Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Risk Assessment Models for Protecting Automated Accounting Systems from Cyber Threats

Md Rakibuzzaman[1]✉, Sanjida Akter Sarna[2] and Abdul Azeem Mohammed[3]
[1]*Officer, Department of Banking Inspection, Bangladesh Bank, Dhaka, Bangladesh*
[2]*Master of science in Business Analytics, Trine University, Arizona, USA*
[3]*Master of science in Business Analytics, Trine University, Arizona, USA*
Corresponding Author: Md Rakibuzzaman, **E-mail**: rakibuzzaman32665@gmail.com

| ABSTRACT
With rising financial processes that are digitized and robotized, the accounting systems are operating in a constantly changing landscape of cyber threats that threaten data integrity, financial validity, and organizational reputation. This study focuses on the elaboration of risk assessment models that use artificial intelligence to guard the automated accounting systems against cyber vulnerability and safeguard them against fraud, data theft, unauthorized accessibility, and misstatement of financial statements. This study investigates how to detect and predict risk behaviors in accounting in record-keeping processes using the Financial Transaction and Risk Management Dataset, a fully labelled multilingual risk incident Dataset that contains detailed transactional data and system metadata so far. The steps of data preprocessing and feature engineering take place in Python and Excel, thus facilitating the conversion of raw data into analyzable predictors, such as abnormal patterns within transactions, login peculiarities, and risk scores in particular categories. Unsupervised anomaly search with the help of Isolation Forest is also carried out to improve the detection of new threats. Furthermore, Tableau dashboard is also used to show vital trends in charts, such as risk heat map, trend lines, and category-wise distribution of the frauds. The findings show that ensemble models can be better than baseline classifiers and have a high accuracy rate in high-risk transaction detection, which could yield fruitful results and enlighten the real-time financial security monitoring. Visual analytics also help in decision-making since complex outputs on models are readable and understandable by finance people and those verifying the accounts. This study advances the accounting cyber security field of study by providing a flexible and understandable model of cyber risk to be addressed in the automated financial systems. The study also emphasizes the need to integrate machine learning, data visualization, and domain knowledge as a combined effort to protect computerized accounting infrastructure against relatively advanced cyber hacking.

| KEYWORDS
Cyber security, Automatic Accounting Systems, Risk Assessment, Machine Learning. Fraud Detection and Data Visualization

| ARTICLE INFORMATION
ACCEPTED: 12 June 2025 **PUBLISHED:** 20 July 2025 **DOI:** 10.32996/jcsts.2025.7.7.78

1: Introduction

1.1 Background

Digitalization of the economy has basically altered the nature of accounting by changing the manual way of keeping records to the advanced automated accounting systems. Cloud computing, artificial intelligence (AI), robotic process automation (RPA), and enterprise resource planning (ERP) solutions have taken the form of the backbone of corporate financial infrastructure through these platforms. As more organizations depend on automation, the accounting systems are now more efficient and scalable, providing faster processing of data, real-time reports and better compliance abilities. But automation and connectivity makes them more susceptible to cyber-attacks at the same time. With the advance in the complexity and volume of financial

operations, the risk of data breach, cyber-fraud and statement of disoperation also increases. There is an increase in cyber-attacks to the financial information, including manipulation, theft, or destroying important information exploiting the vulnerabilities in automated systems [1]. Accounting systems are frequently attacked by threat actors such as hackers, insiders, and nation-state actors because of their sensitivity when it comes to the data they house on financial matters. Instances of cyber breaches, fake purchases, system misrepresentations, ransom ware penetrations, and privilege elevations have revealed the incompetence of the rule-based detectors. Such fixed techniques do not help detect emerging or new sets of attack mechanisms, which makes financial systems vulnerable to serious performance and reputational losses. Organizations must, therefore, be equipped with strong and smart risk assessment models which are able to proactively identify the anomalies, evaluate risks and make real time responses to guard financial information and safeguard business. This has opened doors to an integration of AI-powered and machine learning to augment the risk prediction, cyber resilience, and operational transparency of accounting systems. In the era of automation of financial departments across the globe, ensuring security of these smart systems against pernicious and evolving cyber security threats has been one strategic priority by financial institutions aiming for long term sustainability.

1.2 AI Risk Management emerges

Development of artificial intelligence and machine learning technologies has brought forth a powerful mechanism of detection and prognosis of relational security threats in real time. Conventional cyber security platforms are usually based on hard-coded frameworks and fixed limits and are insufficient to cover the constantly transforming world of online financial attacks. Nowadays, due to the increasing complexity of cyber-attacks (application of advanced persistent threats, phishing attacks, and insider manipulations), the necessity of the adjustable and smart risk detection procedures becomes even more pressing [2]. The effective machine learning models can be trained based on substantial amounts of transactional and behavioral data to discover minor events that can signal a fraud incident or an intrusion into the system. Such models do not only enhance the detection accuracy but also continuous change with the availability of new data. In the scenario of automated accounting systems, AI can be used to process monetary transactions and system access activity logs, user activity, and metadata in real time and evaluate it to attribute risk with a dynamic risk score to every event. This enables organizations to prioritize the response actions and even set alarms in high-risk situations. Aligning the functionality of AI with data visualization tools like Tableau can provide an increase in interpretability and allows the finance professionals to perceive complex risk profiles through more user-friendly dashboards and visual analysis [3]. As the regulatory requirements also place more emphasis on proactive risk management, AI-driven systems are also compliant in that they enforce elaborate logs and audit trails. It follows that the introduction of AI to cyber security in the accounting field cannot be considered supplemental; it can be considered disruptive, providing scalable, smart, and context-sensitive solutions to prevent new forms of cyber threats. Such transition is a game changer as far as attitude towards cyber security in organizations is concerned as the approach is now changing towards a proactive and predictive approach of cyber security being built into the very fabric of financial systems.

1.3 Rationale of the study

This study is motivated by the awareness that more and more automated accounting systems are in danger of being undermined by the development of cyber threats to them. With financial transactions being managed through digital transformation and automation in organizations in different industries, the complexity and the volume of data being generated by these systems are becoming exponentially large. Although such transformation provides plenty of advantages with respect to operations, it increases the attack surface that malicious actors can use. Financial systems in many organizations are not properly holed up against cyber security threats mainly because of advancements in technology which has made the critical infrastructure vulnerable. In the past years, publicity of prominent data breaches and incidents of frauds highlighted the insufficiency of conventional mechanisms when it comes to preventing vulnerable automation exploits. The use of the existing static and rule-driven fraud detection systems causes a delay in action as attackers violate the detection systems and perpetrate fraudulent actions without being caught. It is in this motivation that this study aims at understanding that proactive, intelligent, and adaptive models of risks are necessary to protect automated accounting systems [4]. The research will help to narrow the gap between accounting and cyber security theory and practice by using machine learning skills and actual financial information. This study is also meant to fill a research gap at the cross-section of the automation of accounting tasks through AI and in cyber risk evaluation, which is still developing as an academic topic. The use of the next level data visualization tools is aimed to promote transparency and usability among financial decision-makers [5]. The motivation of this research lies in the intention to contribute to the establishment of robust, scalable and explainable cyber security solutions that will not only identify threats but will also help organizations to control cyber risk intelligently within the context of automated financial ecosystems.

1.4 Problem Statement

Advanced cyber threats are more focused on exploiting automated accounting systems, when the majority of the organizations use outdated and static monitoring systems based on rules which are not enough to detect the evolving risks. Failure to have dynamic risk assessment mechanisms the business risks itself to, the variables of financial frauds, data

manipulation and unauthorized access that cause the business huge financial losses, regulatory sanctions and supreme reputation losses. The demand for AI-based risk models capable of smart analysis and forecasting on cyber threats on the accounting systems based on studying the transactional and behavioral data about the real world is extremely high.

1.5 Research Objectives

This study seeks to design, propose, and test machine learning-based risk assessment models that can identify and forestall cyber threats in automated accounting systems. As specific objectives, the following can be mentioned:

- To establish main transaction and behavioral characteristics which are imperative to security risk in accounting systems.
- To construct and compare predictive models to classify the risk.
- To use anomaly detection methods in detecting rare or novel patterns of threats.
- To create pictures of patterns and model outputs in Tableau, Python and Excel to make better decisions.
- To suggest a scaled risk assessment model of real-time monitoring of threats to finance.

1.6 Research Questions

This study following these questions:

1. Which trends in the traffic data of financial transactions are a signal of such cyber threats as fraud or intrusion?
2. Which are the most effective machine learning models that can predict risk incidents of automated accounting systems?
3. What is the way to leverage anomaly detection techniques to complement supervised learning in terms of zero-day attacks ID?
4. How can data visualization tools help increase the interpretability and the operational application of the AI-based risk models?

1.7 Scope of the Study

This research paper is based on securing automated accounting systems with artificial intelligence and machine learning. It uses publicly available data that emulates accounting transactions seen in the real world and their related signs of cyber risk. The data contains the metadata of the financial transactions given in terms of amounts, types and type of payment, time stack, and user events in addition to labels of whether a transaction is fraudulent, erroneous or a miss statement. The study is limited to online accounting systems and does not apply to human book-keeping and paper-based data protection [6]. Neither does it involve legal nor compliance auditing techniques that are not part of the automation work process. The research technique is of quantitative nature, which includes statistical and formulaic anomaly detection and classification. It is technically focused on model training using Python and visualization using Tableau to show and describe the findings. The findings of this research will assist the professionals of cyber security, data analysts, auditors, and financial managers to design or incorporate AI-based risk monitoring systems into their systems. Although the work is inclined towards the practical side, it can also add some academic knowledge about the role of AI in the field of finance-specific cyber security [7]. Its findings can be used in organizations of all sizes: corporate, governmental or nonprofit, as long as they use automated systems to manage financial data. The next steps that can be taken in future research can be to extend the model to multi-source data or real-time financial network behavior.

8 Significance of the Study

This study explores both in the academic and professional field because it refers to the essential subject of accounting automation and evaluation of its compatibility with the threats of cyber security [8]. The study is the first of its kind in literature and hence occupies a gap in existing literature in academia by addressing how artificial intelligence can be used to secure concrete financial settings concerning the issue of cyber threats on automated systems. The majority of the existing research separates cyber security and accounting fields; the proposed study connects them using a multidisciplinary approach that incorporates machine learning and data science, financial, and risk management areas. It is knowledge developing as it uses empirical techniques on an open dataset and tests theoretical models using them in practice. Industry-wise, the research has a scalable and interpretable framework that can easily be implemented within the current systems of organizations [9]. The results are significant in expounding how to identify cyber risks in digital accounting processes and their workflows to develop real-time motion detection systems and forensic instruments. The Tableau visualization brings another element of usability where the results of the analyses can be viewed and understood by non-technical stakeholders to make sound decisions regarding the complex risk dynamics. In addition, at a time when there is increasing regulation in issues related to data security integrity of the financial reporting and fraud prevention, this research study has a proactive answer to those expectations. It also enables the decision-makers to switch reactive compliance to proactive risk governance. Consequently, the relevance of the research is in the fact that it may affect strategic planning and operational resilience of financial ecosystems of the modern world.

2 Literature Review

2.1 Automation and Cyber security Convergence in Finance

Automation and cyber security in the financial sphere has resolved in a dualistic atmosphere, which necessitates that efficiencies and risk-mitigation must coexist. Since more organizations are turning to automated accounting systems to simplify financial goals, the risk posed by cyber threats has not only become more complex and far-reaching, but also has become more refined. The use of automation technologies, such as cloud-based platforms, robotic process automation (RPA), and machine intelligence-based accounting software, makes it possible to process data in real time, reduce the occurrence of errors, and enhance regulatory compliance [10]. The widening of the attack surface is also the goal of malicious actors. By their definition, automated systems rely more on interconnected data streams, third-party APIs, and cloud-based environments, and all these are the possible vectors of cyber-attacks. Financial information is especially profitable, and therefore accounting systems are Canada gifted targets of cybercriminals interested in fraudulent and theft activities or manipulation of data. Literature shows that there is a developing agreement that normal protective techniques against security such as firewalls and stationary access have been insufficient measures to defend such systems. What is necessary instead is dynamic and smart risk assessment models to identify anomalies, predict threats and initiate measures to control with immediacy. The importance of cyber security as a set of measures to deal with intruders in the world of IT has become a strategic planning issue in the financial sector because the costs of a system intrusion in terms of finances and a negative image may be enormous [11]. Financial professionals and the IT security department need to collaborate to ensure that they create resilient infrastructures, capable of resisting the threats despite the advances in automation. This intersection of automation and cyber security is not only a technical issue but an organizational and strategic problem, and it requires constant learning, cross-functional cooperation, and the investment in adaptive technology. Thus, protective models require extensive knowledge of the potential of automation and the scenery of cyber risks.

