Universal Library of Engineering Technology Research Article

ISSN: 3064-996X

Open Access | PP: 33-41

DOI: https://doi.org/10.70315/uloap.ulete.2023.006

Performance Analysis of Machine Learning Models for Cybersecurity Risk Classification in IT Projects

Prasanth Varma Addepalli[1], Sridhar Reddy Bandaru[2], Dhuli Shyam[3], Prabu Manoharan[4], Muzaffer Hussain Syed[5], Uday Kumar Ragireddy[6]

[1]Lead Data Architect/ Engineer, Federal Motor Carrier Safety Administration, Atlanta, Georgia.

[2]Program Management, IT, Microsoft, Senior ACE Engineer, Redmond, WA.

[3]Business Application, IT, Nagase Holdings America Corp, Manager, Application & Software Development, NYC, NY.

[4]Information Technology, Bourns Inc, HRIS Manager, California, USA.

[5]IT Project Lead, Vdrive IT Solutions Inc.

[6]Sr Technical Program Manager, Vdrive IT Solutions, Inc, Richardson, Texas.

Abstract

The recent improvement of cyber threats in the contemporary IT setting has aggravated the necessity to establish effective ways of classifying and managing cybersecurity risks. Increasing complexity in systems and more advanced attacks require more advanced analytical tools that can identify risks in time and properly. This paper carries out an extensive examination to assess machine learning (ML) systems in efficient cybersecurity risks identification in IT ventures. The study focuses on the nature of risk environments, supervised and unsupervised methods in ML, and how models, including SVM, Random Forest, Logistic Regression, and the use of clustering-based methods, play their role to determine vulnerabilities. Also, the paper explores such critical issues as skewed data, malicious manipulation, model drift, and human or organizational biases that affect risk outcomes. The detection of threats and decision-making but still have limitations in terms of scaling, interpretability, and deployment in the real world. Combining the ideas of risk assessment and the power of ML, this study indicate that ML has massive opportunities to enhance the cybersecurity risk management as long as the operational and technical issues are tackled in a systematic manner.

Keywords: *Cybersecurity, Artificial Intelligence (AI), Information Technology (IT), Risk Classification, Machine Learning (ML).*

INTRODUCTION

Hackers, cybercriminals, and rogue workers have taken notice of the extremely sensitive material, hoping to steal it and harm the organization's reputation. Organizations all over the world constantly update and develop their information systems, so it's critical to implement sufficient security and control measures to guarantee that all sensitive data is safe within their systems to preserve its confidentiality and integrity [1]. Organizations are now aware of their obligations to safeguard their information and physical assets because there is ample evidence that data security threats are growing annually, and most significantly, the impact these threats have on the organization has been severe. The goal of cybersecurity is to ensure that user assets and the organization's security resources are obtained and protected against specific physical hazards in the online environment. Availability, confidentiality, and integrity which can include nonrepudiation and genuineness—are some of the general safety goals [2]. Information security ideas and those interpretations share certain commonalities. the definition of information security and then argue that, according to conventional definitions, the scope of cyber security is wider than that of information protection.

Information security (InfoSec) risks, which are focused on ensuring the availability, confidentiality, and integrity of information, are created when technology is used to access information. More specifically, ISRM is the process of controlling these risks; it is the method of continuously identifying, assessing, treating, and keeping an eye on hazards in order to achieve risk acceptance [3]. Security threat management has become a crucial component in the current IT development since projects usually encounter various vulnerabilities that can be dynamic. Prioritizing the risks can enable the teams to know where the weak points can be and how they might affect the system performance or how they might affect the data protection. IT teams can strategize response actions, enhance decision-making, and overall project-wide security by classifying risks into distinct categories to respond proactively to risks. With the increasing involvement of ML in security operations, the assessments of alternative models in identifying and classifying possible threats in IT systems are useful in identifying the most efficient techniques. This information enables teams to select the models with more accuracy and quicker detection.

Through the incorporation of well-organized risk evaluation processes, IT projects more resilient and more secure.

AI is described as intelligence created artificially that gives a computer or machine the capability to solve difficult and complex tasks. Information technology and physiological intelligence are combined to create AI, which may be employed computationally to accomplish objectives [4]. The capacity to think through memory formation, comprehension, pattern recognition, adaptive decision-making, and experience-based learning is intelligence. ML is also relevant in enhancing IT cybersecurity as it empowers the systems to respond to data, thereby automatically identifying abnormal or malicious behaviors. Through the analysis of the trends in network behavior, user behavior, and system logs, ML [5] models can detect threats that overlooked by traditional rule-based methods. These methods help to multi-track the malware, phishing, and intrusion attempts faster and less manual attention should be given. With the development of cyber threats, ML constantly becomes more flexible, and it is a powerful tool of proactive and smart security management in contemporary IT-based environment.

Structure of the Paper

The paper is organized is as follows: Section II describes the cybersecurity risk environment in IT projects. Section III describes machine learning systems and methods of risk classification. Section IV talks about the major issues about risk classification using ML. Section V is a review of the relevant literature and Section VI is the conclusion and future directions.

