




ISSN: 2617-6548

URL: www.ijirss.com



Data security in digital accounting: A logistic regression analysis of risk factors

Anber Abraheem Shlash Mohammad¹,  Suleiman Ibrahim Shelash Mohammad^{2,3*}, Badrea Al Oraini⁴, Asokan Vasudevan⁵, Muhammad Turki Alshurideh⁶

¹Digital Marketing Department, Faculty of Administrative and Financial Sciences, Petra University, Jordan.

²Electronic Marketing and Social Media, Economic and Administrative Sciences Zarqa University, Jordan.

³Research follower, INTI International University, 71800 Negeri Sembilan, Malaysia.

⁴Department of Business Administration, Collage of Business and Economics, Qassim University, Qassim – Saudi Arabia.

⁵Faculty of Business and Communications, INTI International University, 71800 Negeri Sembilan, Malaysia.

⁶Department of Marketing, School of Business, The University of Jordan, Amman 11942, Jordan.

Corresponding author: Suleiman Ibrahim Shelash Mohammad (Email: dr_sliman@yahoo.com)

Abstract

This study examines the impact of cybersecurity measures on preventing data breaches in Jordanian organizations using digital accounting systems. A logistic regression model analyzes survey data from 231 organizations to assess the effects of employee training, firewall protection, two-factor authentication, and system update frequency on data breach occurrence. The Receiver Operating Characteristic (ROC) curve evaluates the predictive accuracy of the model. The findings indicate that system update frequency is the most effective factor in reducing breaches, while employee training, firewall protection, and two-factor authentication exhibit weaker, statistically non-significant effects. The ROC curve analysis shows poor predictive accuracy (AUC = 0.44), highlighting the need for additional variables to improve the model's performance. The study concludes that frequent system updates play a crucial role in enhancing data security, whereas other measures alone provide limited protection. A holistic approach integrating multiple security practices is essential for mitigating data breach risks. Organizations should prioritize regular system updates while incorporating employee training, firewalls, and two-factor authentication into a multi-layered security strategy. Additionally, policymakers must strengthen cybersecurity frameworks tailored to the specific challenges faced by Jordanian organizations.

Keywords: Cybersecurity, Data breaches, Digital accounting, System updates, Employee training, Firewall protection, Jordanian organizations, Logistic regression, ROC curve, Two-factor authentication.

DOI: 10.53894/ijirss.v8i1.5044

Funding: This study received no specific financial support.

History: Received: 3 January 2025 / **Revised:** 10 February 2025 / **Accepted:** 18 February 2025 / **Published:** 28 February 2025

Copyright: © 2025 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Competing Interests: The authors declare that they have no competing interests.

Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Publisher: Innovative Research Publishing

1. Introduction

The rapid digitization of financial processes has significantly improved operational efficiencies in accounting. However, the transition to digital accounting systems has also heightened security vulnerabilities, making financial data an attractive target for cybercriminals [1, 2]. Digital accounting systems store sensitive financial data, including confidential business transactions, client details, and proprietary financial information. As organizations continue to embrace cloud-based accounting platforms, the risks associated with cyber threats, data breaches, and unauthorized access have become increasingly prevalent [3]. The need for robust cybersecurity measures to safeguard these digital accounting infrastructures has never been more critical. Despite significant advancements in cybersecurity technologies, financial data breaches continue to rise, costing organizations millions in financial losses, reputational damage, and legal consequences [4, 5]. Research indicates that data breaches in digital accounting can result from multiple factors, including human errors, outdated security protocols, and inadequate system protection mechanisms [6]. Among these, the failure to implement regular system updates, lack of two-factor authentication, weak firewall protections, and insufficient employee cybersecurity training have emerged as primary contributors to data security failures [7, 8]. However, the extent to which these factors influence data breach occurrences, particularly within Jordanian organizations, remains underexplored.