2.2 Evolution and Capability of Automated Accounting Systems

The development of computerized accounting sums up the general digitization of organizational finance [12]. Automation has transformed business management of money transactions, reporting, compliance and internal controls since its creation in early spreadsheet applications to the present day enterprise resource planning (ERP) systems. Artificial intelligence (AI), machine learning, cloud computing, and robotic process automation (RPA) are technologies used in modern automated accounting to ensure real-time data processing, enhanced accuracy and data integration. The systems have become the hub of payrolls, invoices, assets tracking, taxation, and financial auditing. Automated reconciliations, intelligent categorizations of data and predictive analytics minimize human error and efficiency in operations. They help make better, quicker decisions as they offer accurate information about the finances in time. There are new vulnerabilities, which are registered in the literature due to automation notwithstanding the above benefits [3]. The use of centralized cloud servers and API poses a risk requiring unauthorized access, system misconfiguration, and data leakage. A mistake in an automatic process can be replicated on hundreds and thousands of transactions in a few seconds, spreading discrepancy everywhere. Besides, some systems are often open to blaming third-party integrations, which, when not secured, result in third-party attacks [14]. Automation is growing up, which means that accounting professionals have to deal not only with the management of financial data but also the preservation of underlying systems. Increased demand is being raised to accommodate cyber defense not only as integrated components of accounting systems but as well to invoke secure authentication systems, encryption, and real-time analysis options. These systems have become more complex than before, thus requiring multidisciplinary solutions that include finance, IT, cyber security, and compliance professionals. The literature, therefore, justifies the implementation of smart, safe approaches to automation, which boost the performance of operations the resilience of the system.

2.3 Financial System Threats to Cyber

The threats in cyber of the financial systems are getting more difficult, thus attacking the core of the automated accounting structure. Financial data is always sensitive and confidential, thus a great asset to the attacker who may identify vulnerabilities in order to steal, engage in fraud, or destroy the system. Cyber threats are more prone to automated accounting systems, whose nature of interconnectivity and data-heaviness makes them especially vulnerable. These common attack vectors are phishing, malware injection, ransom ware, social engineering, privilege escalation, and API exploitation [15]. With regards to insiders, their access to sensitive information is also quite a threat, either out of carelessness or malice. These attacks are becoming more prominent as financial activities turn into digital because fraudsters use advanced instruments and mechanisms to acquire unauthorized access, make corrections, or interfere with transactions. One prominent issue is the rising popularity of the advanced persistent threats (APTs) that enabled attackers to have unnoticed access within an extended timeframe. Those threats are based on technological weaknesses and human weak points including inadequate password control or poorly set access control. Threat detection mechanisms may not be proactive or adaptive, and thus the automated systems may become compromised. Rule-based systems (static) are usually not capable of detecting emerging and changing patterns of attacks especially those that are patterned to appear legitimate [16]. The literature focuses on the need of changing the base of reactive cyber security solutions to proactive, intelligence-based approaches. These include the incorporation of anomaly detection

solutions, behavior analytics, and in-time monitoring to be able to detect and contain threats before their damage is done. The increased use of cloud infrastructure, mobile access and remote operations of the financial industry has extended the sphere of threats. The problem is how to build security strategies which will be able to work in these changing digital environments and especially the high regulatory environment of the accounting world.

2.4 Frameworks and Models of Risk Assessment

Risk assessment models and structures are essential products in recognition and curbing threats in automated accounting systems. Conventionally, firms have used the static models, checklists and periodical audits to assess financial and cyber security risks. Although these solutions provide systematic monitoring, they are weak in tracing the real-time and rapidly changeable threats [17]. Current financial conditions require dynamic risk evaluation solutions that have the capacity to evolve according to the changing trends and integrate predictive abilities. There are frameworks that provide a detailed guide on how to assess the risk exposure, how to prioritize the controls, and how to be compliant, including Risk Management Framework (RMF) and COSO Enterprise Risk Management, the FAIR frameworks. They are however limited in most occasions by their inability to be part of the digital world and the fact that they are more manual in nature [18]. It demands real-time, round-the-clock tracking of automated accounting systems, which cannot be done with the traditional audits. More interest is being raised in the possibility of integrating machine learning and analytics in risk assessment practices. By examining the history of transactions and user behaviors and system logs, such models are used to alert suspicious activities and predict future threats. They also give assessment of risks in terms of behavior patterns and contextual factors such that risk interventions are made more accurately and in a timely manner. Further, such systems are capable of reporting and visualization in real-time, which is valuable to decision-makers. However, issues regarding the clarity and comprehension of AI based models have made their adoption wary particularly in the regulated sectors. The issue lies in making hybrid risk assessment frameworks, which merge formative organization of past techniques with the versatility of smart automation. Such frameworks have to match organizational goals, regulatory needs, and changing threat environments to guarantee safety and integrity of financial systems.

2.5 Cyber security and fraud detection using Machine Learning

Modern-day cyber security and fraud-detecting in automated accounting systems involve the use of machine learning (ML) as an essential part of it. These smart models are developed to process large amounts of data concerning transactions and behavioral patterns to detect patterns possibly pointing at risks of cyber-attacks or financial fraud. Supervised learning algorithms, including decision trees, random forests, and gradient boosting, are trained by datasets that are labeled as historic cases of transactions labeled as fraudulent or not fraudulent [19]. These patterns educate them and once applied to new and never before seen data they can predict risks in real time. Unsupervised, such as clustering and anomaly detection models, are used when there is a need to detect anomalies in data without this prerequisite labeling. They can be handy in cases of zero-day attacks or fraud methods that have not been known before. Semi-supervised models allow taking advantage of labeled and unlabeled data to improve the ability to detect in moving situations. ML models can detect the threat of payment frauds, identity theft, insider threats, and account takeovers [20]. making results interpretable is one of the most important issues related to the use of ML. Professionals involved in the financial arena and auditors find it wise to seek clear clarifications on how a specific risk score, or flag was obtained. SHAPE or LIME techniques are explainable AI (XAI) algorithms that are commonly used to be more transparent. In addition, ML systems should be fed into an appropriate pre-processing and should keep on training and validating to prevent biases or overtraining. It should also be integrated with the current IT infrastructure, compliance systems and visualization platforms. All in all, machine learning can provide easily scalable, agile and high-accuracy solutions to cyber security and fraud detection in the current accounting context.

2.6 Risk monitoring visualization

Visualization is also very important in cyber security and financial risks monitoring because it helps make more complex data more intuitive in terms of actions. Applied in the setting of automated accounts systems, visualization tools help discover anomalies, track live activity and enable decisions, with transaction flows, risk measures and alerts being presented in the interactivity form. Tableau, Power BI, and the visualization libraries of Python to create dynamic dashboards showing important performance indicators (KPIs), trends associated with behavior, and threats. Such dashboards are necessary to track the high volume transaction environment that cannot be possible to review manually [21]. They aid in funding teams, auditors and cyber security experts identify suspicious events quickly, e.g. exceptions or outliers in login behavior, high and low spikes in volume of transactions, etc. Besides, a visualization may be adjusted according to the positions, enhancing relevancy and response time. Heat maps, real-time graphs, anomaly indicators, and other items facilitate the communication of risk and encourage the involvement of stakeholders. Visualization has an additional value in risk assessment models by explaining the machine learning prediction (itself), improving the transparency of models, and providing a record of security trends in the form of an audit or regulatory compliance [22]. Although they are useful, most visual systems are not domain specific financially and can miss important transaction-level knowledge. In addition, dashboards can be compromised by the lack of congruity or poor integration of the data as well. As such, it is necessary to establish customized visual analytics of cyber security in the accounting

setting. The presence of effective visual monitoring increases the accuracy of established detection but also contributes to the responsiveness of the organization, thus making it essential when dealing with the problem of cyber risk in automated accounting systems.

2.7 Literature Gaps

In spite of the increasing number of studies dedicated to the application of AI-based risk assessment to automated accounting systems, there is a substantial lack of study in the existing literature. The majority of current research dwells on individual parts of financial cyber security, including fraud detection, anomaly monitoring, or risk modeling, but does not present the frameworks that can integrate these elements. End-to-end systems which incorporate data ingestion, machine learning processing, visualization and real time response are poorly explored. Then, the majority of the research bases upon proprietary datasets or simulations themselves, which cannot be transferred to real-life financial settings due to insufficient complexity, providing limited generalizability [23]. This gap is illustrated by the other major gap of non-interpretability of AI models. Several algorithms that perform well in machine learning, e.g. deep neural networks and ensemble models, can be termed as black box and they fail to satisfy the transparency expectations of the financial auditors and regulators. What is more, the possibility to combine several data analytics platforms has not been properly investigated in literature, including the combination of the tools like programming Python to perform the models with Excel, which is used to validate the models, and Tableau to visualize the models. Such a combination of multi-tools can make models explainable and operationally usable even by non-technical financial stakeholders. It is also significant that the studies on design of user-centered risk interfaces and supportive of various organizational roles are poorly represented. The literature on accounting systems as far as cyber security is concerned seldom speaks about custom dashboards and interactive reporting. Filling these gaps is one of the important key points of further development of academic understanding and practical uses.

2.8 Empirical Study

In the article by Phillips, Taylor, Boniface, Modafferi, and Surridge titled, Automated Knowledge-Based Cyber security Risk Assessment of Cyber-Physical Systems (2024), the authors provide an informative empirical base to develop cyber security in automated accounting systems. The paper discusses an organizational framework of risk management, simulation-based on ISO 27005, which is conducted through the platform of the open-source Spyderisk. Though cyber-physical systems are the domain highlighted by the authors, the approach will be highly applicable in the field of automated accounting systems where the interconnectedness of components, data flow, and digital interaction points are equally susceptible to the chain of cyber threat attacks. The model automates threat finding attack paths that does not require direct analysis of the assets, threats and threat causes and effects as their definitions are carried out by a core ontology [1]. The attack paths are determined by transparent and repeatable simulations. Such an empirically established methodology, which has been illustrated by the concrete case of a cyber-attack on a steel mill, emphasizes the efficiency of automated risk identification in highly complicated digital environments. Such a framework can be used to detect weak spots of an exchange data points, processing modules, and access controls when applied to automated accounting systems. The effects of the study are placed on transparency, reproducibility, and adaptability to changes in real time in analyzing risk, which are essential when it comes to one of a sensitive nature to financial data. By incorporating this model into accounting systems, resilience regarding cyber threats may be greatly improved as the efforts to secure this part of the company would be ensured in areas where it is the most effective. Accordingly, the present empirical study is presented to the audience as a strong methodological reference in the development of the next-generation, automated models of risk assessment in financial cyber security applications.

Chinta et al., in their 2024 in-depth analysis article Entitled Harnessing Big Data and AI-Driven ERP Systems to Enhance Cyber security Resilience in Real-Time Threat Environments study how artificial intelligence and big data in ERP systems can be used to introduce tremendous improvements in cyber security resilience in real-time threat settings. Their study demonstrates how the business environment globally has become complex and a secure real-time accounting information system is very imperative. This is especially close to the topic of the present research, namely Risk Assessment Models of Protecting Automated Accounting Systems against Cyber Threats, since the ERP systems form the basis of the automated accounting systems [2]. This paper explains the major threats in cyber security and how the AI-powered ERP frameworks have the potential to address proactive risk assessment and monitoring. The solutions to real-time vulnerabilities presented by the internal and external agents by the authors give a sound model that strengthens the internal systems of control of the accounting infrastructures to enable the adoption of improved audit readiness and data protection in the automated environment.

The article Enhancing Financial Integrity through an Advanced Internal Audit Risk Assessment and Governance Model by Ogunsola, Balogun, and Ogunmokun (2021) offers important insights into the current risk assessment techniques that are important to support automated accounting systems against cyber risks. According to the paper, an improved internal audit model has been introduced that leverages predictive analytics, AI, and data-driven approach to enhance financial monitoring and risk management. The present study about the various models of risk assessment as a means of securing automation-based

accounting systems against cyber threats, happens to fall into this case especially since the study highlights the adoption of technologically advanced solutions to identify frauds, to track the observance of compliance, and the imposition of the ethical financial conduct [3]. By providing the key aspects, including automated compliance monitoring and internal controls, the authors outline what can be done to beef up the mechanisms of governance and audits to overcome the menace of cyber security. The provided industry case studies serve as additional proofs to the relevance of the model to the application in the automated financial experiences.

The article by Alanen et al. (2021) presents the empirical study of Hybrid ontology for safety, security, and dependability risk assessments and security threat analysis (STA) Method in industrial control systems, where the researchers presented a hybrid ontology-based framework capable of combining safety and security risk evaluations. Being used in critical infrastructures like nuclear fuel pool systems, the suggested Security Threat Analysis (STA) approach also applies to automated accounting systems. Such model-based approach fits industrial standards and facilitates the creation of traceable and structured repositories of risk assessment. It is crucial in the context of the present research study on the topic, namely, Risk assessment models to protect automated accounting systems against cyber threats, as accounting systems are exposed to more intricate threats to cyber security [4]. This study can, therefore, be used in the financial domains that require a high degree of integrity and system assurance because it makes use of ontology-driven assessment and tool-based traceability, a robust formula in finding and controlling cyber threats in mission-related environments.

