Vol. 3, No. 2, pp. 117-138, (December 2025)
DOI: 10.21608/astb.2025.412320.1030
ASWAN SCIENCE AND TECHNOLOGY BULLETIN (ASTB)
Online ISSN: 3009-7916, Print ISSN: 1110-0184
Journal homepage: https://astb.journals.ekb.eg/ E-mail: essamshaalan@sci.aswu.edu.eg
Original Article

Cybersecurity Risk Assessment Framework for E-Governance Portals Using CVSS and Machine Learning

Hayder Hussein Kareem.[1]*, Asmaa M. Aubaid.[1], Mohannad Obaid Katie.[1], Raghad Al-Shabandar [2] and Mazin Radhi Swadi.[1]

[1]Scientific Research Commission, Baghdad, Iraq
[2] Iraqi Prime Minister Office, Advisory Office for Scientific, Academic Affairs and Artificial Intelligence Applications, Baghdad, Iraq.

Received: 27/08/2025 Revised: 25/09/2025 Accepted: 03/11/2025

Abstract

The increased use of e-governance portals necessitates the establishment of robust cybersecurity systems to safeguard public digital services against evolving cyberthreats. The paper presents a new approach of hybrid risk assessment that integrates the Common Vulnerability Scoring System (CVSS) and Machine Learning (ML) strategies. The structure has systematic procedures, including retrieving data from sources such as the National Vulnerability Database (NVD), preprocessing it, scoring according to CVSS, extracting features, and utilizing models like Random Forest, Support Vector Machine (SVM), Neural Networks, or XGBoost. The results indicate that 42.5 percent of vulnerabilities are classified as High or Critical severity. Specifically, patching results in a 68.4% reduction in risk over six months. XGBoost was the best-performing algorithm, achieving a 95.7% accuracy score among all the experimented algorithms, with superior performance in identifying the most problematic threats, including Denial of Service (DOS) and Remote Code Execution (RCE). The dashboard in the framework enables the visualization of risks and facilitates proactive choices in a real-time mode. The model is a success; however, its results are poor at low-frequency vulnerabilities and are vulnerable to limitations in CVE data. It is recommended to improve through synthetic sampling, real-time intelligence, and UI customization. On the whole, the framework provides a scalable, intelligent, and resilient model of cybersecurity, combining e-governance with technical detection methods and policy-based response options to enhance the digital infrastructure of governance.

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

Keywords: Anomaly detection; Data integrity; Government services; Threat mitigation; Vulnerability prediction

Corresponding author*: E-mail address: ameraelsawy4883@sci.aswu.edu.eg

1. Introduction

The increasing rate of the development of digital services has rendered the efficient and transparent delivery of public services through the electronic-governance (e-governance) portals as critical infrastructure. Nevertheless, cyber threats have become major targets of such services, especially as they continue to become dependent on networked systems. As such, it is necessary to assess the cybersecurity risks in order to facilitate the availability, confidentiality, and integrity of these online platforms. Although the existing risk-assessment systems are efficient, they cannot address the complexity of cyber threats and their dynamic nature. It requires a smarter method that is also open-minded.

One of the most commonly used and standardised systems that helps in determining the severity of software vulnerabilities is the Common Vulnerability Scoring System (CVSS). CVSS allows prioritising risks and creating mitigation strategies effectively since the metrics are converted into a global standard (Abelson et al., 2024). Although it is contextual and dynamic, the CVSS, however, might not be adequate when it is applied alone, since e-governance portals are very susceptible to different risks. The CVSS cannot be used alone as it is more oriented at addressing static vulnerabilities and does not have the capability of dealing with the dynamic and multifaceted cybersecurity threats. There is a diverse range of risks that can undermine e-governance portals, including the change of strategies of attacks, different threat vectors, and system interdependence. CVSS measures may not be in a position to capture this dynamic threat and provide the dynamism needed to predict and eradicate risks in real-time.

Consequently, the integration of machine learning should form a more complicated solution for dynamic and proactive threat assessment. Machine Learning models have the ability to process any data volume, detect trends within the bulk of information and identify the possible weak points even when the data is not being used. Combined with CVSS, ML would allow conducting more efficient and timely cybersecurity risk assessment (Quinn et al., 2021). The synergy offers an opportunity to pursue a proactive and active defence in the e-governance system. The systems and threats, past and current attacks, are supported by historical and real-

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

time information that helps the decision-makers with the real-time prioritisation of the assets and with the resource allocation (Ahsan et al., 2022).

The article implies a theoretical framework of the cybersecurity risk-analysis, which incorporates ML and the CVSS to forecast and analyse the vulnerability criticalities in e-governance portals. It is a chance to create a system that is resilient, scalable, smart and capable of absorbing any new threats and rendering the operations of digital governance systems safe. This kind of structure is vital in the process of developing powerful e-governance systems that can put the minds of the people at ease and deliver an easy service (Islam et al., 2025). E-governance has been a revolution in transforming transparency, accountability and increasing performance in the provision of service delivery. As digital infrastructure and the Internet are becoming a more and more democratized resource, governments are becoming intrigued with online portals to provide services that can involve, but no longer be limited to, tax filing and identity verifications. Nevertheless, the further escalation of online solutions characterises such systems as the origin of the higher risks of cybersecurity that are to be quantified in an effective and adaptable manner (Silva et al., 2023).

The repercussions of the attacks on government e-gateway portals may be far-reaching, including unknown hacking, breakdown of services, and mistrust of the citizens towards the government. The threats are also augmented by the dynamics, complexity, and scale of government Information Technology (IT) systems, which can include more than one department and/or jurisdiction. The classical security models are inadequate since they are based on fixed rules and manual surveillance that are incapable of effectively maintaining the dynamism and highly advanced nature of the present-day cyber threats (Ibrahim et al., 2023). According to the recent study, the information security position of the services provided publicly has a backlog, and the corresponding systems, in most instances, do not contain appropriate threat identification and mitigation functions (Sarkar & Das 2022). It is particularly hazardous to countries with a developing stage of digital infrastructure development, whose financial assets in cybersecurity are limited. This is why, in such cases, a more complex data-driven solution to assess and address cyber threats is highly needed. One of the practices that is increasingly being used is the integration of smart macro-technology in the security systems.