IT PROJECTS IN CYBERSECURITY RISK ENVIRONMENT

Risk management has the potential to significantly increase the final success of IT projects, which are fraught with risks. One of the main responsibilities of IT is risk management governance [6]. However, because the output is intangible that is, it is difficult to assess the progress by looking at the artifact being constructed software project management is more difficult to manage than other forms of software engineering. This is in contrast to, say, civil engineering projects. Furthermore, since every major project is frequently unique, prior expertise may not be very useful in foreseeing issues, and the quick development of technology may render prior knowledge outdated. Several frameworks and standards provide substantial information about dealing with cybersecurity threats and using best practices in cybersecurity, governance, and project management.

Cybersecurity Risk Types At IT Project Stages

Risk is a contingency that may arise from a system malfunction or failure that could jeopardize assets, such as people or the environment, and impact the organization's capacity to achieve its operational, financial, and strategic objectives [7]. Cybersecurity in IT is important because of the risks and vulnerabilities as shown in Figure 1.

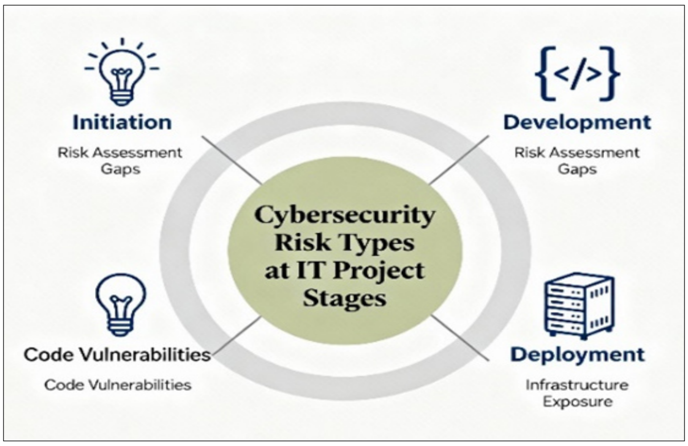

Fig. 1. Risks in IT Projects

- **Development Risks:** Risk can arise from miscommunication or because of the basic nature of the Research and Development project [8]. Development risks are the security concerns that arise in creating and design of software of an IT project. The commonly occurring risks are based on the insecure coding, wrong validation, application of weak third-party libraries and absence of the security-motivated reviews. These vulnerabilities are more difficult and expensive to correct in the later stages of the SDLC when they have been introduced early. Unless these weaknesses are handled with urgency, they may end up causing severe security breaches when the system is implemented. Consequently, security controls should be incorporated into development to minimize the risk of cybersecurity in the long-run.

- **Deployment Risks:** DRRI is a popular tool in measuring the aspects of risk and resilience due to deployment in war veterans [9]. The deployment risks can be defined as the perceived threats, failures, or vulnerabilities that occur when a system, product, or a technological solution, is transferred out of the development phase and into a live or operational environment. Such risks are likely to include configuration, integration, or under-testing, unforeseen user behavior, decreased performance, security, or compatibility with existing infrastructure. Unless dealt with appropriately, the deployment risks may cause data loss, system downtime, lowered performance, and service delivery disruptions.

- **Operational Risks:** Aligning cyber security with operational risk requires increasing IT and risk knowledge transfer. Mutual understanding and comprehension may be fostered by staff rotation and shadowing. Along with recruitment and incentive programs to foster collaboration, joint competency centres must also be taken into account. Senior management should supervise and promote formal knowledge transfer programs.

Factors That Affected Vulnerability In IT Project Ecosystems

Critical infrastructure operators have difficult challenges when it comes to risk management and protective scheme selection. In an organization's security ecosystem, vulnerabilities are crucial because they affect the assets, threats, countermeasures, and cost-benefit analysis. Depending on the type of assets they impact, vulnerabilities may fall into one of several classifications. A critical component of risk management is identifying and assessing vulnerabilities, as seen in Figure 2.

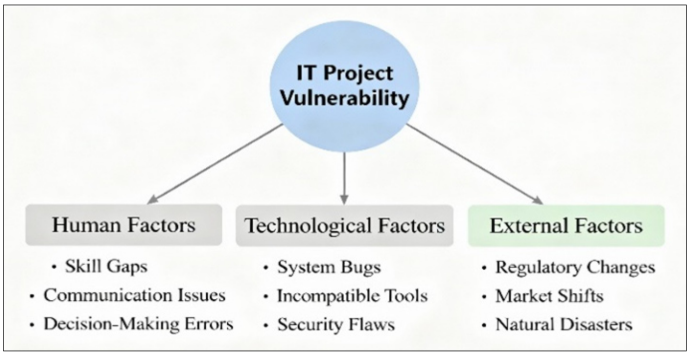

Fig. 2. Factors in IT Projects

- **Human Factors:** Every employee has a responsibility to safeguard an organization's information. Education, training, and knowledge are an ongoing issue in human factors and security—possibly the finest non-technical solutions available. Security-related concerns and requirements must be incorporated into regular business operations through clear policy and staff training [10]. Ignorance rather than malevolent intent is the root cause of many insider issues, yet this is just as risky since unintentional mistakes can have significant effects, and connections can enhance the potential scope of harm.