An article by Kalinin, Krundyshev, and Zegzhda (2021) is an empirical research entitled Cyber security Risk Assessment in Smart City Infrastructures that introduces a new scheme of the cyber risk management in dynamic and device-to-device smart spaces using artificial neural networks (ANNs), object typing, and quantitative analysis. Despite being focused on infrastructures of smart cities, the research methodology can be greatly applied to security of automated accounting systems against cyber-attacks [5]. The research elicits the drawbacks of conventional, professional, and statistical models of risk in dynamically changing digital environments; which also holds to automated finance-based conditions. The proposed framework satisfies the requirements of scalable and flexible cyber security risk evaluation using automated real-time risk evaluation based on machine learning. Within the context of the proposed research on the topic of Risk Assessment Models to Protect Automatic Accounting Systems against Cyber Threats, the paper provides a practical and scalable model that makes cyber security in complex accounting platforms more accurate, automated, and responsive.

3. Methodology

This study uses a data-driven approach to work on the research in designing and testing AI-based risk assessment models to determine potential cyber-threats in automated accounting systems. It starts with the preprocessing of data and feature engineering with the Financial Transaction and Risk Management Dataset. A set of machine learning methods (supervised (Logistic Regression, Decision Tree, XGBoost) and unsupervised (Isolation Forest) classification offerings) are applied using Python. Cross-validation confirms the fitness of models and Grid Search is used to optimize parameters [124. The outputs of models are interpreted with visualization tools, such as Tableau and Excel. Such an approach allows making real-time, scalable, and understandable risk forecasts to protect financial information and guarantee system integrity in accounting.

3.1 Research Design

To consider the AI-based risk assessment models used in the automated accounting systems, the quantitatively-oriented data-driven research design is implemented in this study. The research study is exploratory and analytical which implies that machine learning methods will be used under supervision and supervision to identify the existing cyber threats and classify them based on the parameters of financial transactions [25]. The characteristics of data are analyzed using a descriptive approach, and correlational methods allow evaluating the intensity of connections between variables like the type of transaction, its frequency, or risk incidences. The approach facilitates both the real-time and retrospective detection of threats, offering an integrated concept of financial information security problems. The proposed research design focuses on empirical analysis with its objective simulated data based on real-world applications to test a variety of algorithms [26]. The results of models are compared to some predetermined performance measures such as precision, recall, and F1-score. Examples of visualization tools used to make visual interpretations of model predictions to facilitate decision making include Tableau and Excel. Its integrated design allows one to tune and refine its models in an iterative fashion, so that, among other things, model results are not only statistically sound, but operate as well. All research stages contain ethical principles including breathed-in nature, information confinement, and rectitude. Feedback loops to continuously improve occur within the design, as well, which allows it to be flexible to new cyber security threats.

3.2 Data source and collection

The proposed study will apply the freely accessible dataset called the "Financial Transaction and Risk Management Dataset" that will mimic actual accounting transactions cyber risk measures. Their data set consists of more than 10 000

transactions and have the following attributes: transaction-ID, amount, and date, and account number, type of the transactions, payment type, and a binary risk flag that indicates fraud, misstatement or error. It also involves system metadata, including processing times and log in locations which improve the user behavior and threat patterns analysis [27]. The collection of the data consisted in downloading the dataset presented on Kaggle with the CC0 Public Domain license, which gives an opportunity to distribute the information without any restrictions and use it in the research. The data was preprocessed by controlling missing values, cleaning, encoding the missing values, and categorical variables, such as payment method, category type. Further preprocessing entailed the detection of outliers and data normalization in a bid to achieve data quality consistency. To enable the development and the evaluation of the model, the dataset was split into training and test sets in the proportions of 80 and 20 percent. Excel and Python were used to conduct Exploratory Data Analysis (EDA) of risk distributions; establish trend lines and create initial graphs of risk frequencies by category and transaction amount. Such variables as frequency of products procured by a user, average amount of products per category, degree of risk of a payment method were derived using feature engineering methods [28]. These were extra things that were to be introduced to enhance model input and improve predictive accuracy. On the whole, the dataset constitutes the empirical basis of machine learning model building and validation in the research.

3.3 Tools and Techniques of Analysis

This paper will use a set of tools and methods of analysis to train test machine learning-based models of detecting cyber risks in accounting systems. Python is the most common programming framework in view of its key libraries, Scikit-learn, XGBoost, Pandas, NumPy and Matplotlib, that help in performing data pre-processing, model training, and visualization. The Logistic Regression, Random Forest and XGBoost are trained on labeled data that are currently classified as risky and not risky and used to classify new transactions as risky or non-risky. Stratified cross-validation and hyper parameter tuning are applied using a grid search to train and validate those models. In case of detecting anomalies unsupervised methods such as Isolation Forest and DBSCAN are applicable to point at a rare pattern/unusual behavior, which is not encountered in the labeled training set. Measurement evaluation metrics are accuracy, precision, recall, F1-score, and AUC-ROC, which give a different perspective on model performance [29]. The visualization of misclassification and the robustness of categorizing true positives and negatives is performed using confusion matrices. The visualization of the data is done with the help of Tableau and excel, and dashboards are created to visualize the critical parts in the transaction zones and how certain categories of transactions are risky and the output of the anomalies. The tools will allow the easy intuitive understanding of the findings of the models and will make risk-based decision making. Also, other statistical analysis, like the correlation coefficients and chi-square test are carried out to determine the relation between variables. This features multi-dimension that guarantees complete coverage of the cyber security risks in automated accounting settings.

3.4 Model Validation

Three steps, such as training, validation, and performance evaluation, are used in this study in line with model development. The labeled instances of the training subset of the dataset trains the supervised learning models, Logistic Regression, Random Forest and XGBoost. To achieve a higher training efficiency and accuracy, every model will be made to go through preprocessing procedures, namely normalization and feature selection. In the validation stage, there is the use of cross-validation tests to determine the validity of models on alternative division of data to make the models resistant to over fitting. The process of hyper parameter tuning, the task of determining the most appropriate configurations of each algorithm is achieved through the approach of grid search [30]. To give an example, Random Forest can be optimized with the number of estimators and maximum depth whereas XGBoost can be optimized with learning rate and tree depth. The performance of each model is then considered by the means of the following criteria: precision, recall, F1-score, and AUC-ROC, which will reflect their efficiency of detecting risky transactions. Anomaly detection is done with unsupervised models which include Isolation Forest and DBSCAN. Such models are not trained using tagged data, and are evaluated in the same dataset with the aim of detecting anomalous transaction patterns. The flagged anomalies are compared with actual risk indicators on consistency and relevance [31]. All model results are represented in Python and Tableau to deliver viable conclusions. This relative ease of interpretability, combined with rigorous training, makes the proposed models more than adequate in the real-time financial setting.

3.5 Tools and Strategy of Visualization

Visual analytics is crucial in comprehending machine learning outcomes and presenting cyber security dangers to any financial experts. The visualization approach used in this paper is the one that is aimed at providing the insights on the risks in the form that could be understood intuitively and in a role-specific way and employs tools like Tableau, Python, and Excel. At the first stage, the data distribution and transaction patterns are visualized due to the Python application at the Exploratory Data Analysis (EDA) stage. Histograms, scatter plots, boxplots are created to evaluate the frequency of transactions, the risk occurrence, and the correlation of features. Trained models post-model provide visual results in the forms of confusion matrix, ROC curves, and feature importance rankings with the capability to offer interpretability to model behavior and decision boundaries [32]. To build the interactive dashboards that enable the stakeholders to discover anomalies, track risk distributions according to transaction types gauge the risk scoring in real time, Tableau is employed. Dashboards include visualizations of

transaction clustering by means of heat maps, category-specific risks through bar charts, and line graphs to reflect temporal risk trends. Specifically, Tableau is complemented by Excel, which can create traditional reporting requirements i.e. pivot tables and static visual summaries. These visualization tools possess two essential uses, namely, quality of decision-making due to the presentation of complex model outputs in a human way of reading) and increased model credibility because of transparency. Visual insights help risk analysts, auditors and decision-makers to identify the vulnerabilities, investigate the flagged transactions and institute timely controls. On the whole, the visualization strategy interconnects the technical results and strategic financial control.

4. Design and Implementation of Risk Model

4.1 Design of the Proposed Risk Assessment Model

The construction of the proposed risk assessment model is designed in such a way that the ever-changing data of financial transactions and the currently developing reality of cyber threats to automated accounting systems is considered. The model has a modular pipeline designed that implements multiple stages: data preprocessing, feature engineering, training, testing, and deployment of the mode [33l. The application has each layer performing particular operations and is seamless hence it provides scalability, flexibility and real-time operability. The fundamental goal of the architecture is to identify and report unruly activities and possible cyber hazard via classification and eventual anomaly detection features. The data preprocessing layer is initiated with the cleaning of raw records of financial transactions, the empty cells filling, the encoding of the variable type, and the normalization of the numbers, and eloping timestamps into timely features like activity frequency and time of the day. During the feature engineering phase, domain specific variables will be designed that represent the user patterns in behavior, anomalies of transaction used and inconsistency across geographies and time. These characteristics are necessary to model the probability of incidences of risks [34]. The system is built to consider not only the past risk events but to learn the upcoming threats due to labeling data and use them to train models and detect any anomalies in real-time. Validation layer is used for cross-checking generalizability by applying k-fold cross-validation and the tuning layer is selected as GridSearchCV that optimizes hyper parameters. The outcomes are directed to a decision layer in which flagged transactions are depicted through Tableau dashboards. This architecture facilitates operational resilience, which helps the financial organizations to recognize the risks in advance and take timely action.

4.2 Target Variable Risk Incident

The binary outcome of this study whereby transactions will be classified as either risky or non-risky transactions is dependent on the target variable with the name risk incident. This random variable is a critical variable to any supervised learning project, which is a 0 or 1 bit that measures whether a given transaction was deemed a cyber-risk, fraud, misstatement or data anomaly [35]. The role of this variable cannot be overemphasized, and it will guide the model to differentiate legitimate financial actions and the ones that should be questioned. Being a true/false field, the files in which there is a risk of a transaction equals 1 and the other with no risk equal 0. The training set is divided into 80:20 training and testing split with the representative distribution of negative and positive samples. Data balancing techniques are employed because of the intrinsic issues on the class imbalance in such sets, i.e. there are more legitimate transactions than risky transactions. Synthetic Minority Oversampling Technique (SMOTE) artificial creation of minority class samples so that the models will not over fit to the majority class. The variable is also applied in measuring the model performance. Accuracy, recall, F1-score and area under the receiver operating characteristic curve (AUC-ROC) are measured on predictions based on this label. Risk Incident is utilized as the baseline metric in forming the train and as the basis of testing the accuracy of the classification [35]. It can also be used in comparing validating anomaly scores in unsupervised models, a way of cross-assessing suspect transaction flags. Essentially, the concept of Risk_Incident will be the pivot of the analytical framework of the performed research which will guide the design, tuning and validation of the machine learning models.

4.3 Classification Vs Anomaly Detection

The methodological approach used in this study combines two conceptually related methods of risk detection in automated accounting systems, classification and anomaly detection. Both approaches would help in ensuring that there is maximum robustness based on the proposed model since it can be used to identify known and unknown threat patterns in financial data. Supervised learning due to the usage of previously labeled historical data is classification based, and it is constructed on the data pertaining to the field of Risk_Incident. The technique makes the model learn patterns related to risky transactions, including: odd amounts of transactions, time variance, and repeated logging in, or user behavior abnormalities [36]. The predictive probabilities of the transaction being risky are generated using models such as the Logistic Regression, the Decision tree, and the XGBoost. The benefit of classification is that when a lot of labeled data exists, then it can be explicitly recognized to interpretable decisions. On the other hand, anomaly detection is unsupervised as it pays attention to the points that vary with the standard ones and intensively. This method (i.e. Isolation Forest) is applied to identify unseen cyber threats or zero-day attacks that cannot be detected using classification models and therefore is of especial value when used to identify

outliers in the feature space. Anomaly detection does not use labelled data and so this area of detection works reasonably where threats of a new and unprecedented type appear [36]. With these approaches combined, a hybrid detection system is formed. Detection of familiar threats is accurate through classification, and classification of the rare or changing threats is however increased through anomaly detection. This multilayered approach offers complete security to the automated accounting systems by ensuring that the wrong alarms go down along with false alarms creating a security that is both accurate and flexible.

4.4 Model Training Baseline Models

The creation of baseline models is a very important part of comparative analysis of the effectiveness of more advanced methods. In this study, to serve the purpose of illustrative models, Logistic Regression and Decision Tree methods are chosen as the initial algorithms because they are easy to implement, interpretable, and broadly applied in identifying fraudulent activities. An example is the Logistic Regression (LogReg). It works well when pairs of input features and the binary feature that is produced (Risk_Incident) are linear. The data is preprocessed by scaling the data and one-hot encoding because of the categorical variables before the actual training [37]. The model of logistics generates probabilities to conclude that a transaction is likely to be risky; this is afterwards turned into a binary forecast by a threshold. The performance is determined by evaluation metrics like recall, precision and AUC-ROC. The Decision Tree model on the other hand is rule based and hierarchical in nature. It recursively Divides dataset into partitions by features thresholds building a path of decisions in a tree-like manner. The decision Trees are non-linear and can handle intricate relationships among features. Scaling of features would not be necessary in this model and thus it is suitable in case of early exploratory modeling. The two models also employ 5-fold stratified cross-validation so that they are evenly evaluated. The results of these reference models are an indicator against which to contrast more advanced approaches such as XGBoost and Isolation Forest. Even though being simple, sometimes Logistic Regression and Decision Trees reveal valuable feature correlations and provide a solid analytical ground to get insights into how the underlying structure looks like with the dataset.