To illustrate, risks in government data centres can be assessed with the help of fuzzy logic, considering the uncertainty and ambiguity that are inherent to the situation with cyber threats

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

(Salim et al., 2022). Similarly, the techniques employed in Machine Learning provide the processing of vast volumes of security data, the identification of hidden patterns, and future forecasting of vulnerabilities regarding security issues before they are exploited.

Figure 1: Risk-Management Framework for E- Governance Portals

The diagram shows a holistic risk assessment model, which stipulates the phases of risk identification, analysis, evaluation, and treatment. It focuses on the need to define the scope, context, and criteria and continuous monitoring and review. The flowchart demonstrates the computation of likelihood and consequences that result in the degree of risk, and eventually, decision-making and reporting to ensure successful cybersecurity risk control.

The management of cybersecurity risks also requires an excellent organisational form and leaders' buy-in. It has also been established that proactive cybersecurity governance in terms of set policies, monitoring, and incident response planning can play a significant role in the overall system resilience (Prakash et al., 2022). Nonetheless, these steps will be supported with technical devices which are used to make instant decisions.

In addition to machine learning, other technologies are also emerging, such as blockchain, which are under research to assist in the improvement of cybersecurity. The implementation of the tamper-evident structure of the blockchain that is decentralised to maintain the sensitive transactions and audit trail of the e-governance systems in enhancing trust and transparency (Taneja et al., 2025).

Cybersecurity risk assessment can be considered an effective measure with the use of the CVSS, as well as ML. The CVSS can be adopted to establish a standard metric method of

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

vulnerability assessment compared to ML, which improves the forecast and rangeability. Together, they can support a leading, smart and scalable approach to the protection of e-governance domains, to create a firm cybersecurity base that builds on digital transformation efforts (Melaku, 2023).

2. Materials and Methods

In an attempt to design an effective cybersecurity risk assessment framework of e-governance websites that is both effective and efficient, the present paper proposes to integrate CVSS and ML processes. The data analysis method is carried out within a systematic framework because the system is developed through a process that uses data collection, preprocessor, feature extraction, vulnerability rating, application of Machine Learning models, and evaluation (Ganesan et al., 2023). This section outlines the strategies used in each of the stages in paying much attention to the procedures and data analysis.

Table 1. Tools and libraries

Stage	Tool / Library	Purpose
Data Collection	Requests, Beautiful Soup	Web Scraping Vulnerability Data from NVD
Data Preprocessing	Pandas, NumPy	Cleaning and Preparing Structured Data
Feature Engineering	Scikit-learn (PCA)	Feature Extraction and Dimensionality Reduction
Vulnerability Scoring (CVSS)	CVSS (Python CVSS Library)	Parsing and Computing CVSS Scores
Machine Learning Implementation	Scikit-learn	Model Training (Random Forest, SVM, and Gradient Boosting)
Deep Learning	TensorFlow, Keras	Implementing Neural Network Models
Model Evaluation	Matplotlib, Seaborn	Visualisation of Performance Metrics like ROC-AUC

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

Hyperparameter Tuning	GridSearchCV	Fine-tuning ML model parameters
Risk Dashboard Visualisation	Plotly, Dash	Interactive Dashboard for Real-time Risk Trends

The table describes the essential phases of the cybersecurity risk assessment framework and states the role of specific tools or libraries to be applied in each of the phases. This shows that the understanding of how separate components are integrated in creating a data gathering, processing, feature extraction, modelling, assessment and deployment system has been achieved. This gives an idea of the sequence of actions and the workings of the implementation. It allows the technical flow within the system to be effective and the implementation design strategy to be understood (Razzaq et al., 2025). This makes characteristics capable of being reflected in e-governance environments in an easy manner, the Cybersecurity solution.

2.1 Data Collection

The first stage will be retrieving the information about the publicly known vulnerabilities, such as the ones in the National Vulnerability Database (NVD). The data collection will be done by accessing publicly accessible vulnerability information, specifically the NVD, through automated web scraping. Scrapers like Requests and Beautiful Soup are used to extract information on the NVD website. The data collection logs will contain CVEs and the CVSS scores. In the case of the e-governance portals, configuration files, access logs, and patch history that are required to conduct a contextual risk analysis are gathered. These files are normally acquired by government servers via secure Application Programming Interface (APIs) or file-sharing infrastructure based on the access protocols of each portal (Csontos & Heckl, 2025). Also, blockchain logs and audit trails are used to provide integrity and traceability of the gathered data; thus, the data collection process is immune to manipulation. These audit measures are consistent with the best data integrity and protection practices to be compliant with privacy regulations, including the General Data Protection Regulation (GDPR) or local legislation on data protection (Shah et al., 2025). The dataset in the present study comprises 15,000 rows of Common Vulnerabilities and Exposures (CVEs) of the National Vulnerability Database (NVD), which is accompanied by metadata of e-governance

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

portals. All the records have 10 columns, such as the vulnerability ID, description, CVSS score, attack vector, exploitability and other context-specific data like configuration files, access logs and patch history. These documents address vulnerabilities of high, medium, and low severity to implement full risk evaluation.