- **Technological Factors:** There is a major impact of technological factors on vulnerabilities in the IT project ecosystem which are usually due to poor software design, poorly configured systems, old component, and poor testing. The mapping of the software vulnerabilities territories is one of the essential steps towards creating an efficient security solution. It is hard to resist a threat with which one is not familiar. Unpatched systems, broken-third party libraries, and insufficient security-by-design are some of the issues that increase the attack surface. Those technological gaps indicate why the development standards should be stronger and vulnerability management on a continuous basis is necessary.

External Factors: External factors lead to vulnerabilities in the IT project ecosystems by bringing in risks that are not necessarily within the organization scope of control. The undiscovered weaknesses may be transferred to the project environment by third-party vendors, cloud services, and supply-chain components. Implemented regulatory changes, industry compliance requirements and geopolitical conditions can also introduce new security forces or reveal loopholes in the current controls. Also, the prevalence of cyber-attacks on common infrastructures, platforms or service providers may have an indirect effect on project security. These pressures underline that it is necessary to have solid vendor assessment and ongoing environmental scanning as well as robust supply-chain security tools

Table 1. The Summary of Cybersecurity Risk Environment in IT Projects

Category	Description	Causes / Contributors	Impact on IT Projects	Mitigation / Best Practices
Development Risks	Security vulnerabilities that were added during software development and coding.	Lack of insecure coding, insecurity in validation, insecure libraries, or missing security audits.	he improbable vulnerabilities later, the probability of breach later, and the remediation cost is higher.	Security Testing, SDLC practices, Automation.
Deployment Risks	Risks that arise during the deployment of systems when they move between the development and live systems.	Incorrect configurations, integration, lack of testing, performance.	Service failure, system failure, data loss, compatibility.	Deployment preparation, checking, testing the environment, back-up measures.
Operational Risks	Risks associated with daily use and operation of the system.	Lack of knowledge transfer, role ambiguity, human factors, lack of coordination.	Failure of operations, occurrence of security incidents, lack of consistency in the processes.	Personnel rotation, training, competency centers, effective managerial control.
Human Factors	Weaknesses due to the actions of human beings, lack of sensitivity and unintentional acts.	Training deficiency, insider mistakes, bad policies, procedure ignorance.	Information breaches, mistakes in configuration, exposure to attacks.	Sensitization, good policies, life-long learning.
Technological Factors	Security design, architectural and technical vulnerabilities.	Unsecured systems, insecure design, old components, poor testing.	Increased vulnerability to attacks, persistent vulnerabilities.	Code standards, vulnerability management, and secure-by-design.
External Factors	Uncontrollable risk factors that are external to the organization.	Vendors Third-party vendors, cloud dependencies, supplier supply-chain concerns.	Gaps in compliance, proximate violations, dependency violations.	Vendor evaluation, supply-chain protection, compliance with regulation, outsourcing.

MACHINE LEARNING SYSTEMS IN THE CYBERSECURITY RISK CLASSIFICATION

Cybersecurity is a collection of methods and instruments designed to prevent unwanted access, modification, or destruction of computers, networks, software, and data [11]. A computer security system and a network security system are combined to produce a network security system [12]. ML is strongly associated with computational statistics, a branch of AI that deals with using technology to make predictions. It is strongly associated with mathematical optimization, which supplies the field with theory, methods, and application areas.

Machine Learning Approaches

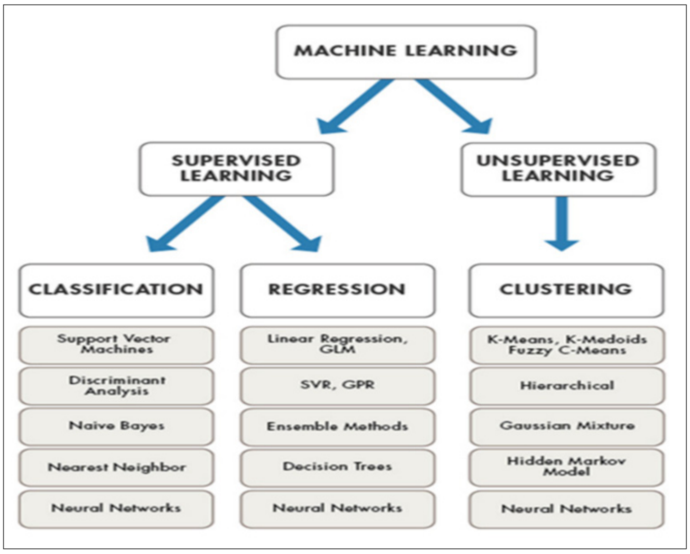

Fig. 3. Machine Learning Approaches for Risk Classification

Supervised and unsupervised are the two basic methods of ML. Important information is contained in labeled data for supervised learning [13]. Figure 3 illustrates that classification is the most common activity in supervised learning, and hence most frequently utilised in IDS. This is despite the fact that human data labelling is expensive and time-consuming. Therefore, the most significant obstacle to supervised learning is an absence of labelled data. However, by using useful feature information in unlabeled data, unsupervised learning facilitates the collection of training data.