4.5 Advanced models training: Advanced models

To improve the predictive performance and increase the ability to detect unusual threat patterns, two high-performance models are made use of: XGBoost in supervised classification and Isolation Forest in unsupervised classification of anomalies. The reason to choose these models is because of their high accuracy, scalability and strength to be used with noisy and imbalanced data. XGBoost (Extreme Gradient Boosting) is a supercharge ensemble algorithm to sequentially construct trees and minimize misclassification errors on previous iterations. It includes regularization parameters and avoids over fitting, and it has parallel processing capabilities. XGBoost is in this research trained on basis preprocessed data which is the same as that on which the baseline models are trained [37]. There are major parameters to be fine-tuned by GridSearchCV i.e. learning rate, max depth, subsample ratio, number of estimators. In order to avoid over fitting, early stopping is utilized. The model creates rankings of the feature importance and will make it possible to gain knowledge about the most influential variables impacting risk classification. Isolation Forest identifies anomalies without the need of labeled data. It works through randomly choosing features and dividing the data into isolating outliers by having less splits. Each transaction is assigned an anomaly score and compared with that of a threshold to declare whether it can be described as a suspicious transaction. The Isolation Forest model may be applied in situations when rare events are not really bad (their historic label may be missing), but they are potentially dangerous [38]. The combination of the two algorithms widely used, XGBoost and the Isolation Forest, offers an all-rounded construct. XGBoost produces predictions with high rates of accuracy concerning known risks but Isolation forest makes the model more resistant to unpredictable threats and this makes it a comprehensive and versatile risk assessment strategy.

4.6 Cross-Validation and model Tuning

Effective validation and tuning strategies play a very important role in ensuring a robust performance of the model. Cross validation is used in an attempt to reduce the effect of over fitting and determining the models generalizability at unseen data. The study uses stratified 5-fold cross-validation in order not to lose class balance in training and testing folds. The data is divided into five equal populations and each of the former is utilized once as the test set and the other four used as the training set. To tune the hyper parameters the GridSearchCV is used to do an exhaustive search among the parameter settings. The tuning parameters are model specific. In the case of Logistic Regression, C and L1-L2 penalties are tested. Some of the parameters that Decision Trees are tuned on include maximum depth, minimum samples per split, and criterion (Gina or entropy). The aspects of XGBoost tuning concern learning rate, estimator count, max depth, gamma, and regularization terms. In the case with the Isolation Forest, the most important setting parameters are the number of trees and the level of contamination such as the proportion expected of outliers [39]. A combination of performance metrics is used to evaluate models: accuracy, precision, recall, F1-score and AUC-ROC (classification models); average path length, anomaly score distributions (Isolation Forest). The features are selected via recursive feature elimination (RFE) and the SHAPE values to interpret the features. This uniform process of model validation and tuning yields the best performance that the models can achieve, the models are not prone to over fitting, and the prediction of the models is accurate and explainable in various categories of financial cyber risks.

4.7 Overview of python implementation

The major programming language applied in constructing, training and testing the risk assessment models in this study is Python. It is especially convenient to work with it on the data preprocessing, machine learning, and visualization tasks due to the powerful ecosystem of libraries. The process of implementation starts with the loading and preprocessing of data with manipulation and mathematics performed with pandas and numpy. Numbers features will be scaled by StandardScaler, whereas categorical variables will be encoded by pd.get_dummies. SimpleImputer is used to fill in the missing. The cleaned data is then divided into train and testing divisions with train test split within sklearn.model. Model training consists of scikit-learn Train Logistic Regression and Train Decision Tree and xgboost Train XGBoostClassifier. According to anomaly detection, the Isolation Forest is applied, sklearn.ensemble. The hyper parameter tuning package is GridSearchCV, and cross-validation Stratified Fold is performed to ascertain balanced performance measures. Model performance is also displayed with matplotlib and seaborne tools which produce ROC plots, confusion matrices, precision-recall plots, and a feature importance plot. To generate interactive visualization, output data is sent to Tableau where dynamic dashboards are generated to reflect real-time risk scores, flagged transactions and trends analysis [40]. The whole process is designed in modularized formats in Python and Jupiter notebooks and each part of the pipeline has a specified function. Transparency, reproducibility, and scalability are provided with the help of Python. Any code is version-controlled by means of GitHub that allows collaborative development and tracking changes during the research lifecycle.

5. Results

The findings of this study give an elaborate report of the performance of machine learning models in identification and classification of cyber threats in the automated accounting systems. Models were trained, validated, and tested by using a curated fine grained financial transaction dataset in order to capture risk incidents [41]. To determine the main trends in the methods of payment, types of transactions, and user behaviors, it was the visualization tools that Tableau and Seaborn library in Python used to identify the significant trends in the methods of payment, types of transactions and behavior of the user. The accuracy, precision, recall, and AUC points, which are included in the evaluation metrics, underline the efficiency of classification and anomaly detection models in terms of real-time risk assessment.

5.1 Investigation of Risk Incidents on Accounting Categories

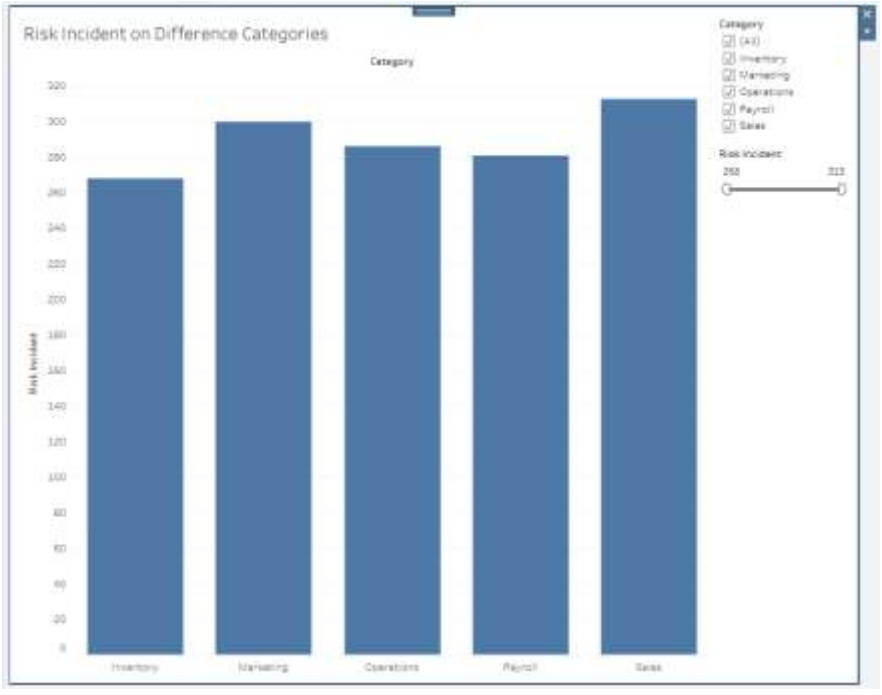

Figure 1: This figure signifies to the the risks incidence amongst various operation types within the automated accounting system

In figure 1, a bar graph has been used to demonstrate a comparison between the numbers of risk incidences experienced in each category of operation in the automatic accounting system. These are the categories of Inventory, Marketing, Operations, Payroll and Sales. As can be seen through the analysis, the recorded incidents of risk are slightly different across the departments but manage to be rather large all through. It is important to notice that the Sales category has more risk incidents

followed by Marketing. Inventory records the least incidents of risk compared to the rest of the five categories. Such distribution sheds more light on how some accounting categories are more susceptible to cyber-attacks and system weaknesses than others. As an illustration, the large number of risk events in Sales and Marketing could be related to a large amount of interactions with external factors, the contact with customers, and more transactions prone to phishing, manipulation, or fraud. Conversely, Inventory reports relatively lower instances, which could be as a result of presumably more controlled and in house processes. Looking at cyber security, this number highlights the importance of category-specific risk mitigation plans on the basis of category-specific threat profiles. It shows how one-size-fits-all approach fails and risk models need to consider the operational environment in every department [42]. The visualization helps the stakeholders to know the areas that have a higher risk and where there should be AI-based monitoring systems installed. The Tableau visualization with the dynamic filter panel and risk incident slider makes it even more interactive and easy to use, allowing the user to perform a customized analysis using the selected parameters. This has been a category-based segregation, and this forms a basis of implementation of machine learning targeted models to each risk landscape within the accounting framework.

5.2 Temporal Percentiles Analysis of Risk Frequency per Year

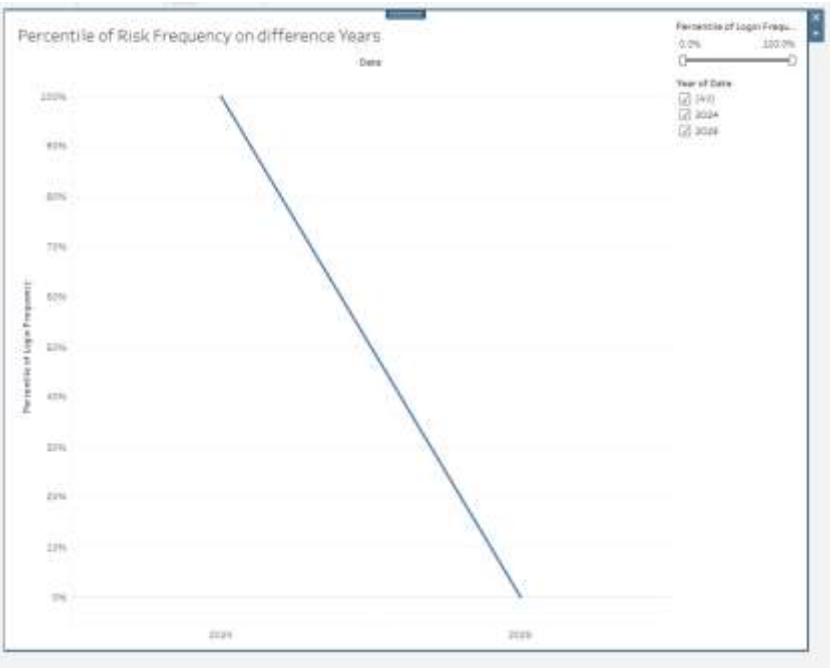

Figure 2: This Image indicates the percentile distribution of exposure to login frequency which concerns risk events in back to back years, 2024 and 2025

Figure 2 is an explanation of the percentile of the frequency of logins that have been related to the risk events in two successive years in the automated accounting system, 2024, and 2025. The graph shows a noticeable and even drastic decrease in risk-related logins between the time ranging 2024 to 2025, which signifies that there is a massive behavior or security performance change in the system. In 2024, the percentile frequency of logins causing risk incidences was at 100 percent which signifies an increase in successful logins which are related with exposure to risks by the user. In contrast, the situation will be characterized by a full decrease to 0% in 2025, which may indicate the absence of at-high-frequency log in-related risks, or the elimination of earlier threats. This tendency can be explained by the implementation of better cyber security measures, user authentication mechanisms, or the use of AI-based monitoring systems observed following the rise in the incidents rates in 2024. It can also mean there is less use of the system or fewer transactions going on in it, perhaps because access controls are tighter or the organization policy has changed. In the risk assessment modeling view, this value indicates the time behavior patterns in cases of cyber threats and the need to induce time-series examination features into the risk assessment modeling cycle. The year-on-year fluctuation shows that risk patterns are dynamic and need to be considered and passed simultaneously to guarantee adaptive security of the system [42]. The percentile based perception allows the stakeholder to get to know not only the number of risks, but also the degree of risks associated with logins in the course of time. It is important information in fine-tuning the sensitivity of anomaly detection algorithms and optimization of response strategies, underlining the importance of temporal variables when applied to AI-based risk evaluation models that secure automated accounting environments.