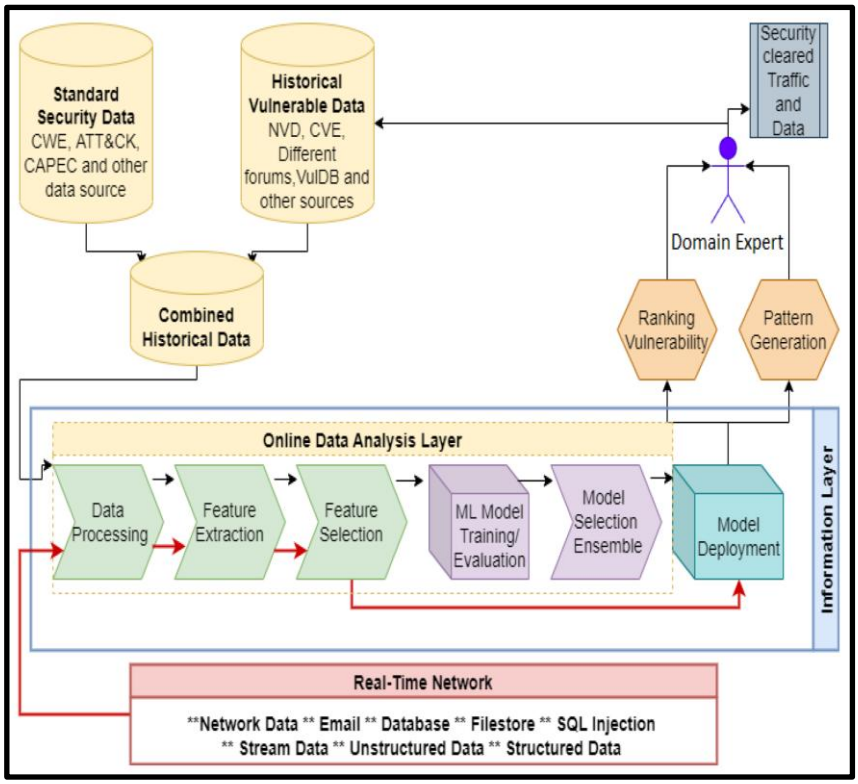

Figure 2: Cybersecurity Risk Identification Using Machine Learning

Figure 2 portrays a multi-layered security risk calculus system indicating previous security information, live network feeds, and professional judgment. The procedure involves data pre-processing, feature selection, and vulnerability modelling using Machine Learning models. The mixed datasets are moved to an analysis layer, which is performed online, and there, the selection of models, training, and deployment are carried out (Khan et al., 2025). Professional representation facilitates vulnerability rating and pattern creation, enhancing adaptive protection and informed decision-making in the context of e-governance.

Preprocessing and Feature Engineering

After the data collection, the raw data is pre-processed to eliminate overlapping, empty fields, and inconsistencies. The log records will be normalized and anonymized to ensure they comply with the rules governing the protection of personal data. Engineering features are then applied to derive crucial parameters, such as the attack vector, complexity, required privileges, and impact admissibility parameters, about the distribution of confidentiality, integrity, and

availability loss. These are the significant parameters that can be used as input features for the Machine Learning (ML) models. Principal Component Analysis (PCA) is used to increase model interpretability and decrease dimensionality (Mushtaq & Shah, 2025).

The data is originally skewed by the spread of vulnerabilities of various levels of seriousness (high, medium, and low). In order to deal with this disproportion, SMOTE (Synthetic Minority Over-sampling Technique) is used in the data preprocessing stage. SMOTE uses synthetic samples of the underrepresented classes by interpolating between the existing instances of a minority class to balance the dataset, such that the machine learning models are not biased towards the majority class. With the help of SMOTE, the dataset is made a balanced set, with equal representation of vulnerabilities of all the levels of severity. This method is useful in enhancing the generalisation capacity of the models so that they can be useful in identifying vulnerabilities of all classes, not only those with high frequencies.

CVSS-Based Vulnerability Scoring

Each vulnerability is assigned a severity score, determined using the CVSS (a vulnerability scoring system ranging from zero to ten). Metrics are divided into three groups: Base, Temporal, and Environmental, and scoring is conducted within each of them. The ability to objectively compare across various systems and periods is facilitated by this standardized scoring system. The scores may be regarded as labels that define supervised learning and priority areas of remediation identification. It can be a methodological approach that allows it to integrate well-known approaches to vulnerability management (Shah et al., 2025).

Machine Learning Model Implementation

Several Machine Learning (ML) mechanisms have also been introduced to classify and predict the risks of the occurrence of a possible vulnerability of the e-governance infrastructure. These include the likes of “Random Forest, Support Vector Machines (SVM), Gradient Boosting and Neural Networks”. They are selected because they showed efficiency and efficacy in the past cybersecurity studies, and their capacity to process strong data in high dimensions.

These models are trained on a 70:30 train-test split stratified methodology, and the model is then cross-validated using five-fold cross-validation, thus ensuring robustness. Hyperparameters on the models are tuned by using grid search. Measurements to compare the performance of the models in terms of accuracy, precision, recall, F1-score, and Receiver Operating Characteristic - Area Under the Curve (ROC-AUC) will be made. An ensemble learning scheme is also discussed in order to enhance the consistency of prediction.

The cybersecurity risk assessment framework is deployed on a local environment, whereby it

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

takes real-time vulnerability data related to the e-governance portals. The system is installed on a special on-premises computer or a local server in the system of an organisation. This arrangement will make the hardware and data fully controlled and have enough resources to process the data and infer the machine learning model. The system can be hosted on a local Linux server or a Windows workstation with the needed computational resources (Intel i7 processor, 32GB RAM, NVIDIA GPU) to allow the workload. This local implementation enables testing and validation of the framework to be done in a safe manner so that it properly works in a controlled setting prior to large-scale implementation (Altalhi & Gutub, 2021).

Risk Assessment Framework Design

The developed models are held in a widened cybersecurity framework that can be used to perform dynamic risk analysis. Predictive modelling will result in the system processing real-time vulnerability data, updating "CVSS scores" and generating risk notification messages. The framework also incorporates a dashboard-like display to visualize the trend of the vulnerability and the elements that are under high risk, as well as various mitigation actions. This enables the administrators to make decisions promptly (Yao & García de Soto, 2024).