Supervised Learning

Supervised learning is based on training a data sample from an identified data source in advance. models that use AI to identify underlying patterns and correlations [14]. Creating a model that can accurately anticipate fresh real-world data is the goal of the learning process. Supervised learning trains a model of the relationship between inputs and outputs using ground truth data. The labeled supervised learning datasets are ground truth data. As demonstrated in Figure 4, trained models use their knowledge of that data to forecast new, unseen data.

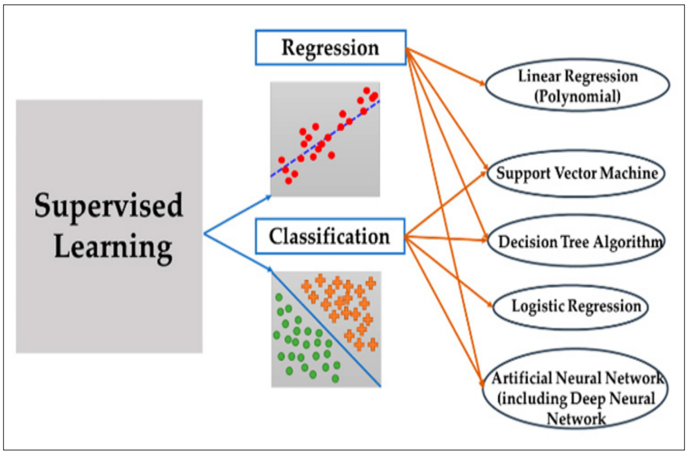

Fig. 4. Supervised Learning Approach

Unsupervised Learning

The use of unlabelled input and the generation of analytical data are both made easier by unsupervised ML approaches. The state of the art in unsupervised ML has been greatly enhanced by recent breakthroughs in factor analysis, latent models, hierarchical learning, clustering approaches, and outlier identification [15]. Recent advances in unsupervised ML, including the advent of “DL” methodologies, have substantially improved ML. These methods simplify the examination of raw data without necessitating much engineering or domain knowledge for feature generation.

Machine Learning Models and Techniques for Risk Classification

Studies are concentrating on ML and its extensive collection of tools and methods to detect, thwart, and react to complex cyberattacks due to the growing threat of cybersecurity [16]. ML [17] can be used to give analytical-based methods for attack detection and response in a number of cyber security fields. Security procedures can be improved by automating repetitive operations and allowing security analysts to do semi-automated tasks more quickly. Below are a few well-liked ML models and methods for cyber security:

Support Vector Machine (SVM)

SVM are among the most reliable and accurate ML algorithms. Both SVR and SVC are essential parts of it. Decision boundaries are the foundation of the SVC. A decision border divides an instance set into two halves according to their class values. Binary and multiclass classifications are both supported by the SVC. The ideal separation hyperplane is defined by the support vector, which is the point that is closest to the separation hyperplane. As part of the categorization procedure, the feature space locations on either side of the separation hyperplane denote different classes of mapping input vectors.

Random Forest (RF)

An RF is a collection of decision trees that, before producing a single, cohesive answer, takes into account the outcomes of each tree. Every decision tree is a conditional classifier; a condition is compared to one or more characteristics of the data under study at each node of the tree that is visited from the top. These work well with big data sets and multiclass issues, although deeper trees could lead to overfitting.

K-Nearest Neighbor (K-NN)

K-NN is a supervised learning method that does not rely on parameters and may be used for both classification and regression. There are no presumptions made about the underlying distribution. Rather, it finds the k nearest training examples in the feature space that match the new observation and makes a prediction of the target variable according to majority label or mean whether it is a task classification or regression.

Clustering

Data is clustered using a similarity metric in this type of unsupervised learning. Clustering algorithms can learn from audit data, thus the system administrator does not need to explicitly identify the different attack classes [18]. the real-time detection of signatures using clustering methods. Both normal and disordered network data were generated by the density-based clustering scheme known as the SLCT. Two distinct clustering schemes are available The alternative method can be used to detect both normal and assault scenarios, as well as to supervised identify ordinary traffic.

Logistic Regression (LR)

LR is another common statistical model based on probability that is used to solve classification problems. One common method for estimating probabilities in LR is the logistic function, which is often called the sigmoid function. As a general rule, the LR hypothesis limits the function to the integers 0 and 1 [19]. To determine the relationship between a dataset's independent factors and its categorical dependent variable, this type of classifier is used.