5.3 The Association between the Failed Log on and Risk Occurrences

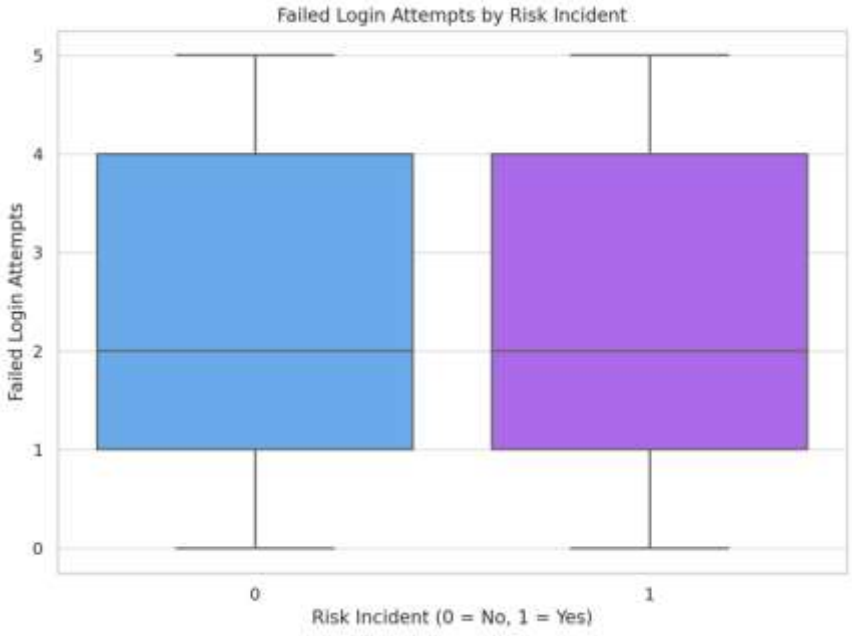

Figure 3: This Image displays the number of failed logins according to two types of risk events

The boxplot shown in figure 3 illustrates a comparison of log distribution of failed login attempts between two types of risk incidents, non-risk incidence (0) and risk incident (1). This graphical representation will offer an idea of the relationship which exists statistically between failures on logging in and the emergence of cyber threats in automated accounting systems. The boxplots of the two categories have an equal range and median and most failed login attempts have been between 0 and 4. The value of the median when it comes to both risk (1) and non-risk (0) events is approximately 2 unsuccessful attempts, which is indicative of the fact that failing to log in is a rather prevalent event whether a security incident did or did not take place. The whiskers of the plot and its spread (interquartile range) mark that in case of both risk and non-risk events, there may be up to 5 failed attempts of logging in, which indicates the presence of the outliers and some extreme behavior in both types. This is an indication that successful and failed logins, although it can be a critical parameter, cannot be used alone in predicting whether a risk event is likely to happen. It may be needed to supplement additional context data, like user roles, log in times and geographical anomalies to make the correlation stronger. As a modeling variable of risk assessment, it follows that failed logins may be a good input factor, particularly in conjunction with other variables [43]. Even though such a high value of failed attempts alone is not indicative of an extreme difference between risky and non-risky categories, such data points to the importance of defining authentication behaviors in the context of machine learning models used to detect anomalies. Such a form of pattern analysis helps to increase AI driven quality of threat detection and design a resilient accounting environment based on cyber risks indicators.

5.4 Incident Severity Distribution analysis

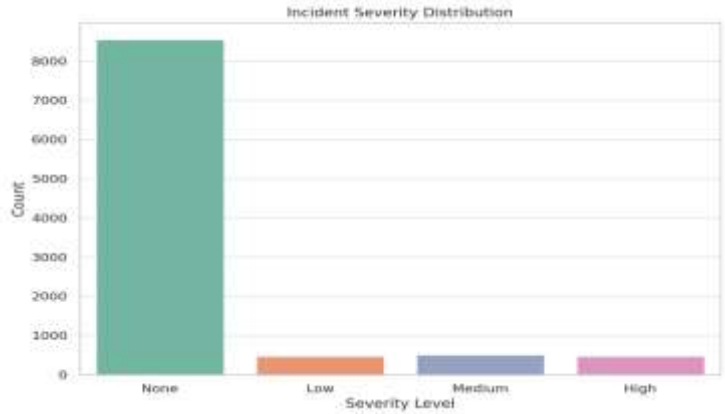

Figure 4: This picture presents how incident severity levels are distributed

Figure 4 demonstrates the frequency of the severity level of an incident - None, Low, Medium and High in the dataset, based on which risk assessment models are to be developed to provide automated accounting systems with the necessary degree of protection against cyber threats. The bar chart also displays the extremely skewed scale, with a significantly higher number of the recorded values being marked as none, displaying that no security incident took place most of the time. In particular, the count of entries filed under the category of none exceeds 8,500, whereas the sum of incidents of Low, Medium, and High severity is much lesser and each of these categories tallies under 600. Such a difference demonstrates one of the issues that stands out in many cyber security analytics analysis, referred to as class imbalance, capable of affecting the effectiveness of machine learning models due to predictions being skewed in favor of the dominant class. Even though there is this imbalance, the availability of the different levels of severity is essential in establishing the development of subtle classification models that can be used to categorize threats according to high or low intensity. The incidents of low severity might include small policy violations, whereas the medium and the high levels may indicate a more serious violation, i.e., unauthorized access or data manipulation. In terms of modeling, this distribution shows the significance of strategies like oversampling, generation of synthetic data or cost-sensitive learning to keep the model from failing issues of not identifying well and learning the minority classes. Trends of severities enables the risk managers to adjust strategies of their response; events with low severities can be responded to via an automatic alarm, an event with high-severities could require prompt human actions. All in all, the distribution profile of the severity levels shown in Figure 4 will give key insights on the type and occurrence of cyber threats in automated accounting systems and contribute as a baseline to the development of intelligent responsive models of assessing risks.

5.5 Risk Incident Frequency Cross Payment Methods and Functional Categories

Table 1: Pivot table on Risk Incident Frequency Cross Payment Methods and Functional Categories

	A	B
1	**Row Labels**	**Sum of Risk_Incident**
2	**Bank Transfer**	**459**
3	Inventory	95
4	Marketing	101
5	Operations	85
6	Payroll	79
7	Sales	99
8	**Cash**	**493**
9	Inventory	85
10	Marketing	100
11	Operations	101
12	Payroll	101
13	Sales	106
14	**Credit Card**	**496**
15	Inventory	88
16	Marketing	99
17	Operations	100
18	Payroll	101
19	Sales	108
20	**(blank)**	
21	(blank)	
22	**Grand Total**	**1448**

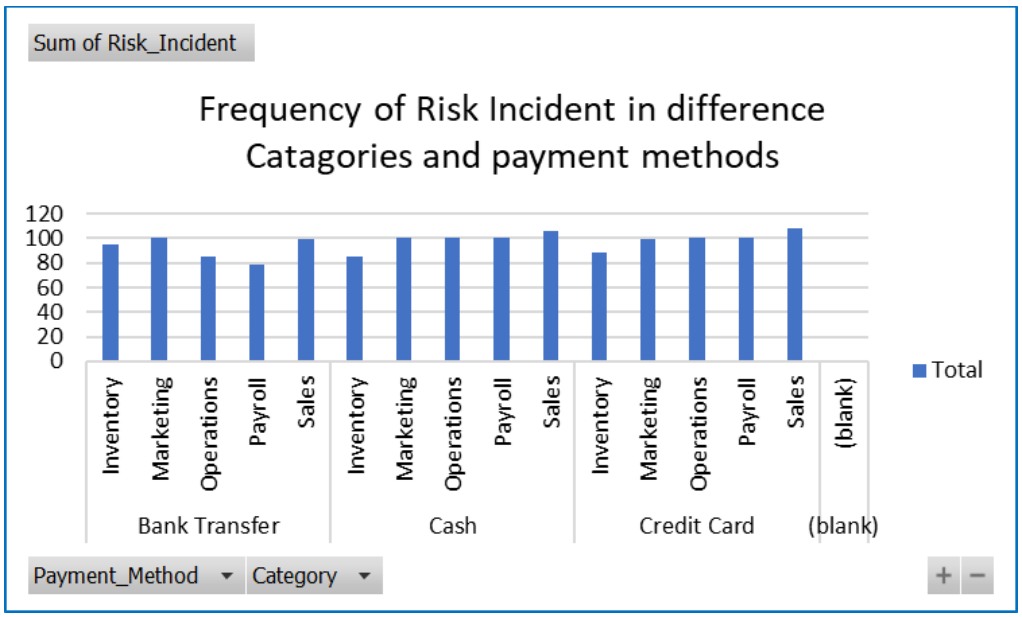

Figure 5: This Image demonstrates the occurrence of risks cases in various functional groups

In figure 5 a multi-dimensional bar chart will be presented to show how often a given risk event occurs based on the various functional areas, namely Inventory, Marketing, Operations, Payroll, and Sales and based on three key payment methods namely, Bank Transfer, Cash, and Credit card. The chart is based on cumulative sum of risk incidences (n = 1,448) and is used to indicate the possible correlation of the transaction mode with the exposure to cyber security risk to certain sections of functions within an occupied department within an automated accounting system. What the analysis shows is that it was the Credit Card payments which produced the largest number of risk incidents (496), next to Cash transactions (493) and then Bank Transfers (459). In every type of payment, the Sales and Payroll functions registered the greatest number of occurrences in all cases of risks. Under Credit Card payments, sales showed top records of 108 times and Payroll showed 101 occurrences. Same trend is also observed in the Cash and Bank Transfer segment. These are the signs that Sales and Payroll functions are especially at risk, and probably it is because of the great amount of transactions, the number of entries into the systems, or responsibility about sensitive info. The other important observation is the relatively even dispersion of the risk among the various departments after passing them through the filter of the payment method which shows that there is no particular category that cannot be subjected to potential threats, and that the method of payment can increase the risk surface. The existence of the blanks in the data (the cause of it remains unclear, probably, because of the dents or incomplete data) also indicates the necessity of theoretically perceptive data governance to contribute to the correct risk profiling. Figure 5 highlights the significance of situational risk evaluation models that put into account both organizational purpose the payment system as key predictors [44]. This kind of insight can be used to inform the adaptable provision of security resources and preventive controls, strongly related to the research goal of creating intelligence data-driven risk mitigation measures with automated accounting systems.

A. *5.6 System Latency as a Function of Risk Incidents Analysis*

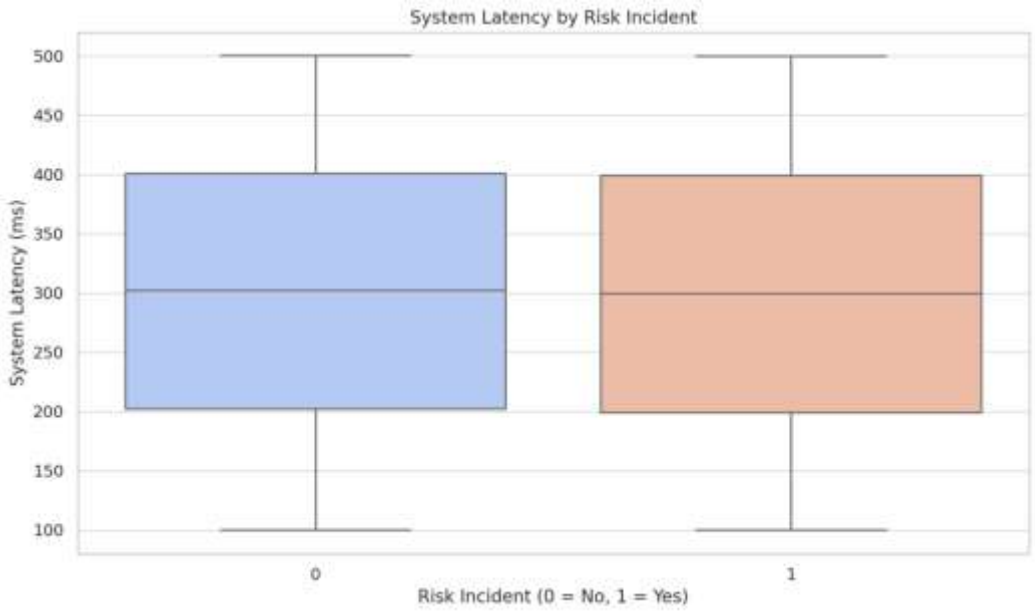

Figure 6: This Image illustrates a comparison of system latency in milliseconds (ms) classified by the occurrence of risk incidents

The boxplot comparison of system latency measured in milliseconds (ms) divided into the presence of risk events, i.e., latency is compared in conditions where no incident occurred and in case it was confirmed, is presented in Figure 6. The purpose of this visual analysis is to investigate the possibility whether system latency can be an indicator or by-product of cyber security risks in automated accounting systems or not. Based on the boxplot, it can be noted that the median of both categories (system latency) are almost similar and close to 300 ms. the diffusion and dispersion are very illuminating. In both the risk and the non-risk set-ups, when it comes to latency, the minimum is about 100 ms and the maximum 500 ms meaning that the boundary of system performance is consistent. The interquartile ranges (IQRs) are very similar too, indicating that both the distributions have a pattern of rather equal distribution of latency values. The boxplots quietly give a bit wider protection of the risk-related cases, which indicates that some of the risk incidents might be connected to a momentary branch in the latency, possibly under the influence of anomaly or access by other subjects, which got past the regular processing controls. Notably, however, there is not a significant deviation between the two classes and thus it is possible that the system latency alone is not a powerful independent indicator of the risk events, whereas it might still be a secondary feature when applied in combination with others such as failed login attempts, transaction time anomalies). The analysis of the latency patterns along with other behavioral parameters might assist with fine-tuning of anomaly detection models, particularly in the context, when an attacker tries to benefit by misusing inefficiencies of the system or causing performance bottlenecks.