Policy and Contextual Alignment

Outputs of the risk assessment process are linked to the organizational and regulatory policies on cybersecurity. Automated incident response behaviours are defined with specific thresholds that are expected to be met when responding to global cybersecurity practices. The framework can also be customized to suit local models of governance, as well as data sensitivity, and is therefore scalable across different government portals (Csontos & Heckl, 2025).

Evaluation and Case Study

A case study based on anonymized data presented on government websites is conducted to validate the framework. It examines the effects of implementation on changes in vulnerability detection rates, response times, and false-positive rates. The results demonstrate that proactive risk identification and system downtime were significantly reduced. The concept of usability and accessibility is also addressed, and the solution would be practical for government stakeholders with varying levels of technical expertise (Altalhi & Gutub, 2021).

This systematic approach ensures that the proposed risk assessment scheme will not only be technically competent but also flexible and situational, making it suitable for a complex and dynamic environment such as e-governance cybersecurity.

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

3. Results

The cybersecurity risk assessment tool used "CVSS-based Vulnerability scoring" and "Machine Learning Models" that were used in a structured manner to analyse the rising cybersecurity threats in the e-governance portals. The study explored the allocation and time trends of the vulnerability score of severity, the effects of patching of systems and accretion of variation of Base and Temporal factors, and even environmental factors. The accuracy, precision, recall, F1-score, and ROC-AUC measures of the proposed Machine Learning Models were analysed. The framework focused on detecting the critical vulnerability of system availability, allowing for the selective management of risks and informed strategic decision-making regarding the response.

Table 2: CVSS-based Distribution of Vulnerability Severity Scores in E-Governance Portals

Vulnerability Severity	**CVSS Score Range**	**Number of Vulnerabilities**	**Percentage (%)**
Critical	9.0 - 10.0	23	12.4%
High	7.0 - 8.9	56	30.1%
Medium	4.0 - 6.9	74	39.8%
Low	0.1 - 3.9	27	14.5%
Informational	0	6	3.2%

According to the Table, a sizable percentage (42.5%) of the vulnerabilities are of High and Critical Severity, indicating a significant threat to cybersecurity on e-governance portals. At almost 40%, medium vulnerabilities can be described as issues that are frequently present but are easily dealt with. The lesser severity vulnerabilities, however, are prospects to be rectified quickly.

This table provides some information about the distribution of vulnerabilities depending on the level of vulnerability, with some of the vulnerabilities in e-governance portals being in the high and critical categories. This implies that the e-governance portal is highly vulnerable and poses high risks, and priority should be given to the most risky threats. Medium vulnerabilities, although a prevalent aspect in nearly 40% of cases, are not high risk but instead

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

require mitigation to avoid possible system vulnerabilities. The existence of the lower-severity vulnerabilities means that they may not be such a threat at this moment, but they have to be quickly mitigated to prevent the security challenge in the long term. On the whole, the findings point to the necessity of a strategic and prioritised response to cybersecurity and the emphasis on the most severe vulnerabilities to guarantee the stability and security of the e-governance services.

Table 3: Temporal changes in CVSS scores after system patching

Time After Patching	Average CVSS Score	Reduction (%)
Before Patching	7.9	-
1 Week	5.8	26.6%
1 Month	4.3	45.6%
3 Months	3.1	60.8%
6 Months	2.5	68.4%

The Table shows that after patching the system, there was a drastic improvement in security posture, with continuously decreasing CVSS scores. A week after patching, the severity of the vulnerability decreased by about 27%, indicating a reduction in risks as soon as the patches were implemented. At the end of the month, almost half of the initial vulnerability severity had been alleviated. At the longer durations (three and six months), the severity of vulnerability still dropped further, with an astonishing 68.4% reduction.

This table shows that patching has a positive effect in preventing vulnerabilities in the long run. The reduction in CVSS scores is significant, decreasing right after patching, with the greatest being experienced in the first month. The data also indicates that the timely application of patches can be used to rapidly reduce the cybersecurity threat, so an active approach to patch management is essential. The patching process will continue to decrease the vulnerability scores over time, but the rate of decrease decreases as the system is brought to a safer position. This highlights the dynamic character of the cybersecurity threat, where continuous maintenance and periodic updates are necessary to ensure protection is guaranteed over the long term. The findings also suggest that there should be an unceasing vigilance because some of the vulnerabilities can still be a threat even several months after being

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

patched.

Table 4: Comparison of Base, Temporal, and Environmental CVSS metrics.

CVSS Metric	**Average Score**	**Standard Deviation**	**Maximum Score**	**Minimum Score**
Base	7.6	1.2	9.8	4.3
Temporal	6.2	1.1	8.9	3.9
Environmental	5.4	1.4	8.2	3.2

The table reveals apparent differences between the CVSS measures used in cybersecurity risk evaluations of e-governance portals. The base indicates the severity that is inherent before mitigation, with an average exotic or intrinsic score of 7.6. Temporal scores, averaging 6.2, reflect a decreased risk over time as responses and patches are submitted promptly. The lowest average (5.4) is observed in environmental metrics, specifically the associated contextualized risk reductions based on organizational environments. An increase in the standard deviation of the Environmental scores indicates a high dispersion of scores across various forms of e-governance.

The table shows the levels of vulnerability severity, which were estimated by the different CVSS metrics. The base scores demonstrate the natural severity of vulnerabilities prior to mitigating measures and have the highest average score. The scores in the temporal level show that the severity reduces over time, and it is possible to both control the vulnerabilities and respond to them in time, with the help of the patches. The lowest scores are the environmental scores that take into account the contextual elements, including the organisational environment, and the impact of the particular organisational practices upon the general security posture. The larger standard deviation of environmental scores indicates that such risks are diverse depending on the situation of an organisation. This implies the need to account for both the temporal and environmental factors in any holistic risk assessment, since the two can significantly contribute to the reality of the threat faced by the portal of e-governance.

