-0001 mapping with ATT&CK techniques and NIST controls.

6.4 Discussion Phase of the Above Findings

The evaluated results show the system performance across different dimensions. Compared to traditional machine learning, the hybrid approach shows significant improvement and richness of severity classification. The similarity of mapping pipeline helps to automate relationships which were rarely explored in existing or recent research and requires manual human effort as well as expert domain knowledge. The standpoint is that the system directly addresses challenges faced in GRC which helps with an enterprise level security framework implementation. However, the ground-truth experiment remains untouched because ranking was done with cosine similarity which may bias, graph visual is helpful but complex because of the absence of interpretability that remains an open challenge. In summary, the results show measurable results compared to prior studies by combining machine learning, hybrid deep learning, embedding, graph-based visuals and assistant can be combined into one automated framework that technically supports for high level decision making in GRC.

7 Conclusion and Future Work

This research provides automation pipelines that build cybersecurity knowledge and especially contributes to GRC decision-making by integrating MITRE ATT&CK techniques, NIST SP 800-53 Rev.5 controls and mapped these two using Sentence-BERT semantic embedding with analyzed software vulnerabilities. To secure rapidly evolving threats, this proposed system contributed and addressed the gap in cybersecurity governance tools which rely on manual rule-based mappings yet struggle to remain updated. Compared to traditional approaches this system gives a more context rich risk assessment process by combining linguistic information with traditional scoring. It also enabled automated reasoning across three different cybersecurity frameworks which reduce manual hours of work to seconds.

The hybrid modelling shows significant improvement in performance compared to structured-only predictive capability. Where the LightGBM fusion with TF-IDF achieved ~83% accuracy, ~0.74 macro F1 and the MLP fusion with ~82% accuracy, macro F1-score of ~0.72. Using Sentence-BERT embedding the system produces reasonable context-aware top 3 mapping across three domains. From the top 3 mappings a knowledge subgraph (150 nodes) was built using NetworkX – shows a transparent view of attacks and controls connectivity with vulnerabilities. Although the system shows promising results it has some limitations that should be acknowledged in future. Cosine similarity scores are automatically calculated to reduce manual work, and it is moderate due to different language style and details of all three datasets based on this the system can suggest meaningful outcomes approximately which requires qualitative expert validation that strengthens the confidence of operational use. Continuous updates, additional framework (ISO 27001, CIS controls) integration and incorporating advanced language models for embedding remains as future work.

Reference

1. Carello, M.P., Bonomi, S. and Querzoni, L. (2025) 'A study on NLP-based semi-automated mapping of cybersecurity controls on vulnerabilities', in *Lecture Notes in Computer Science*, vol. 15456. Springer Nature Switzerland, pp. 297–315. doi: 10.1007/978-3-031-89350-6_18.
2. Lasantha, N.W.C., Tilwari, V., Maduranga, M.W.P., Chakraborty, N., Abeysekara, R. and Sharma, D. (2025) 'Hybrid machine learning approach for enhanced vulnerability detection in cloud environments using NIST and MITRE frameworks', in *2025 5th International Conference on Advanced Research in Computing (ICARC)*. IEEE, pp. 1–6. doi: 10.1109/ICARC64760.2025.10962945.
3. Kaur, P., Ramkumar, K.R. and Kaur, A. (2025) 'A detailed study of vulnerability detection using common vulnerabilities and exposures from NVD using machine learning and deep learning models', in *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)*. IEEE, pp. 1979–1982. doi: 10.1109/ICCSAI64074.2025.11064008.
4. Karimi, M. and Mendez Mena, D.M. (2025) 'Data-driven IT/OT cyber risk evaluation and mitigation prioritization using machine learning', in *2025 IEEE Conference on Artificial Intelligence (CAI)*. IEEE, pp. 962–969. doi: 10.1109/CAI64502.2025.00169.
5. Bhosale, P., Kastner, W. and Sauter, T. (2024) 'Mapping ICS vulnerabilities: prioritization and risk propagation analysis with MITRE ATT&CK framework and Bayesian belief networks', in *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, pp. 1–8. doi: 10.1109/ETFA61755.2024.10710893.
6. López, A.D.E., Pinilla, M.A. and Carvajal Mora, H.R. (2025) 'A novel risk-based methodology for enhancing industrial control systems security: a systematic review and case study', *IEEE Access*, vol. 13, pp. 160313–160339. doi: 10.1109/ACCESS.2025.3609252.
7. Karim, H., Gupta, D. and Sitharaman, S. (2025) 'Securing LLM workloads with NIST AI RMF in the Internet of Robotic Things', *IEEE Access*, 13, pp. 69631-69649. doi: 10.1109/ACCESS.2025.3561235.
8. Kryukov, R.O., Fedorchenko, E.V., Kotenko, I.V., Novikova, E.S. and Zima, V.M. (2024) 'Security assessment based on attack graphs using NVD and MITRE ATT&CK database for heterogeneous infrastructures', *Informatsionno-upravliaiushchie sistemy [Information and Control Systems]*, vol. 2, pp. 39–50. doi: 10.31799/1684-8853-2024-2-39-50.
9. Elmarkez, A., Mesli-Kesraoui, S., Oquendo, F., Berruet, P. and Kesraoui, D. (2024) 'A similarity approach for the classification of mitigations in public cybersecurity repositories into NIST-SP 800-53 catalog', in Bouzefrane, S. and Sauveron, D. (eds.) *Information Security Theory and Practice*. WISTP 2024. Lecture Notes in Computer Science, vol. 14625. Cham: Springer, pp. 64-79. doi: 10.1007/978-3-031-60391-4_5.
10. Al-Sada, B., Sadighian, A. and Oligeri, G. (2024) *'Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database'*, IEEE Access, 12, pp. 1217–1234. doi: 10.1109/ACCESS.2023.3344680.

11. Rotibi, A., Saxena, N. and Burnap, P. (2024) 'Winning the battle with cyber risk identification tools in industrial control systems: a review', *IET Cyber-Physical Systems: Theory & Applications*, vol. 9, no. 4, pp. 350–365. doi: 10.1049/cps2.12105.
12. Ekisa, C., Ó Briain, D. and Kavanagh, Y. (2024) 'Leveraging the MITRE ATT&CK framework for threat identification and evaluation in industrial control system simulations', in *2024 35th Irish Signals and Systems Conference (ISSC)*. IEEE, pp. 1-6. doi: 10.1109/ISSC61953.2024.10602968.
13. Ali, A., Hwang, R.-H. and Lin, Y.-D. (2025) 'Evaluating cyber threat intelligence: accuracy, completeness, relevance, and freshness', *IEEE Access*, 13, pp. 157863-157876. doi: 10.1109/ACCESS.2025.3606477.
14. Yulianto, S. and Caronongan, D.C. (2024) 'Investigating cybersecurity assessment practices: enhancing defenses in the Philippines', in *2024 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*. IEEE, pp. 83–91. doi: 10.1109/ICIMCIS63449.2024.10956822.
15. Grigorescu, O., Nica, A., Dascalu, M. and Rughinis, R. (2022) 'CVE2ATT&CK: BERT-based mapping of CVEs to MITRE ATT&CK techniques', *Algorithms*, 15(9), 314. doi: 10.3390/a15090314.