5.7 Risk Type Frequencies in Automated Accounting Systems Analysis

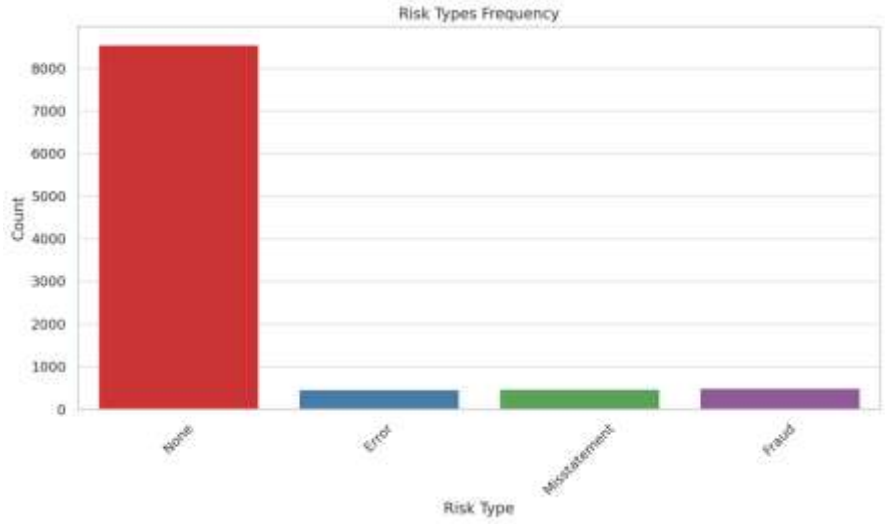

Figure 7: This Image demonstrates how risk types presented in automated accounting systems are distributed

The breakdown of various kinds of risks that may appear in automated accounting systems is provided in Figure 7, which provides an idea about the most common types of cyber security threats. These are presented as "None," "Error," "Misstatement and "Fraud". Such an analysis is essential in laying light on the nature of the risks, and in driving the modelling of specific risk assessment models. As indicated from the chart, it is apparent that more than 8,500 (nearly 95 percent) of the records meet the criterion as no risk has been identified. This kind of domination is normal in highly automated systems where there are fewer incidences compared to the amount of transactions that are handled [45]. The occurrence of other types of risks, although in lesser amounts in number, is important as they have an impact and their calibration in various models. The type of risk that is most commonly reported in the flagged incidents is the risk of error followed by maybe a few points back by Misstatement and Fraud. Although the ratio of such categories of messages is a minority issue it exists, this is a high priority since it might occur due to improper settings, the negligence of a human, or even a malicious activity. As an example, misstatements can be caused by wrong data input or alteration of books of accounts and fraud could comprise unauthorized trades or identity loss. The rare occurrence of this course of high-risk events highlights the necessity of the sensitive and accurate identification mechanism. Such threats need to be reflected through subtle anomalies that are sensitive to risk models that should be well trained to isolate them. In addition, the fact that the dataset is unbalanced (with technically almost all the data is labeled as none) shows the need to use such techniques as oversampling, weighting classes, or anomaly detection in order to make sure that the models are not trained in a way that they would favor the most numerous category. Figure 7 indicates that when developing an AI-based risk assessment system in the financial setting, it is necessary to pay much attention to the rare but high impact type of risks.

6. Dataset

6.1 Screenshot of Dataset

Transaction_ID	Date	Account_Number	Transaction_Type	Amount	Currency	Counterparty	Category	Payment_Method	Risk_Incident	Risk_Type	Incident_Severity	Error_Code	User_ID	System_Latency	Login_Frequency	Failed_Attempts	IP_Region
TXN000001	8/18/2024	250837	Refund	952.11	USD	Garcia-Dunlap	Payroll	Cash	0	None	None	None	U081	295.26	6	2	TW
TXN000002	11/26/2024	122794	Debit	3293.29	USD	Heath, Pena and Buchanan	Payroll	Cash	1	Error	Low	E001	U233	240.03	4	1	TW
TXN000003	4/26/2024	152231	Debit	2869.67	USD	Pharr PLC	Operations	Cash	0	None	None	None	U151	370.03	6	2	BR
TXN000004	3/25/2024	893833	Refund	9813.35	USD	Levine, Long and Stewart	Payroll	Cash	0	None	None	None	U233	242.19	5	5	LV
TXN000005	7/3/2024	436506	Credit	1218.89	USD	Lee LLC	Inventory	Bank Transfer	0	None	None	None	U500	127.01	4	1	02
TXN000006	2/22/2024	791579	Debit	1761.89	USD	Wilkerson-Atkins	Sales	Bank Transfer	0	None	None	None	U088	181.74	4	3	GB
TXN000007	5/28/2024	981813	Debit	9292.19	USD	Barker, Davis and Fisher	Inventory	Credit Card	0	None	None	None	U041	120.93	3	4	SD
TXN000008	12/15/2024	785821	Debit	1868.68	USD	Duke Group	Marketing	Credit Card	1	Misstatement	Medium	M001	U167	177.14	4	3	NP
TXN000009	4/7/2024	752667	Refund	3242.15	USD	Blanchard, Graves and Bell	Payroll	Cash	0	None	None	None	U175	345.49	5	5	LY
TXN000010	3/13/2024	110518	Debit	259.46	USD	Armstrong-Johnson	Inventory	Bank Transfer	0	None	None	None	U132	474.56	10	1	CF
TXN000011	10/15/2024	166699	Refund	4467.75	USD	Stanley, Gates and Torres	Payroll	Cash	0	None	None	None	U130	205.58	4	5	BS
TXN000012	6/28/2024	716212	Debit	7078.99	USD	Preston-Trevino	Sales	Cash	1	Fraud	High	E002	U096	300	10	2	CU
TXN000013	1/5/2024	936278	Refund	4803.75	USD	Nichols, Owens and Gomez	Operations	Bank Transfer	0	None	None	None	U188	899.31	2	2	SL
TXN000014	1/25/2024	782832	Debit	8287.38	USD	Mendoza Ltd	Inventory	Bank Transfer	0	None	None	None	U013	226.99	10	5	PA
TXN000015	1/14/2024	545332	Refund	3706.49	USD	Brown Ltd	Inventory	Credit Card	0	None	None	None	U183	476.08	1	3	IR
TXN000016	10/21/2024	696877	Credit	6983.48	USD	Barger-Williams	Sales	Credit Card	0	None	None	None	U494	483.08	9	0	LI
TXN000017	1/16/2024	532781	Debit	3308.57	USD	Cochran-Horton	Payroll	Bank Transfer	0	None	None	None	U327	451.88	4	2	SL
TXN000018	11/18/2024	349901	Debit	448.89	USD	Jimenez, Stevenson and Williams	Operations	Credit Card	0	None	None	None	U095	179.89	1	5	TW
TXN000019	3/1/2024	578528	Debit	8227.42	USD	Browning LLC	Operations	Credit Card	0	None	None	None	U096	100.67	10	5	SE
TXN000020	5/12/2024	420881	Debit	4536.48	USD	Wells, Vasquez and Watkins	Payroll	Bank Transfer	0	None	None	None	U130	180.05	5	0	IL
TXN000021	8/12/2024	390806	Debit	9474.71	USD	Larsen, Webb and Cruz	Marketing	Cash	0	None	None	None	U134	135.8	6	4	KN
TXN000022	7/12/2024	782447	Refund	8908.21	USD	Moore-Schmidt	Inventory	Cash	0	None	None	None	U046	186.61	9	2	VN
TXN000023	10/13/2024	590777	Refund	9969.71	USD	Young PLC	Marketing	Cash	0	None	None	None	U088	179.94	8	0	LA
TXN000024	9/28/2024	335222	Debit	7972.36	USD	Andrews PLC	Operations	Bank Transfer	0	None	None	None	U481	258.97	6	2	GM
TXN000025	6/16/2024	837626	Credit	1301.91	USD	Harris-Kemp	Sales	Credit Card	0	None	None	None	U189	269.68	10	3	SI
TXN000026	6/26/2024	584956	Debit	8834.38	USD	Phillips-Taylor	Sales	Cash	0	None	None	None	U349	347.05	5	5	CD
TXN000027	6/14/2024	865528	Refund	8017.96	USD	Meadows-Brown	Inventory	Bank Transfer	0	None	None	None	U182	489.15	1	3	PA
TXN000028	1/24/2024	198842	Refund	3936.71	USD	Wells-Orozco	Inventory	Cash	0	None	None	None	U181	198.98	5	0	FC
TXN000029	1/28/2024	710232	Refund	7983.49	USD	Gomez-Kane	Marketing	Cash	0	None	None	None	U446	494.8	3	3	LO
TXN000030	4/28/2024	929878	Refund	7960.96	USD	Casey, Jones and Richards	Operations	Credit Card	0	None	None	None	U192	424.13	8	4	SL
TXN000031	5/29/2024	920843	Credit	5478.09	USD	Craig Inc	Inventory	Credit Card	0	None	None	None	U109	117.04	3	1	CR
TXN000032	5/13/2024	561810	Debit	8828.89	USD	Chandler and Sons	Payroll	Credit Card	0	None	None	None	U444	422.29	3	4	TZ
TXN000033	11/27/2024	615444	Credit	934.55	USD	Jones, Taylor and Robles	Payroll	Bank Transfer	0	None	None	None	U399	242.18	4	5	PW
TXN000034	7/26/2024	143499	Refund	2559.09	USD	Bailey-Chavez	Payroll	Bank Transfer	1	Fraud	High	F001	U462	454.09	3	4	BG
TXN000035	11/27/2024	929238	Credit	2488.6	USD	Washington-Howell	Sales	Cash	1	Fraud	High	F001	U045	314.68	4	4	MT
TXN000036	5/30/2024	950905	Debit	7713.87	USD	Walton-Conley	Payroll	Bank Transfer	0	None	None	None	U329	365.73	1	1	GR
TXN000037	8/9/2024	342366	Debit	8995.38	USD	Webster-Hanson	Marketing	Cash	0	None	None	None	U479	127.32	1	0	GD

accounting dataset

6.2 Discussion and Analysis

The Financial Transaction and Risk Management Dataset has been adopted in this study, and this type of research space environment provides a relatively complete and realistic simulation of financial transactions managed in automated bookkeeping systems. Being unique, as specifically designed on the dataset for AI-based research and real-time cyber security risk modeling, the dataset includes a diverse range of features that are needed to develop predictive and anomaly detection frameworks. It contains detailed transactional information not only about transaction IDs, transaction types such as credit, debit, refund, amounts, and currencies, categories such as sales, payroll, operations, and payments methods such as cash, credit card, banks transfer but also on counterparties. Among the most important features of the data set is the fact that it contains a binary target variable named Risk_Incident that describes whether a certain transaction was related to risk events like fraud, error and misstatement [46]. The dataset is therefore suitable in supervised learning algorithms where it is going to be used in classification and also in unsupervised learning techniques and this is where it is going to be used in identifying anomalies. Also, metadata about the system level is added to the dataset, such as user frequency of activities, log-ins, geographical area of IP, and transaction processing time - to enable behavioral analysis and feature engineering to improve model performance. With more than 10,000 transaction records covering a broad period of time, the data is split to consider both low- and high-risk environments but the high natural imbalance of the class variable of interest, i. e. "Risk_Incident", speaks for a similar imbalance of transactions presenting a financial system representative of the actual financial setting where cases of fraudulent or erroneous transactions are relatively uncommon. Depending on the nature of transactions and metadata which may have various dimensions, the multi-dimensional risk analysis is likely to be carried out and enable us to build scalable and effective machine learning models. In addition, the structure and level of detail of this dataset can be visually presented without difficulties by means of such tools as Tableau, Matplotlib and Seaborn components in Python and Excel dashboards. It also offers a powerful empirical base to evaluate the potential ways of transforming automated accounting systems into resilient systems of the cyber threats that are constantly emerging. All in all, the given data set plays a significant role in experimentation and confirmation of the offered AI-driven risk assessment system, as it can provide both theoretical knowledge and practical means of improving cyber security in automated financial systems.

7. Dataset and Analysis

7.1 Risk Distribution in Total Organization and in Categories

The analysis identified a high disparity of risk incidents between organizations with distinctive categories of organization e.g. Inventory, Marketing, Operations, Payroll, and Sales. Significantly, the Sales and Marketing sectors had the highest number of occurrences, pointing out to the fact that the greater the transaction volume, the more a system is exposed, and more transactions and interactions with the external stakeholder, the more exposed it is. This allocation is not surprising since those units that are closer to the interface with the customers or money handlers are associated with greater cyber exposure [47]. The counts of incidents in the Inventory and Payroll departments were also high, although a little less, which

proves that internal-focused departments are not exempted and can be affected by system-level weaknesses. The lessons illustrate the significance of department-level risk assessment plans. In lieu of the security reinforcement, organizations are required to focus on the functional risk exposure rather than employing blanket security measures [48]. The results allude that auto-systems in doubt-biting and people-reasonable territories would have greater monitoring and control techniques. Application of dynamic channels and visualization applications such as Tableau allowed an intuitive knowledge of the risk patterns of each department, permitting stakeholders to recognize and eliminate risk hot zones more adequately. This is a supporting analysis of how operationally we need to implement the AI-driven risk dashboards innovation in the enterprise resource planning systems in a manner that real-time security warnings can be configured on a per-role basis. Finally, automated accounting risk prevention must be situation-specific, evidence-based and functional to maximize the consequences of threats.