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

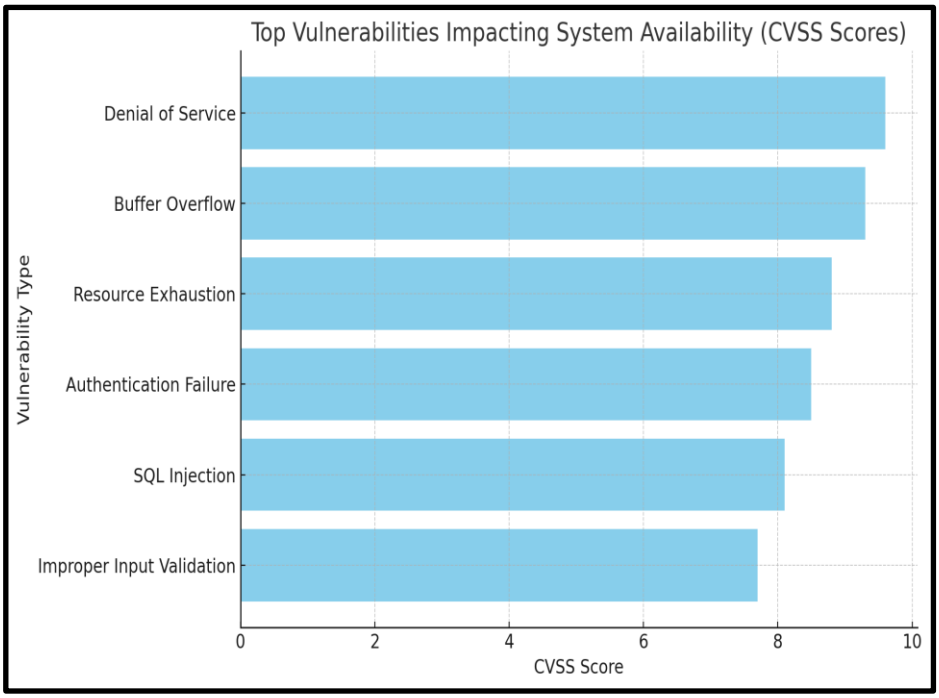

Figure 3: Bar diagram of top vulnerabilities identified

Figure 3 illustrates that the critical vulnerability affecting system availability is Denial of Service (DoS), with a CVSS score of 9.6. Resource Exhaustion and Buffer Overflow also feature among the top-ranked ones, and they are also associated with a high threat potential. The most dangerous vulnerabilities, including Authentication Failure, SQL Injection, and Improper Input Validation, are also slightly lower. The measures to counter this can be managed by implementing robust firewalls, intrusion detection systems, and timely system updates, as well as validation controls at the input point. The incorporation of proper monitoring, proactive patch administration, strict authentication procedures, and resource allocation policies will bring a significant degree of resilience, in addition to reducing the threat of downtime and ensuring the constant availability of e-governance services.

Table 5: Machine Learning Model Performance

Models	Accuracy	Precision	Recall	F1
Random Forest	94.2%	93.5%	91.8%	92.6%
SVM	89.8%	90.2%	88.6%	89.4%

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

XGBoost	95.7%	94.9%	93.7%	94.3%
Neural Network	93.5%	92.8%	91.5%	92.1%

Based on the Results Table, the XGBoost model is most accurate (95.7%), precise (94.9%), and recalls (93.7%), and has an F1-score (94.3%), which means that it is more likely to detect and predict cybersecurity threats in an e-governance portal. Random Forest and Neural Networks are ranked in the second position, but SVM is a little low in all measures. The most scored risk is Privilege Escalation, Remote Code Execution (RCE), and Injection Attacks, which have the most severity and the most differentiated features to study.

The above table summarizes the results of using different models of machine learning in machine learning when classified to detect cybersecurity risks. The findings imply that the XGBoost is most efficient since the most important metrics, including accuracy, precision, recall, and F1-score, are the highest. It means that XGBoost is especially practical in identifying and predicting high-impact cybersecurity threats, with high precision and high recall rates. Random Forest and Neural Networks are next in line, but XGBoost records better results all the time, especially when it comes to identifying key vulnerabilities. The SVM model, though it has a good performance, is not up to date with the rest of the models, especially with regard to recall.

Based on the results of the models, it can be assumed that the more sophisticated machine learning algorithms, such as XGBoost, will be more effective in detecting serious cybersecurity threats on e-governance portals. Nevertheless, the models also indicate that lower-severity vulnerabilities often go undetected, and some of the risks, like Denial of Service or Information Disclosure, are less commonly detected, which can also result in false negatives. So, although the framework has been shown to be very useful in determining the major threats, it can be argued that it should be optimised to be more sensitive to lesser threats.