CHALLENGES IN MACHINE LEARNING BASED RISK CLASSIFICATION

Challenges encountered in classification of risk in ML include prioritizing the security and stability of models while dealing with noisy, imbalanced, and rapidly changing cybersecurity data [20]. ML classifiers are susceptible to high-performance adversarial attacks, data-poisoning, and model drift, and they may decrease their reliability [21] and accuracy. It is also hard to explain limited and hence difficult to trust the model outputs in critical IT project decision making. These issues demonstrate a necessity to have strong, transparent and flexible ML algorithms to be effective in classifying risks.

- **Security policy Promotion:** Information security rules are difficult for organizations to promote and spread [22]. The majority of IT managers reported that their companies had information security policies in place to handle various threats, but only a fraction of those companies had truly made this a culture among their workforce, according to research by the Economist Intelligence Unit.

- **Non-Compliance with Security Policy:** Security measures for sensitive information the general public views disobedience as more of a people problem than a technological one. Three categories of non-compliance behavior have been identified by researchers: malevolent behavior, negligent behavior, and unawareness. Negligent behavior is driven by the desire to violate an organization's security policy without endangering that organization, whereas malicious activity is largely driven by the goal to harm an organization's information assets.

- **Shadow Security:** The core idea behind "shadow security" is that "employees going around IT to get the IT services they want on their own." When these workers believe that compliance is beyond their capabilities or have a detrimental effect on their productivity, they take their own security precautions. A password security policy that mandates a complex password (12 characters minimum, including uppercase and symbol) may make it difficult for some employees to memorise the password. As a result, the password can be shown on the computer screen and scribbled on a sticky note.

- **CPS Security:** CPS Security refers to the protection of the whole environment, from the physical to the cyber, from information security to network security and privacy. In CPS, centralized architecture is using to connect devices [23]. There is a possibility of a threat that uses IoT devices as a tool to harm humans. So, one of the research challenges in CPS is to find measures to block the attack. also, the area in CPS is resource management in a dynamic environment to handle a large data volume with a complex decision-making algorithm and computation in the autonomous mode.

LITERATURE REVIEW

The literature review has shown that the proposed risk-based and automated security strategies are effective in terms of increasing threat detection and decision-making, however, its scaling, accurate model, and practical validation are still the challenges to address.

Le and Maple (2019) presented a systematic approach consisting of three modules: a knowledge-based system to aid in the detection of critical threats, a monitoring module to reveal changes in the security context of the CAV and its environs, and a simplified assessment module to record evolving risks and modify mitigations as required. Analyse CAV platooning via the lens of a case study [24].

Rahmati et al. (2018) offered Tyche, a secure development approach that leverages the risk-asymmetry in physical device operations to mitigate the risk that smart home app users face without adding additional decision-making burdens. All IoT platforms should implement Tyche's proposed risk-tailored permissions. Apps are granted access to devices at a granularity determined by the level of danger they pose when users utilise risk-based permissions. At first, a set of licenses made available by the well-known Samsung SmartThings platform [25].

Hong et al. (2017) suggested a dynamic risk propagation-based information security risk algorithm (ISRADRP). Information systems in the Energy Internet are initially divided into various divisions by ISRADRP based on their logical network location. Next, ISRADRP uses the RM algorithm to calculate the risk value of each partition without taking the danger propagation impact into account. Additionally, ISRADRP uses the Dependency Structure Matrix to determine the inner and outside propagation risk values for each division. Ultimately, the information system's overall risk value was determined and the security bottleneck was located. [26].

Henshel et al. (2016) suggested making cybersecurity decisions using a risk-based methodology. The process begins with a continuous risk-based security risk evaluation of the system and continues with the construction of several potential actions and the evaluation of their respective costs and benefits. Also, provide an example of how the method protected a SQL server against a SQL injection attack to prove its worth [27].

Gai, Qiu and Elnagdy (2016) developed a novel method for data classification utilizing a mix of supervised learning approaches to shield customers' or providers' sensitive financial information from prying eyes. In particular, the suggested DTRP approach bolsters the SEB-SIC model. The proposed method is a strategy for making predictions by training on past data [28].

Dorca et al. (2016) investigated the possibility of automating information security risk management and integrating it with software development firm processes using an Agile approach utilizing Kanban. An e-commerce company's relevant information security risks were used to evaluate the technique (Proof of Concept), and the results show improvements in the defined risk management SLAs better business response, and higher team productivity [29].

Table II is a summary of major papers on risk-based security methodologies, their focus, methods, findings, and limitations. In general, the literature demonstrates better threat detection and decision-making but still needs to address such issues as scalability, proper modelling, and minimal verification of the literature. The future work is associated with expanded deployment, more intelligent automation, and improvements based on ML.