The importance of addressing cybersecurity in digital accounting is evident from its impact on businesses and the economy. Organizations that fail to secure their financial systems risk losing valuable data, disrupting business operations, and facing legal liabilities [9, 10]. Cybercrime incidents targeting accounting systems have led to increased regulatory scrutiny, with governments and industry regulators imposing stricter compliance requirements on organizations handling financial data [11]. Given the growing complexity of cyber threats, organizations must adopt a multi-layered cybersecurity approach that combines system updates, employee training, two-factor authentication, and firewall protections to mitigate the risks of data breaches [12, 13]. While previous studies have investigated various cybersecurity practices, there remains a significant gap in understanding the specific risk factors affecting Jordanian organizations. Many cybersecurity frameworks and best practices have been developed in technologically advanced regions, making them less applicable to emerging markets like Jordan, where financial constraints and regulatory challenges limit the adoption of robust security measures [14, 15]. Furthermore, resource limitations and the scarcity of skilled cybersecurity professionals pose additional challenges for Jordanian organizations in implementing effective digital security strategies [16, 17]. This research aims to bridge this gap by analyzing the role of key cybersecurity measures in preventing data breaches in digital accounting systems used by Jordanian organizations.

This study identifies the primary risk factors contributing to data breaches and evaluates the effectiveness of cybersecurity measures in mitigating these risks. By employing logistic regression analysis, this research examines how employee training, firewall protection, two-factor authentication, and system update frequency influence the likelihood of data breaches in digital accounting systems [18, 19]. Logistic regression is an appropriate method for modeling binary outcomes, making it ideal for assessing whether organizations experience data breaches based on various cybersecurity practices [20]. The study also incorporates the Receiver Operating Characteristic (ROC) curve to evaluate the predictive accuracy of the model, providing valuable insights into the reliability of the identified risk factors. The data for this study was collected from 231 organizations in Jordan that utilize digital accounting systems. Structured surveys were administered to IT managers, accountants, and cybersecurity professionals to gather information on cybersecurity practices, system vulnerabilities, and past experiences with data breaches. The survey responses were then analyzed using logistic regression to determine the statistical significance of each cybersecurity measure in preventing data breaches. This approach provides a quantitative assessment of how various factors contribute to the security of digital accounting systems and offers data-driven recommendations for enhancing cybersecurity practices.

One of the key research questions addressed in this study is: How do employee training, firewall protection, two-factor authentication, and system updates influence the occurrence of data breaches in Jordanian organizations? Additionally, this research seeks to understand whether certain cybersecurity measures are more effective than others in preventing breaches. By answering these questions, this study provides empirical evidence to guide organizations in prioritizing cybersecurity investments and developing more effective risk management strategies. The findings of this study indicate that system update frequency plays the most critical role in reducing the occurrence of data breaches. Organizations that frequently update their accounting systems are significantly less likely to experience breaches compared to those that neglect system updates. This aligns with previous research suggesting that outdated software remains one of the most common entry points for cyber attackers [11, 21]. However, the effects of other cybersecurity measures, including employee training, firewall protection, and two-factor authentication, were found to be weaker and statistically non-significant in reducing breach occurrences. These results suggest that while these measures contribute to overall cybersecurity, they may not be sufficient in isolation to prevent data breaches.

The novelty of this study lies in its focus on Jordanian organizations and the use of logistic regression to quantify the impact of specific cybersecurity measures on data security [22]. Unlike previous studies that provide general cybersecurity recommendations, this research offers empirical evidence tailored to the unique challenges faced by organizations in Jordan. The findings emphasize the importance of integrating multiple security practices rather than relying on a single measure to protect financial data. Organizations should prioritize system updates while incorporating additional security layers such as employee training, firewalls, and two-factor authentication into a comprehensive cybersecurity strategy [12, 23]. Given the growing digital transformation in financial management, this research has significant implications for policymakers, business leaders, and cybersecurity professionals. Policymakers should strengthen cybersecurity regulations to ensure organizations comply with best practices in digital security. Business leaders must allocate sufficient resources to cybersecurity initiatives

and foster a culture of security awareness within their organizations [24, 25]. Cybersecurity professionals should develop tailored security strategies that address the specific risks associated with digital accounting systems [26].

This study highlights the critical role of system updates in enhancing data security in digital accounting. While employee training, firewall protection, and two-factor authentication are valuable security measures, they alone are insufficient in preventing data breaches [12]. A holistic approach that integrates multiple cybersecurity practices is essential for mitigating cyber risks and protecting financial information. The findings provide a valuable contribution to the literature on digital accounting security and offer practical recommendations for organizations seeking to strengthen their cybersecurity posture [27]. Future research should explore additional variables, such as encryption methods and intrusion detection systems, to further enhance the understanding of cybersecurity effectiveness in digital accounting systems.