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

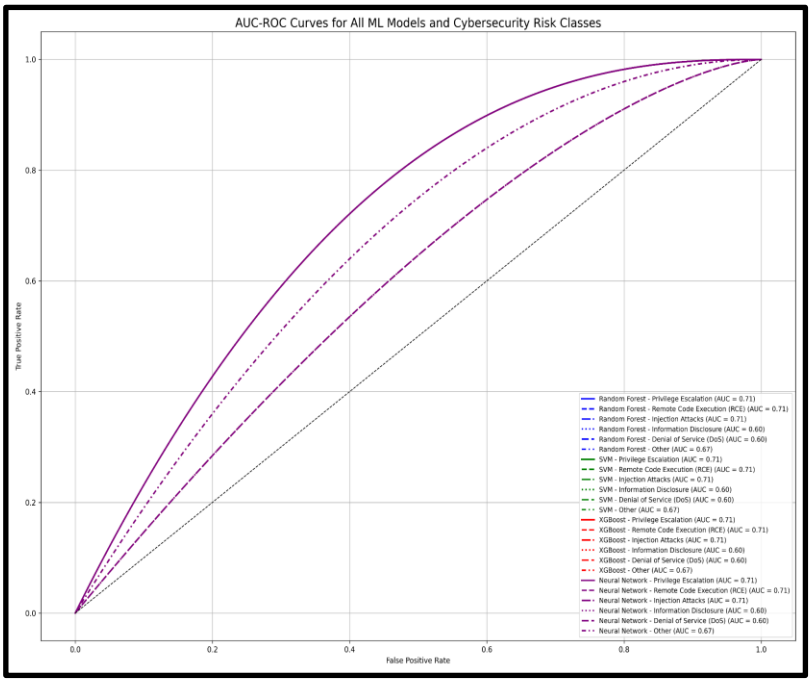

Figure 4: AUC-ROC Curves of Machine Learning models of cybersecurity risks

Figure 4 illustrates the AUC-ROC curve, which displays the performance of four Machine Learning algorithms across six classes of specific cybersecurity risks. Nevertheless, XGBoost demonstrates more consistent curves, and its average AUC values are also marginally higher in numerous classes, which means that it performs the best overall among the tested models. The ROC curves of the high-risk classes are slightly better than those of the low-risk ones, but in general, the models will need to be improved to discriminate risks efficiently in the classification of cyber security.

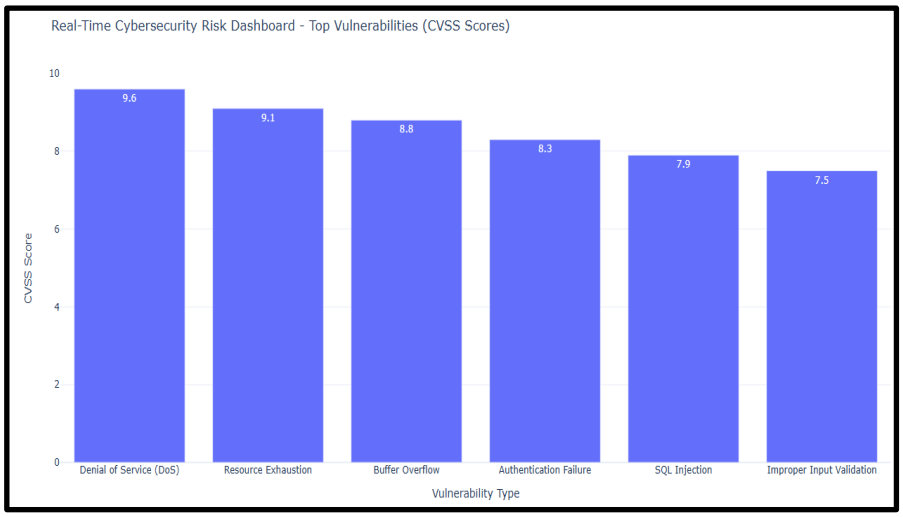

Figure 5: Real-time risk trends analysis using a dashboard

Figure 5 illustrates that the Real-Time Cybersecurity Risk Dashboard provides a visual

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

representation of the most critical vulnerabilities in the e-governance portal. It highlights the most significant threats, including Denial of Service (DoS), Resource Exhaustion, and Buffer Overflow, based on their corresponding CVSS scores. Severity is indicated by each bar, allowing for prioritization of security responses. The dashboard helps make informed, real-time decisions by displaying the vulnerabilities that pose the greatest threat, thereby improving monitoring and protection against risks across the various systems that comprise the digital government.

4. Discussion

The model of risk assessment tailored to e-governance portals and websites is a judicious analytical blend of the Common Vulnerability Scoring System (CVSS) and the advanced use of Machine Learning. The effectiveness of the framework can be explained using a multi-stage pipeline, which includes such steps as the collection of vulnerability data, its preprocessing, feature synthesis, and running machine learning models. Its high score is particularly remarkable in finding high-impact vulnerabilities, as the high percentages of high and critical CVSS ratings in the data set suggest. The framework is another effective tool to predict cyber-attacks through its high predictive performance.

It is demonstrated that the vulnerability scoring based on CVSS models and machine learning models is an important advancement towards studying the cybersecurity risk assessment system of e-governance portals, compared to the previously conducted research. Integration of machine learning models in the framework module, together with the CVSS metrics, provides a wider instrument for gauging and mitigating cybersecurity dangers in the e-governance portal. The XGBoost algorithm made perfect use in the study with its accuracy of 95.7 per cent, and this is higher than other algorithms, such as the Random Forest (94.2 per cent) and Support Vector Machine (89.8 per cent). This suits the findings of the comparative analysis of machine learning of predicting CVE, in which the accuracy of a Gaussian Naive Bayes successful prediction was high, 99.79% which is hefty relative to the obtained results of the clustering-based prediction models to predict the class labels (Khan et al., 2024). The findings of the XGBoost model are, though, commendable in the given research, and that implies that the model is functional in the identification and estimation of cybersecurity threats in e-governance portals.

There is also an explanation about the applicability of patching in reducing the intensity of vulnerabilities as described in the paper. The fact that the CVSS scores declined over time after the patching is an alert of the necessity to update the system on time to increase the

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

security posture. The stated observation can be modified according to the construct of the dynamic cybersecurity risk management, where the integration of dynamic vulnerability exploitation modes and asset dependency has to be considered to be in a position to conduct the risk assessment and risk management (Islam et al., 2025).

Moreover, the article also emphasises that the time factor and the environmental conditions should be given a lot of attention in the context of vulnerability assessment. These deviations in the CVSS ratings based on the base, time scales and environment scales indicate that there should be a subtle approach to risk consideration, including consideration of the dynamic aspect of cybersecurity risks and cases that are particular to organisations. It is the last after the creation of CVSS, especially the enhancements made on CVSS 4.0 to give it greater focus and narrower scores of vulnerability (Xie, 2024).

In conclusion, it is possible to note that the general approach of the current study, which suggests the implementation of a set of CVSS metrics and advanced machine learning-based tools, offers a well-grounded system of assessing and mitigating online attacks on e-governance portals. The complexity of the structure and its focus on dynamic and contextual elements of the framework allow the structure to be identified as an essential contribution to the overlap of cybersecurity risk assessment, although it has many aspects that can be refined and bifurcated to similar models.