Table 2. Summary of Recent Studies on Risk-Based Security Approaches

Reference	Study on	Approach	Key Findings	Challenges / Limitations	Future Directions
Le & Maple (2019)	Risk assessment and mitigation for Connected and Autonomous Vehicles (CAVs)	Three-module framework: knowledge-based threat identification, monitoring module, and dynamic risk assessment module; evaluated using CAV platooning case study	Supports continuous threat identification and dynamic mitigation adjustment; improves safety in changing CAV environments	Limited to CAV platooning scenario; real-world large-scale validation needed	Extend framework to more CAV applications and test in real environments
Rahmati et al. (2018)	Secure development in smart home IoT systems	Tyche: risk-based permissions grouped by risk levels to reduce user decision overhead	Efficiently limits risky app operations; improves user security without increasing cognitive load	Depends on accurate risk categorization; limited to SmartThings-style platforms	Apply risk-based permissions to broader IoT ecosystems; automate risk unit generation
Hong et al. (2017)	Information security risk in Energy Internet systems	ISRADRP algorithm: partitions system, computes baseline risk, adds propagation risk using Dependency Structure Matrix	Identifies security bottlenecks; captures dynamic propagation of risk across system partitions	Relies on accurate dependency modeling; may be complex for large networks	Improve scalability; integrate real-time monitoring for dynamic updates
Henshel et al. (2016)	Dynamic risk cybersecurity decision-making	Ongoing evaluation of risks and subsequent cost benefit analysis of possible course of action; applicable to SQL injection example	Has effective dynamic decision making; enhances system protection by making adaptive decisions	Computational complexity in the process of alternatives evaluation; could need professional tuning	Create automated risk prediction engines; integrate the ML-trained risk prediction

Gai, Qiu & Elnagdy (2016)	Secure classification of financial information	SEB-SIC model using supervised learning + DTRP algorithm for predictive risk classification	Enhances protection of sensitive financial data; accurately predicts high-risk information	Depends on quality of historical data; may need frequent retraining	Extend model to real-time financial environments; include deep learning
Dorca et al. (2016)	Integrating automated processes into agile development for managing information security risk	Agile + Kanban-based automated risk management framework tested in e-commerce environment	Improved team efficiency, faster business response, better SLA performance	Limited scope (single e-commerce PoC); manual configuration still required	Develop fully automated pipelines; evaluate across diverse industries

CONCLUSION AND FUTURE WORK

The increasing reliance of the digital infrastructures necessitates the need to reinforce the cybersecurity risk classification procedures among IT projects. The conventional security approaches are not always able to respond to the pace, the volume, and the complexity of the new cyber threats, which puts a big urgency on the intelligent and adaptable analytical responses. In this paper, a critical analysis of ML models has been carried out to learn more about its usefulness in detecting, classifying, and forecasting cybersecurity threats. The results indicate that ML models: SVM, RF, KNN, clustering, and logistic regression allow achieving a important development in the accuracy and efficiency of risk detection based on the analysis of behavioural patterns and system characteristics. The paper also mentions the systematic obstacles such as adversarial attacks, imbalance in data, lack of explain ability and operational factors which restrict the reliability of models in the real world.

Further studies are needed to make ML models more resilient and explainable to resist adversarial attacks, address the changing threats, and offer more transparency to the decision-makers. The future of automated risk labelling, self-learning systems, and federated learning would decrease data dependency and enhance model generalization in a wide range of IT environments. Also, more powerful human machine teamwork, better policy compliance strategies, and testing in large scale should be considered in future research to prove the ML-based risk classification systems in a realistic working environment.

REFERENCES

1. C. Hewage and A. Bajwa, "Security Policy: What It Is, Why And Challenges," vol. 1, 2018.
2. P. M. Goel, "A Literature Review of Cyber Security," IJRAR1CBP189 Int. J. Res. Anal. Rev., vol. 6, no. 2, pp. 136–140, 2019.
3. G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF," Int. J. Inf. Secur., vol. 17, no. 6, pp. 681–699, 2018, doi: 10.1007/s10207-017-0382-0.
4. P. Vähäkainu and M. Lehto, "Artificial intelligence in the cyber security environment Artificial intelligence in the cyber security environment," 14th Int. Conf. Cyber Warf. Secur. ICCWS2019At Stellenbosch, South Africa, 2019.
5. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in International Conference on Cyber Conflict, CYCON, 2018. doi: 10.23919/CYCON.2018.8405026.
6. K. Irfandhi, "Risk Management in Information Technology Project: An Empirical Study," ComTech J., vol. 7, pp. 191–199, 2016, doi: 10.21512/comtech.v7i3.2498.
7. H. I. Kure, S. Islam, and M. A. Razzaque, "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System," Appl. Sci., vol. 8, no. 6, p. 898, May 2018, doi: 10.3390/app8060898.
8. H. Rodage, H. Lei, and F. Ganjeizadeh, "Risk Management for Research and Development Projects," Int. J. Eng. Res. \& Technol., vol. 3, no. 10, pp. 824–831, 2014.
9. D. Vogt, B. N. Smith, L. A. King, D. W. King, J. Knight, and J. J. Vasterling, "Deployment Risk and Resilience Inventory-2 (DRRI-2): An Updated Tool for Assessing Psychosocial Risk and Resilience Factors Among Service Members and Veterans," J. Trauma. Stress, vol. 26, no. 6, pp. 710–717, 2013, doi: 10.1002/jts.21868.
10. C. Colwill, "Human factors in information security: The insider threat – Who can you trust these days?," Inf. Secur. Tech. Rep., vol. 14, no. 4, pp. 186–196, Nov. 2009, doi: 10.1016/j.istr.2010.04.004.
11. Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.
12. P. Pathak, A. Shrivastava, and S. Gupta, "A survey on various security issues in delay tolerant networks," J Adv Shell Progr., vol. 2, no. 2, pp. 12–18, 2015.
13. H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," Appl. Sci., vol. 9, no. 20, p. 4396, Oct. 2019, doi: 10.3390/app9204396.
14. R. Sathya and A. Abraham, "Comparison of Supervised