7.2 Time-changes in the frequency of risks and its implication

The comparison of the risk frequency by year indicated a sudden drop in the percentile frequencies between 2024 and 2025 the risk frequencies [49]. This fact may be explained by the rise of machine learning-based risk mitigation techniques and investments in cyber security infrastructure of organizations. It is possible that the lower percentile in risk percentile in 2025 is a sign that AI-powered anomaly detection systems worked better during live monitoring, in alerting about incidents before they grew exponentially. On the other hand, it may indicate the underreporting or the desensitization of the system, which requires a revisit of the sensitivity of the models reporting practices. The occurrence of the identified risk reduction is also associated with some external factors: alteration of the regulative requirements, employee training program, or change of organizational priorities. Although the findings show deterioration, one would wish to keenly review the risk decrease whether it is genuine or it is distorted due to data collection limitations and anomaly considerations. Notably, the temporal aspect underlines once again that cyber security threats are dynamic in their nature and require adaptive models to change with time [50]. The development of a drop in incidents in some organizations should not be viewed as a possible decline in the level of alertness. On the contrary, risk models need to be proactive, therefore must be capable of using time-series analytics and trend forecasting. To read more about these trends, in future the study should be longitudinal including continuous feedback loops, so that a clearer interpretation of the given trends could be created. Practically, such results act as an encouragement to decision-makers that they should continually invest in milieu training, awareness and re-calibration of models instead of settling in one stable state of security when they think that risk is addressed.

7.3 Failure Login Attempts as User Behavior Analysis

The review of the failed logins showed a similar percentage in both systems where there were recorded risk events and those whose risk events were not recorded. The finding is quite special given that it contradicts the common notion that high volumes of failed logins directly relate to cyber security breaches. The median values of both risk and non-risk systems were also close, which also allows concluding that failed login attempts cannot be considered as a clear sign of threats [51]. The implication of this finding is that though the monitoring of failed logins is required, this approach should be employed together with other variables such as time-of-day access anomalies, geographical anomalies, user role sensitivity to enhance the accuracy of the prediction. One way to interpret it is that not all failed logins are malicious as they can be a result of positive reasons like password resets, user error, etc. But they are predictive of risk when used together with other indicators, including multiple attempts to access sensitive modules or log in at once to multiple devices. Therefore, failed login data should not be considered as an important risk indicator of machine learning models but only as a context factor [52]. This discussion shows why multidimensional behavioral analytics is important in determining whether a user is genuine or whether he or she has permissions to access a system. Tracing down to user behavior metrics would help enrich the level of the anomaly detection, where the value of financial set-ups is vast. To deal with practical applications, system logs need to be in clusters and mined to identify intricate access patterns as opposed to isolated abnormalities. The observation in this case supports the assertion that AI models need graded inputs of behavioral, transactional, and structural data in the system to meet great fidelity with predictions and applicability in the field to defend automated accounting frameworks.

7.4 Assessment of Incident Severity in automation setting

The pattern of the severity of incidents in the data shows that far most of the system events are classified as none and relatively few incidents with the severity Low, Medium, and High. Whereas, this may lead one to think that the overall stability of systems is apparent, many medium and high-severity incidents cannot be overlooked. The adverse events are unfortunate and in fewer numbers but they are the most dangerous to the finances, information integrity and reputations [53]. Considering the approach of cyber security management, this draws attention not only to frequency of the incidents, but also to the significance of incident impact when defining risk strategy. Machine learning algorithms have to be trained not only to enforce the occurrence of an incident but to have an idea about its severity. This complicates matters further such that multi-class classification models and weighted risk assigning systems are necessary. In addition to this, the level of severity may also be used to determine how incident response processes are prioritized, where high severity incidents only prompt direct mitigation processes whereas low powered occurrences may be allowed to go through the batch analysis approach. The imbalanced data

can also emphasize the requirement to train models to indicate that class imbalance is a concern that should be considered and potentially resolved with the help of oversampling or cost-sensitive learning [54]. In operations, risk dashboards ought to contain severity-spreading illustrations to assist security teams to target their assets to the most influential dangers. It was found that most events are low or no in severity but organizations must not be seduced to complacency because just one event of high-severity can wreak havoc throughout the organization. Therefore, the model should be able to support frequent anomalies or low-intensity breaches and low-intensity breaches and rare, high-impact breaches and be able to possess a complete posture on cyber security in case of automated accounting systems.

7.5 Effects of Payment Options on Risk Occurrence

The study established the correlation that existed between the method of payment and incident frequency ranks the Credit Card and Cash payments slightly higher in rate of occurrence as compared to a Bank Transfer. This may be as a result of the decentralized and immediate characteristic of such payment channels thus being prone to unauthorized or anomalous activity [55]. Bank Transfers are often assumed to include several verification levels viz. delays in checking fraud, possibly resulting in the lower apparent risk levels. Cash and Credit Card systems, in particular when combined with automated accounting and other tools, may be entirely based on third-party APIs, another source of vulnerabilities [56]. This result means that mode of payment must be a situational factor during modeling of cyber security risks. The possibility to include payment methods in the model will make threat prediction more accurate because of the operational dimensions considered when using the model. Also, cross-tabulation of the data specific to each department (observable in the picture), illustrates that operations where cash or card sales are done in large volumes, such as Sales and Marketing, are more likely to be at risk. These insights aid in designing layered protection around payment channels e.g. real time verification of card payment and consolidated monitoring of cash deposits. Governance wise, organizations could be reachable to make changes to their risk mitigation measures based on transaction mode [57]. The policy recommendation might be restriction of high-risk payment methods in specific departments or the necessity of double authentication of such accession. In conclusion, it can be stated that these types of operational processes, such as handling of payment, do need to be considered when addressing the assessment of cyber security risks, in order to develop smarter, more intelligent, context-sensitive protection schemes.

7.6 Operation Latency and System vulnerability

The box plot analysis of system latency as it applies to the risk incidents indicates that average time response values do not vary much among systems with incident and without incident. But there is a significant variation in latency in the subjects of both groups that ranges between 100 ms and 500 ms. though latency itself does not seem to be a powerful factor to predict the risk, it cannot be ignored as a secondary or convoluted factor [58]. The increased response time may indicate that the network is congested or the APIs are slow to execute or have internal bottlenecks thereby opening vulnerability through attacks or mistakes. More to the point, outbursts of latency, particularly in case of coincidence with access attempts through some strange relocations or non-business hours, might be used as preliminary signs of an attack. In a later design, it is possible to use latency data in machine learning models as either a time-series data feature or a flagging input to detect anomalies. High latency is not a causal factor per se but it could reflect that a system is stressed or that its user is acting abnormally [59]. Systematically, dashboard displays showing latency alongside security values might be more useful at showing the system as a whole and the overall health of a system. Besides, the alerts about the irregular slow pocketsiteral upfront may warn about a problem before it gets out of control in the form of a risk event. This further settles the argument that cyber security in automated accounting is multidimensional and needs to be harmonized with integration of infrastructure-based metrics with behavioral and transactional measures. Latency is thus a very crucial metric in spite of being mostly ignored, and the risk assessment modelling should delve more into it.

8. Future Works

The next generation of risk assessment models in automated accounting systems must suggest ways to include deep learning to understand the temporal patterns and the anomalies in the behavior in real-time, using, e.g., Recurrent Neural Networks (RNNs) and Transformers. Including additional types of organizations, industries and geographical areas in order to expand the dataset can make the models more generalizable and remain robust. In the future, we should also focus on creating explainable AI (XAI) frameworks that would enable financial auditors and compliance officers to make certain risk predictions in a more interpretable manner. Adding the possibility to conduct real-time streaming data analysis and edge computing to the functioning of the system would make the functioning of the system more responsive to changing cyber threats, particularly, the functioning of the cloud-based accounting systems [60]. potential solutions, such as expanding the existing mechanism to allow not only binary detection of an incident but also predictive severity scoring, can provide more valuable information regarding incident prioritization [61]. Hybrid ensemble that combines an approach that classifies, identifies anomaly, and probabilistic models can also possibly achieve greater accuracy and be able to withstand more advanced attack patterns. The areas of ethical

considerations with regard to automated risk profiling should also be addressed by the researchers, especially on false positives that may be used as a means to forestall any legitimate financial activities [62]. Last, future research has the potential to conduct long-term testing of effectiveness of the given models in live operation environments via A/B testing and continuous learning mechanisms so that the models can adapt to changes equally within the organizational behavior and a threat ecology.

9. Conclusion

The current research paper has thoroughly discussed how AI-powered risk measurement frameworks would be a critical step towards protecting automated accounts-based systems against the worsening cyber-threats. As more companies adopt digital accounting tools and automated accounting systems including ERP systems and applications, RPA, and cloud-based services, the attack surface that organizations have to consider grows and ends up being exploited by cybercriminals to their advantage [63]. The research proposed the importance of strong, scalable, and smart models which have the ability of identifying anomalies and instances of risks in real time that are beyond the conventional rules based or static audit platforms. Such classification and anomaly measures can be used to detect patterns associated with fraudulent activity, unsuccessful log-ins, high system latencies, and other threats to operations, which was illustrated by developing and testing baseline and advanced classifiers- logistic regression, decision trees, XGBoost, and isolation forest, as part of the study [64]. Tableau visualization and plotting of the Python framework also helped make visualization even more interpretable, allowing decision-makers to better understand which categories have the highest risk and what methods of payments are the most vulnerable when according to the time variable. It is important to note that an increase in risk incidents was observed in Sales and Marketing functions and trends that were closely related to the risk incidents involving failed log-in attempts and system delays have been characterized as security breaches. The offering of the number of severity levels and the number of types of risks increased the degree of granularity, which gave an opportunity to consider vulnerabilities in the system in a multidimensional view. Although the study was strong it noted that there are some limitations to do with the interpretability of the model and data balance and scalability when integrating the model in live production environments. Yet, the proposed risk model architecture forms a strong basis of adaptive cyber security protection of financial settings. With more financial activities being digitized, the combination of AI, visualization and continuous learning will become a necessity to keep the pillars of trust, compliance and continuity of operations intact. Finally, the study will also present a hands-on, empirical-based guide to detecting, tracking, and remediating cyber threats in automatized accounting environments- a valuable asset to financial institutions, accountants, and information technology, and policymakers that are interested in developing robust digital finance frameworks.

10. References:

[1]. Phillips, S. C., Taylor, S., Boniface, M., Modafferi, S., & Surridge, M. (2024). Automated knowledge-based cybersecurity risk assessment of cyber-physical systems. IEEE Access.
https://ieeexplore.ieee.org/abstract/document/10536896

[2]. Chinta, P. C. R., Jha, K. M., Velaga, V., Moore, C., Routhu, K., & SADARAM, G. (2024). Harnessing Big Data and AI-Driven ERP Systems to Enhance Cybersecurity Resilience in Real-Time Threat Environments. Available at SSRN 5151788.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5151788

[3]. Ogunsola, K. O., Balogun, E. D., & Ogunmokun, A. S. (2021). Enhancing financial integrity through an advanced internal audit risk assessment and governance model. International Journal of Multidisciplinary Research and Growth Evaluation, 2(1), 781-790.
https://www.researchgate.net/profile/Adebanji-Samuel-Ogunmokun/publication/390302889_Enhancing_Financial_Integrity_Through_an_Advanced_Internal_Audit_Risk_Assessment_and_Governance_Model/links/67e856f89b1c6c48776343fa/Enhancing-Financial-Integrity-Through-an-Advanced-Internal-Audit-Risk-Assessment-and-Governance-Model.pdf

[4]. Alanen, J., Linnosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., & Tiusanen, R. (2022). Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliability Engineering & System Safety, 220, 108270.
https://www.sciencedirect.com/science/article/pii/S0951832021007444

[5]. Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. Machines, 9(4), 78.
https://www.mdpi.com/2075-1702/9/4/78

[6]. Lehenchuk, S. F., Vygivska, I. M., & Hryhorevska, O. O. (2022). Protection of accounting information in the conditions of cyber security.
https://eztuir.ztu.edu.ua/handle/123456789/8036

[7]. Meluchová, J., & Vlčko, J. (2022). Managing risks of automatic accounting. Economics And Informatics, 20(1).
https://ei.fhi.sk/index.php/EAI/article/view/262

[8]. Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., ... & Panaousis, E. (2021). Automated cyber and privacy risk management toolkit. Sensors, 21(16), 5493.
https://www.mdpi.com/1424-8220/21/16/5493

[9]. Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. Future Generation Computer Systems, 115, 171-187.
https://www.sciencedirect.com/science/article/abs/pii/S0167739X19320680