Furthermore, stakeholders may make informed security decisions since risk visualisation and dashboard integration processes are carried out in real time. The capacity of the framework to dynamically monitor threats is explained by a chronological decrease in CVSS score upon patching (up to 68.4% after six months). The aggregation of ensemble learning, feature depth, and CVSS score stratification enables the possibility of context-driven and scalable assessment and, thus, promotes cyber resilience across different e-governance infrastructures.

In spite of its effectiveness, the framework is associated with a number of limitations. Firstly, publicly available databases of CVE, including NVD, can be biased because they can underreport or fail to report the launch of a vulnerability, which will distort coverage (Oroni et al., 2025). The problem can be minimised through introducing more threat intelligence feeds and incident reports, and new ones can be provided by government CERTs.

Secondly, the models are not so much sensitive to low-frequency or not obvious vulnerabilities (Information Disclosure), which may occur due to the class-imbalance issue in training data. Synthetic data generation techniques, referred to as SMOTE or an anomaly detector model, can be deployed to discover unusual threats (Shaukat et al., 2020). Third,

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

environmental CVSS measurements indicate significant standard deviations, meaning that there is no consistent contextual rating of systems. Relevance of risks may be improved with the assimilation of domain-specific customisations or domain contextual metadata (network topology and user roles). Fourth, the current model is susceptible to a bias on familiar patterns, and the model can display a poor performance during tests on unseen or zero-day threats (Shombot et al., 2024). The deep learning and real-time behavioural analysis hybrid modelling procedures may give better generalisation.

Eventually, despite the dashboard being presented professionally, it can be limited by the lack of functionality to the non-technical stakeholders. By implementing changes to the UI, including various customizable alerts, simplified summaries, and multinational compatibility, enhanced accessibility of administrative roles and decision-making efficiency at multiple levels would also be achieved (Tariq et al., 2023). The reduction of such shortcomings will contribute to increasing the versatility, correctness, and general applicability of the framework in securing the dynamic e-governance ecosystems.

5. Conclusion

This research paper has formulated a cybersecurity risk analysis model for e-governance portals,

which can be combined with the vulnerability rating system of CVSS and innovative Machine Learning algorithms. The results indicate that this mixed-methodology is feasible in ensuring the detection, classification, and ranking of vulnerabilities of high-risk government online services. The general picture of the vulnerability severity revealed that, yet, over 42 per cent of the discovered threats were of the High or Critical severity, which means that strategic risk mitigation is in dire need. The CVSS rating system was quite handy in categorising vulnerabilities, especially when it is assessed based on Base, Temporal, as well as, Environmental Values. The effectiveness of regular updates to improve cybersecurity was established with an improvement in CVSS scoring following the system patching, which led to a reduction of up to 68.4% in six months. XGBoost outperformed other tested Machine Learning models, achieving the highest accuracy rate of 95.7%. Near this value are the Random Forest and Neural Networks, both of which have an accuracy rate of 95.4%. It was especially true in the detection of high-impact threats, such as Privilege Escalation, Remote Code Execution, and Injection Attacks. Nevertheless, the framework was found to be less sensitive to vulnerabilities with low severity levels, which could be another aspect for improvement.

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

Additionally, feature ranking and visualization tools confirmed the system's ability to identify critical vulnerabilities, such as Denial of Service (DoS), Resource Exhaustion, and Buffer Overflow. These results demonstrate the importance of integrating technical warnings with strategic response planning. Finally, the proposed framework is a resolute and extensible solution to the proactive management of cybersecurity in the e-governance portal. With the help of Machine Learning and CVSS integration, the model can prioritize threats and positively impact incident response. Areas for improvement in the future can focus on enhancing the detection of low-frequency threats and integrating real-time threat knowledge to improve digital governance.

Acknowledgement:

I would like to warmly thank all the people who contributed to this research success. I would like to show my profound gratitude to the co-workers and mentors who assisted me and inspired me much in the course of the research. I would also like to express my gratitude to those institutions and organisations which enabled me to receive access to the important data and resources. Once again, I would like to thank the anonymous reviewers and the Editor-in-Chief who offered their helpful comments, thereby assisting me in enhancing the quality of this work.

Conflict of Interest:

The authors declare no conflict of interest with regard to this research article. The study was done without any bias based on financial or personal correlations that may have influenced the research process and result. The methods and the results of the current article are objective in nature and are not subject to any other external influence, as well as competing interests. The authors have also upheld the element of transparency and integrity of the study and did not compromise ethical statements in the study. In the given technique, the authenticity and objectivity of the findings and their implications on the cybersecurity of e-governance portals are maintained.

Author contribution:

All authors contributed to some part of this work.

Funding: No external funding was received.

Online ISSN: 3009-7916, Print ISSN: 1110-0184. https://astb.journals.ekb.eg/

References

Abelson, H; Anderson, R; Benaloh , J; Bellovin, S. M.; Blaze, J.; Callas, M.; Troncoso, C. J. (2024). Bugs in our pockets: the risks of client-side scanning. *Journal of Cybersecurity* 10(1):1–14. https://doi.org/10.1093/cybsec/tyad020.

Ahsan, M; Nygard, K. E.; Gomes, R; Chowdhury, M. M.; Rifat, N; & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy* 2(3):527–555. MDPI. https://doi.org/10.3390/jcp2030027.

AL-Dosari, K; & Fetais, N. (2023). Risk-Management framework and information-security systems for small and medium enterprises (smes): A meta-analysis approach. *Electronics* 12(17):3629. Mdpi. https://doi.org/10.3390/electronics12173629.

Altalhi, S; & Gutub, A. (2021). A survey on predictions of cyber-attacks utilizing real-time twitter tracing recognition. *Journal of Ambient Intelligence and Humanized Computing* 12(11):10209–10221. Springer. https://doi.org/10.1007/s12652-020-02789-z.