and Unsupervised Learning Algorithms for Pattern Classification," Int. J. Adv. Res. Artif. Intell., vol. 2, no. 2, pp. 34–38, 2013, doi: 10.14569/ijarai.2013.020206.

15. M. Usama et al., "Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges," IEEE Access, vol. 7, pp. 65579–65615, 2019, doi: 10.1109/ACCESS.2019.2916648.

16. M. Rege and R. B. K. Mbah, "Machine Learning for Cyber Defense and Attack," DATA Anal. 2018 Seventh Int. Conf. Data Anal. Mach., vol. 22, no. 1, pp. 7–14, 2018.

17. S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 7, no. 2, 2019, doi: 10.5281/zenodo.15362327.

18. R. Das and T. Morris, "Machine Learning and Cyber Security," in 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), IEEE, Dec. 2017, pp. 1–7. doi: 10.1109/ICCECE.2017.8526232.

19. I. H. Sarker, A. S. M. Kayes, and P. Watters, "Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage," J. Big Data, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0219-y.

20. K.-K. R. Choo, "The cyber threat landscape: Challenges and future research directions," Comput. Secur., vol. 30, no. 8, pp. 719–731, Nov. 2011, doi: 10.1016/j.cose.2011.08.004.

21. V. M. L. G. Nerella, "Observability-Driven SRE Practices for Proactive Database Reliability and Rapid Incident Response," Int. J. Recent Innov. Trends Comput. Commun., vol. 7, no. 8, pp. 32–38, Aug. 2019, doi: 10.17762/ijritcc.v7i8.11710.

22. M. Alotaibi, S. Furnell, and N. Clarke, "Information security policies: A review of challenges and influencing factors," in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, pp. 352–358. doi: 10.1109/ICITST.2016.7856729.

23. X. Lyu, Y. Ding, and S. H. Yang, "Safety and security risk assessment in cyberphysical systems," IET Cyber-Physical Syst. Theory Appl., vol. 4, no. 3, pp. 221–232, 2019, doi: 10.1049/iet-cps.2018.5068.

24. A. Le and C. Maple, "A simplified approach for dynamic security risk management in connected and autonomous vehicles," in Living in the Internet of Things (IoT 2019), 2019, pp. 1–8. doi: 10.1049/cp.2019.0140.

25. A. Rahmati, E. Fernandes, K. Eykholt, and A. Prakash, "Tyche: A Risk-Based Permission Model for Smart Homes," in 2018 IEEE Cybersecurity Development (SecDev), 2018, pp. 29–36. doi: 10.1109/SecDev.2018.00012.

26. Q. Hong et al., "An information security risk assessment algorithm based on risk propagation in energy internet," in 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 2017, pp. 1–6. doi: 10.1109/EI2.2017.8245703.

27. D. Henshel et al., "Modeling cybersecurity risks: Proof of concept of a holistic approach for integrated risk quantification," in 2016 IEEE Symposium on Technologies for Homeland Security (HST), 2016, pp. 1–5. doi: 10.1109/THS.2016.7568937.

28. K. Gai, M. Qiu, and S. A. Elnagdy, "Security-Aware Information Classifications Using Supervised Learning for Cloud-Based Cyber Risk Management in Financial Big Data," in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), IEEE, Apr. 2016, pp. 197–202. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.66.

29. V. Dorca, R. Munteanu, S. Popescu, A. Chioreanu, and C. Peleskei, "Agile approach with Kanban in information security risk management," in 2016 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 2016, pp. 1–6. doi: 10.1109/AQTR.2016.7501278.

30. Routhu, K. K. (2022). From Case Management to Conversational HR: Redefining Help Desks with Oracle's AI and NLP Framework. *International Journal of Science, Engineering and Technology*, *10*(6).

31. Vattikonda, N., Gupta, A. K., Polu, A. R., Narra, B., Buddula, D. V. K. R., & Patchipulusu, H. H. S. (2022). Blockchain Technology in Supply Chain and Logistics: A Comprehensive Review of Applications, Challenges, and Innovations. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(3), 72-80.