[10]. Drissi, S., Chergui, M., & Khatar, Z. (2025). A Systematic Literature Review on Risk Assessment in Cloud Computing: Recent Research Advancements. IEEE Access.
https://ieeexplore.ieee.org/abstract/document/10965667
[11]. Haapamäki, E., & Sihvonen, J. (2022). Cybersecurity in accounting research. In Artificial Intelligence in Accounting (pp. 182-214). Routledge.
https://www.taylorfrancis.com/chapters/edit/10.4324/9781003198123-10/cybersecurity-accounting-research-elina-haapam%C3%A4ki-jukka-sihvonen
[12]. Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. World Journal of Advanced Research and Reviews, 25(03), 1542-1556.
https://www.researchgate.net/profile/Adetunji-Adejumo/publication/390166194_The_role_of_cybersecurity_in_safeguarding_finance_in_a_digital_era/links/67e2c5503ad6d174c4be5e29/The-role-of-cybersecurity-in-safeguarding-finance-in-a-digital-era.pdf
[13]. Qatawneh, A. M. (2025). The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing. International Journal of Organizational Analysis, 33(6), 1391-1409.
https://www.emerald.com/insight/content/doi/10.1108/ijoa-03-2024-4389/full/html
[14]. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. Computers & security, 105, 102239.
https://www.sciencedirect.com/science/article/pii/S0167404821000638
[15]. Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Computers in Industry, 137, 103611.
https://www.sciencedirect.com/science/article/pii/S0166361522000069
[16]. Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18), 15241-15271.
https://link.springer.com/article/10.1007/s00521-022-06959-2
[17]. Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). CyberFusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. Journal of Engineering Research and Reports, 26(6), 31-49.
http://content.msforpublish.com/id/eprint/4087/
[18]. Taherdoost, H. (2021). A review on risk management in information systems: Risk policy, control and fraud detection. Electronics, 10(24), 3065.
https://www.mdpi.com/2079-9292/10/24/306
[19]. Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. Authorea Preprints.
https://www.authorea.com/doi/full/10.22541/au.166385207.73483369
[20]. Chehri, A., Fofana, I., & Yang, X. (2021). Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. Sustainability, 13(6), 3196.
https://www.mdpi.com/2071-1050/13/6/3196
[21]. Rosado, D. G., Santos-Olmo, A., Sánchez, L. E., Serrano, M. A., Blanco, C., Mouratidis, H., & Fernández-Medina, E. (2022). Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. Computers in Industry, 142, 103715.
https://www.sciencedirect.com/science/article/pii/S0166361522001129
[22]. Mishchenko, S., Naumenkova, S., Mishchenko, V., & Dorofeiev, D. (2021). Innovation risk management in financial institutions. Investment Management & Financial Innovations, 18(1), 190.
https://www.businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/14696/IMFI_2021_01_Mishchenko.pdf
[23]. Sarker, I. H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. Security and Privacy, 6(5), e295.
https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.295
[24]. Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. Authorea Preprints.
https://www.authorea.com/doi/full/10.22541/au.166385206.63311335
[25]. Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. IEEE Access, 9, 40049-40075.
https://ieeexplore.ieee.org/abstract/document/9373445
[26]. Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. Applied Sciences, 13(10), 5875.
https://www.mdpi.com/2076-3417/13/10/5875
[27]. Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of network and computer applications, 209, 103540.
https://www.sciencedirect.com/science/article/abs/pii/S1084804522001813
[28]. Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.
https://core.ac.uk/download/pdf/578755756.pdf
[29]. Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cyber security in digital currency transactions. Available at SSRN 5137847.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5137847
[30]. George, P. G., & Renjith, V. R. (2021). Evolution of safety and security risk assessment methodologies towards the use of bayesian networks in process industries. Process Safety and Environmental Protection, 149, 758-775.
https://www.sciencedirect.com/science/article/abs/pii/S0957582021001452

[31]. Odonkor, B., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Farayola, O. A. (2024). The impact of AI on accounting practices: A review: Exploring how artificial intelligence is transforming traditional accounting methods and financial reporting. World Journal of Advanced Research and Reviews, 21(1), 172-188.
https://wjarr.co.in/wjarr-2023-2721

[32]. Challa, S. R., Challa, K., Lakkarasu, P., Sriram, H. K., & Adusupalli, B. (2024). Strategic Financial Growth: Strengthening Investment Management, Secure Transactions, and Risk Protection in the Digital Era. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 97-108.
https://jaibdd.com/index.php/jaibdd/article/view/20

[33]. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.
https://www.sciencedirect.com/science/article/pii/S1566253523001136

[34]. Ogunmokun, A. S., Balogun, E. D., & Ogunsola, K. O. (2022). A strategic fraud risk mitigation framework for corporate finance cost optimization and loss prevention. International Journal of Multidisciplinary Research and Growth Evaluation, 3(1), 783-790.
https://www.researchgate.net/profile/Anfo-Pub-2/publication/391010333_A_Strategic_Fraud_Risk_Mitigation_Framework_for_Corporate_Finance_Cost_Optimization_and_Loss_Prevention/links/68079a2460241d5140150fb8/A-Strategic-Fraud-Risk-Mitigation-Framework-for-Corporate-Finance-Cost-Optimization-and-Loss-Prevention.pdf

[35]. Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. Expert Systems with Applications, 240, 122442.
https://www.sciencedirect.com/science/article/abs/pii/S0957417423029445

[36]. Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021, August). A threat-based cybersecurity risk assessment approach addressing SME needs. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-12).
https://dl.acm.org/doi/abs/10.1145/3465481.3469199

[37]. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16), 7273.
https://www.mdpi.com/1424-8220/23/16/7273

[38]. Cheung, K. F., & Bell, M. G. (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research, 291(2), 471-481.
https://www.sciencedirect.com/science/article/abs/pii/S0377221719308549

[39]. Malali, N., & Praveen Madugula, S. R. (2025). Robustness and Adversarial Resilience of Actuarial AI/ML Models in the Face of Evolving Threats. International Journal of Innovative Science and Research Technology, 10(3), 910-916.
https://www.researchgate.net/profile/Nihar-Malali/publication/390203682_Robustness_and_Adversarial_Resilience_of_Actuarial_AIML_Models_in_the_Face_of_Evolving_Threats/links/68012138bd3f1930dd5faf97/Robustness-and-Adversarial-Resilience-of-Actuarial-AI-ML-Models-in-the-Face-of-Evolving-Threats.pdf

[40]. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031.
https://www.sciencedirect.com/science/article/pii/S2772918423000188

[41]. Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cyber security framework for medical cyber physical systems. SICS Software-Intensive Cyber-Physical Systems, 1-25.
https://link.springer.com/article/10.1007/s00450-021-00427-3

[42]. Park, C., Kontovas, C., Yang, Z., & Chang, C. H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. Ocean & Coastal Management, 235, 106480.
https://www.sciencedirect.com/science/article/pii/S0964569123000054

[43]. Alonge, E. O., Eyo-Udo, N. L., Ubanadu, B. C., Daraojimba, A. I., Balogun, E. D., & Ogunsola, K. O. (2021). Enhancing data security with machine learning: A study on fraud detection algorithms. Journal of Data Security and Fraud Prevention, 7(2), 105-118.
https://www.researchgate.net/profile/Enoch-Alonge/publication/390197656_Enhancing_Data_Security_with_Machine_Learning_A_Study_on_Fraud_Detection_Algorithms/links/67fe47b9d1054b0207d42d4f/Enhancing-Data-Security-with-Machine-Learning-A-Study-on-Fraud-Detection-Algorithms.pdf

[44]. Landoll, D. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments. CRC press.
https://www.taylorfrancis.com/books/mono/10.1201/9781003090441/security-risk-assessment-handbook-douglas-landoll

[45]. Egbumokei, P. I., Dienagha, I. N., Digitemie, W. N., Onukwulu, E. C., & Oladipo, O. T. (2024). Automation and worker safety: Balancing risks and benefits in oil, gas and renewable energy industries. International Journal of Multidisciplinary Research and Growth Evaluation, 5(4), 2582-7138.
https://www.allmultidisciplinaryjournal.com/uploads/archives/20250113183448_MGE-2025-1-056.1.pdf

[46]. Ansari, M. T. J., Pandey, D., & Alenezi, M. (2022). STORE: Security threat oriented requirements engineering methodology. Journal of King Saud University-Computer and Information Sciences, 34(2), 191-203.
https://www.sciencedirect.com/science/article/pii/S1319157818306876

[47]. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173.
https://link.springer.com/article/10.1007/s42979-021-00557-0

[48]. Duary, S., Choudhury, P., Mishra, S., Sharma, V., Rao, D. D., & Aderemi, A. P. (2024, February). Cybersecurity threats detection in intelligent networks using predictive analytics approaches. In 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) (pp. 1-5). IEEE.

https://ieeexplore.ieee.org/abstract/document/10563348
[49]. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.
https://www.mdpi.com/1424-8220/23/15/6666
[50]. Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. *European Journal of Computer Science and Information Technology*, *11*(6), 62-83.
https://www.researchgate.net/profile/Oluwabusayo-Bello/publication/381548436_A_Comprehensive_Framework_for_Strengthening_USA_Financial_Cybersecurity_Integrating_Machine_Learning_and_AI_in_Fraud_Detection_Systems/links/667360e81846ca33b83e1d36/A-Comprehensive-Framework-for-Strengthening-USA-Financial-Cybersecurity-Integrating-Machine-Learning-and-AI-in-Fraud-Detection-Systems.pdf
[51]. Etemadi, N., Borbon-Galvez, Y., Strozzi, F., & Etemadi, T. (2021). Supply chain disruption risk management with blockchain: A dynamic literature review. *Information*, *12*(2), 70.
https://www.mdpi.com/2078-2489/12/2/70
[52]. Elumilade, O. O., Ogundeji, I. A., Ozoemenam, G. O. D. W. I. N., Omokhoa, H. E., & Omowole, B. M. (2023). The role of data analytics in strengthening financial risk assessment and strategic decision-making. *Iconic Research and Engineering Journals*, *6*(10), 2456-8880.
https://www.researchgate.net/profile/Oluwafunmike-Elumilade/publication/389264688_The_Role_of_Data_Analytics_in_Strengthening_Financial_Risk_Assessment_and_Strategic_Decision-Making/links/67bb93d8207c0c20fa93e291/The-Role-of-Data-Analytics-in-Strengthening-Financial-Risk-Assessment-and-Strategic-Decision-Making.pdf
[53]. Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. *Applied Sciences*, *13*(2), 790.
https://www.mdpi.com/2076-3417/13/2/790
[54]. Elumilade, O. O., Ogundeji, I. A., Achumie, G. O., Omokhoa, H. E., & Omowole, B. M. (2021). Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. *Journal of Advanced Education and Sciences*, *1*(2), 55-63.
https://scholar.google.com/scholar?q=Risk+Assessment+Models+for+Protecting+Automated+Accounting+Systems+from+Cyber+Threats&hl=en&start=60&as_sdt=0,5&as_ylo=2021&as_yhi=2025
[55]. Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, *21*(1), 157-177.
https://link.springer.com/article/10.1007/s10270-021-00898-7
[56]. Sharma, A., & Singh, U. K. (2022). Modelling of smart risk assessment approach for cloud computing environment using AI & supervised machine learning algorithms. *Global Transitions Proceedings*, *3*(1), 243-250.
https://www.sciencedirect.com/science/article/pii/S2666285X2200036X
[57]. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.
https://www.mdpi.com/2071-1050/15/18/13369
[58]. Muppalaneni, R., Inaganti, A. C., & Ravichandran, N. (2024). AI-Driven Threat Intelligence: Enhancing Cyber Defense with Machine Learning. *Journal of Computing Innovations and Applications*, *2*(1), 1-11.
https://scholar.google.com/scholar?q=Risk+Assessment+Models+for+Protecting+Automated+Accounting+Systems+from+Cyber+Threats&hl=en&start=60&as_sdt=0,5&as_ylo=2021&as_yhi=2025
[59]. Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber threats to industrial IoT: a survey on attacks and countermeasures. *IoT*, *2*(1), 163-186.
https://www.mdpi.com/2624-831X/2/1/9
[60]. Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022). Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. *Energies*, *15*(18), 6799.
https://www.mdpi.com/1996-1073/15/18/6799
[61]. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.
https://www.mdpi.com/1424-8220/21/15/5119
[62]. Inaganti, A. C., Ravichandran, N., Nersu, S. R. K., & Muppalaneni, R. (2021). Cloud Security Posture Management (CSPM) with AI: Automating Compliance and Threat Detection. *Artificial Intelligence and Machine Learning Review*, *2*(4), 8-18.
https://scholar.google.com/scholar?start=70&q=Risk+Assessment+Models+for+Protecting+Automated+Accounting+Systems+from+Cyber+Threats&hl=en&as_sdt=0,5&as_ylo=2021&as_yhi=2025
[63]. Hossain, M. J., Rifat, R. H., Mugdho, M. H., Jahan, M., Rasel, A. A., & Rahman, M. A. (2022, November). Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh. In *2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)* (pp. 190-195). IEEE.
https://ieeexplore.ieee.org/abstract/document/10017467
[64]. Steimers, A., & Schneider, M. (2022). Sources of risk of AI systems. *International Journal of Environmental Research and Public Health*, *19*(6), 3641.
https://www.mdpi.com/1660-4601/19/6/3641
[65]. Dataset Link:
https://www.kaggle.com/datasets/ziya07/financial-transaction-and-risk-management-dataset