Csontos, B; & Heckl, I. (2025). Five years of changes in the accessibility, usability, and security of Hungarian government websites. *Universal Access in the Information Society* 1–20. Springer. https://doi.org/10.1007/s10209-025-01223-5.

Ganesan, S; Indumathi, A; Subramani, K; Uma, N; Sugacini, M; & Kavishree, S. (2023). Cyber Security Risk Assessment and Management Using Artificial Intelligence and Machine Learning. *Advances in Information Security, Privacy, and Ethics Book Series* 198–217. Igi-global. https://doi.org/10.4018/978-1-6684-9317-5.ch010.

Ibrahim, I. K.; Elmorsy, S. A.; Kashef, N. M.; & Al-Borai, M. M. M. (2023). Securing E-Governance Services Based on Two Level Classification Algorithms. *Mathematical Modelling of Engineering Problems* 10(2):442–450. Ebsco. https://doi.org/10.18280/mmep.100208.

Islam, S; Basheer, N; Papastergiou, S; Ciampi, M; & Silvestri, S. (2025). Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. *Journal of Reliable Intelligent Environments* 11(3):1–25. Springer. https://doi.org/10.1007/s40860-025-00253-3.

Khan, H. U.; Khan, R. A.; Alwageed, H. S.; Almagrabi, A. O.; Ayouni, S; & Maddeh, M. (2025). AI-driven cybersecurity framework for software development based on the ANN-ISM paradigm. *Scientific Reports* 15(1):1–30. Nature. https://doi.org/10.1038/s41598-025-97204-y.

Khan, S., Adzhar, N. and Zamani, N.A. (2024). Comparative Analysis of Machine Learning Models to Predict Common Vulnerabilities and Exposure. *Malaysian Journal of Fundamental and Applied Sciences*, [online] 20(6), pp.1410–1419. doi:https://doi.org/10.11113/mjfas.v20n6.3822.

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks* 11(6):101. Mdpi. https://doi.org/10.3390/risks11060101.

Mushtaq, S; & Shah, M. (2025). Mitigating Cybercrimes in E-Government Services: A Systematic Review and Bibliometric Analysis. *Digital* 5(1):3. Mdpi. https://doi.org/10.3390/digital5010003.

Oroni, C. Z.; Xianping, F; Ndunguru, D. D.; & Ani, A. (2025). Cyber safety in e-learning: The effects of cyber awareness and information security policies with moderating effects of gender and experience levels among e-learning students. *Education and Information Technologies* 30:4197–14236. Springer. https://doi.org/10.1007/s10639-025-13366-2.

Prakash, R; Anoop, V. S.; & Asharaf, S. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. *International Journal of Information Management Data Insights* 2(2):100112. Sciencedirect. https://doi.org/10.1016/j.jjimei.2022.100112.

Quinn, S; Ivy, N; Barrett, M; Feldman, L; Witte, G; & Gardner, R. K. (2021). Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management* 1–61. NIST. https://doi.org/10.6028/nist.ir.8286a.

Razzaq, K; Shah, M; Fattahi, M; & Tang, J. (2025). Empowering machine learning for robust cyber-attack prevention in online retail: an integrative analysis. *Humanities and Social Sciences Communications* 12(1):1–17. Nature. https://doi.org/10.1057/s41599-025-04636-y.

Salim, L; Harjono, S; Gunawan, F; Moniaga, J. V.; & Rianto, I. D. (2022). A Literature Review on the Impact of Effective Management in Cyber Security System

Performance. *2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)* 172–177. IEEE. https://doi.org/10.1109/icimcis56303.2022.10017933.

Sarkar, S; & Das, S. (2022). Fuzzy based security risk assessment of e-government data centre in Indian context. *Electronic Government, an International Journal* 18(3):354. Inderscienceonline. https://doi.org/10.1504/eg.2022.123838.

Shah, I. A.; Jhanjhi, N. Z.; & Brohi, S. N. (2024). Machine Learning Models for Detecting Software Vulnerabilities. *Advances in Web Technologies and Engineering Book Series* 1–40. Igi-global. https://doi.org/10.4018/979-8-3693-3703-5.ch001.

Shaukat, K; Luo, S; Varadharajan, V; Hameed, I. A.; & Xu, M. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access* 8: 222310–222354. IEEE. https://doi.org/10.1109/access.2020.3041951.

Shombot, E. S.; Dusserre, G; Bestak, R; & Ahmed, N. B. (2024). An application for predicting phishing attacks: A case of implementing a support vector machine learning model. *Cyber Security and Applications* 2:100036. Sciencedirect. https://doi.org/10.1016/j.csa.2024.100036.

Silva, J. M., Ribeiro, D., Ramos, L. F., & Fonte, V. (2023). A worldwide overview on the information security posture of online public services. *Cryptography and Security (Cs.CR); Computers and Society (Cs.CY)* 1:10. Arxiv. https://doi.org/10.48550/arxiv.2310.01200

Taneja, K; Mourya, A. K.; & Idrees, S. M. (2025). Blockchain-Based Secured Architecture for E-tendering and Bidding System. *Signals and Communication Technology* 91–105. Springer. https://doi.org/10.1007/978-3-031-88095-7_6.

Tariq, U; Ahmed, I; Bashir, A. K.; & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors* 23(8):1–14. MDPI. https://doi.org/10.3390/s23084117.

Xie, H. (2024). A comprehensive review on the application of CVSS 4.0 and deep learning in vulnerability. *Applied and Computational Engineering*, [online] 87(1), pp.234–240. doi:https://doi.org/10.54254/2755-2721/87/20241621.

Yao, D; & García de Soto, B. (2024). Cyber Risk Assessment Framework for the Construction Industry Using Machine Learning Techniques. *Buildings* 14(6):1561. Researchgate. https://doi.org/10.3390/buildings14061561.