32. Attipalli, A., BITKURI, V., Mamidala, J. V., Kendyala, R., & KURMA, J. (2022). Empowering Cloud Security with Artificial Intelligence: Detecting Threats Using Advanced Machine learning Technologies. *Available at SSRN 5741263*.

33. Padur, S. K. R. (2022). Intelligent resource management: AI methods for predictive workload forecasting in cloud data centers. *J. Artif. Intell. Mach. Learn. & Data Sci*, *1*(1), 2936-2941.

34. Routhu, K. K. (2022). From RFID to Geofencing: IoT-Enabled Smart Time Tracking in Oracle HCM Cloud. *International Journal of Science, Engineering and Technology*, *10*(4).

35. Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju,

S. K. K., Chundru, S. K., & Vangala, S. R. (2022). Data Security in Cloud Computing: Encryption, Zero Trust, and Homomorphic Encryption. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 31-41.

36. Padur, S. K. R. (2022). AI augmented platform engineering, transforming developer experience through intelligent automation and self optimizing internal platforms. *International Journal of Science, Engineering and Technology*, *10*(5), 10-5281.

37. Polu, A. R., Buddula, D. V. K. R., Narra, B., Gupta, A., Vattikonda, N., & Patchipulusu, H. (2021). Evolution of AI in Software Development and Cybersecurity: Unifying Automation, Innovation, and Protection in the Digital Age. *Available at SSRN 5266517*.

38. Padur, S. K. R. (2020). From centralized control to democratized insights: Migrating enterprise reporting from IBM Cognos to Microsoft Power BI. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol*, *6*(1), 218-225.

39. Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, V., Enokkaren, S. J., & Attipalli, A. (2021). Systematic Review of Artificial Intelligence Techniques for Enhancing Financial Reporting and Regulatory Compliance. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(4), 73-80.

40. Padur, S. K. R. (2019). Machine learning for predictive capacity planning: Evolution from analytical modeling to autonomous infrastructure. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *5*(5), 285-293.

41. Attipalli, A., Enokkaren, S., BITKURI, V., Kendyala, R., KURMA, J., & Mamidala, J. V. (2021). Enhancing Cloud Infrastructure Security Through AI-Powered Big Data Anomaly Detection. *Available at SSRN 5741305*.

42. Singh, A. A. S., Tamilmani, V., Maniar, V., Kothamaram, R. R., Rajendran, D., & Namburi, V. D. (2021). Predictive Modeling for Classification of SMS Spam Using NLP and ML Techniques. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(4), 60-69.

43. Padur, S. K. R. (2020). AI augmented disaster recovery simulations: From chaos engineering to autonomous resilience orchestration. *International Journal of Scientific Research in Science, Engineering and Technology*, *7*(6), 367-378.

44. Reddy Padur, S. K. (2021). From Scripts to Platforms-as-Code: The Role of Terraform and Ansible in Declarative Infrastructure Rollouts. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 621-628.

45. Kothamaram, R. R., Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., & Maniar, V. (2021). A Survey of Adoption Challenges and Barriers in Implementing Digital Payroll Management Systems in Across Organizations. *International Journal of Emerging Research in Engineering and Technology*, *2*(2), 64-72.

46. Padur, S. K. R. (2018). Autonomous cloud economics: AI driven right sizing and cost optimization in hybrid infrastructures. *International Journal of Scientific Research in Science and Technology*, *4*(5), 2090-2097.

47. Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., Maniar, V., & Kothamaram, R. R. (2021). Anomaly Identification in IoT-Networks Using Artificial Intelligence-Based Data-Driven Techniques in Cloud Environmen. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(2), 83-91.

48. Padur, S. K. R. (2021). Bridging Human, System, and Cloud Integration through RESTful Automation and Governance. *the International Journal of Science, Engineering and Technology*, *9*(6).

49. Attipalli, A., BITKURI, V., KURMA, J., Enokkaren, S., Kendyala, R., & Mamidala, J. V. (2021). A Survey of Artificial Intelligence Methods in Liquidity Risk Management: Challenges and Future Directions. *Available at SSRN 5741342*.

50. Padur, S. K. R. (2021). From Control to Code: Governance Models for Multi-Cloud ERP Modernization. *International Journal of Scientific Research & Engineering Trends*, *7*(3).

51. Routhu, K. K. (2021). Harnessing AI Dashboards in Oracle Cloud HCM: Advancing Predictive Workforce Intelligence and Managerial Agility. *International Journal of Scientific Research & Engineering Trends*, *7*(6).

52. Padur, S. K. R. (2021). Deep learning and process mining for ERP anomaly detection: Toward predictive and self-monitoring enterprise platforms. *Available at SSRN 5605531*.

Citation: Prasanth Varma Addepalli, Sridhar Reddy Bandaru, et al., “Performance Analysis of Machine Learning Models for Cybersecurity Risk Classification in IT Projects”, Universal Library of Engineering Technology, 2023; 33-41. DOI: https://doi.org/10.70315/uloap.ulete.2023.006.