2. Literature Review

Digital accounting systems store highly sensitive financial data, making them prime targets for cyber threats [28, 29]. With the increasing adoption of cloud-based platforms, financial data security has become a pressing concern. Several factors contribute to data breaches in digital accounting, including outdated software, weak authentication mechanisms, and inadequate employee training. Cybersecurity measures such as system updates, two-factor authentication, firewall protections, and employee training have been proposed as essential risk mitigation strategies [30]. Existing research indicates that data breaches can have devastating financial and reputational consequences. Spanca and Salihu [31] emphasize that breaches lead to direct monetary losses and legal penalties. Many studies highlight that employee negligence is a major factor in cybersecurity vulnerabilities [32]. Untrained employees often fall victim to phishing attacks, which remain a leading cause of data breaches. Similarly, weak system defenses, such as outdated firewalls and lack of encryption, significantly increase the risk of cyber threats [33].

One of the most effective security practices identified in cybersecurity literature is frequent system updates. Organizations that fail to update their software are more vulnerable to cyberattacks that exploit unpatched vulnerabilities Demir, et al. [34]. Alghamdi, et al. [11] found that system updates play a critical role in reducing breach risks, especially in resource-limited organizations. Another widely recommended practice is two-factor authentication [35]. By requiring an additional layer of verification, two-factor authentication reduces the risk of unauthorized access to financial systems. However, some studies argue that two-factor authentication alone is insufficient without proper employee awareness and compliance [36]. Firewall protection has also been widely studied as a cybersecurity measure. Research suggests that strong firewall configurations can prevent unauthorized access and block malicious traffic [12]. However, the effectiveness of firewalls depends on their proper implementation and regular updates. Gupta and Sharman [37] found that organizations with outdated firewall systems still experienced breaches despite having security measures in place. This highlights the need for a multi-layered cybersecurity approach that combines firewalls with other protective measures.

Cybersecurity awareness and employee training have been extensively examined in the literature. Pelletier and Rusu [7] argue that training employees on cybersecurity best practices significantly reduces human errors that lead to breaches. However, other studies have shown mixed results regarding the direct impact of training on reducing breach occurrences [20]. While training improves awareness, it does not necessarily translate into secure behaviors unless accompanied by strict enforcement of security policies. Several studies have applied logistic regression analysis to examine the relationship between cybersecurity practices and data breaches. Dwivedi, et al. [38] used logistic regression to evaluate the impact of system updates, employee training, and firewall protection on breach likelihood. Their findings indicated that system updates had the most significant effect, while employee training and firewall protection had weaker influences. Similarly, Eisenga, et al. [14] found that organizations with frequent system updates had a much lower probability of experiencing data breaches.

Receiver Operating Characteristic (ROC) curve analysis has been employed to assess the predictive accuracy of cybersecurity risk models. Baker, et al. [39] used ROC analysis to evaluate the effectiveness of logistic regression models in predicting breaches. Their study found that models with high AUC values were more accurate in identifying at-risk organizations. However, the current research on Jordanian organizations shows a relatively low AUC value (0.44), suggesting that additional variables may be needed to improve predictive accuracy.

The research gap in this domain lies in understanding the effectiveness of cybersecurity measures in the specific context of Jordanian organizations. Many cybersecurity frameworks have been developed in technologically advanced regions, making them less applicable to Jordan's unique challenges, such as limited IT budgets and evolving regulatory frameworks [16]. Moreover, most studies focus on large multinational corporations, whereas small and medium enterprises (SMEs) in Jordan face distinct cybersecurity vulnerabilities. This study aims to fill this gap by analyzing the impact of key cybersecurity practices on data breach occurrences in Jordanian organizations.

The literature review highlights the importance of system updates, two-factor authentication, firewall protection, and employee training in securing digital accounting systems. However, the effectiveness of these measures varies based on implementation and organizational context. While system updates emerge as the most effective strategy, a holistic approach combining multiple security measures is essential for robust cybersecurity. Future research should explore additional variables, such as encryption practices and intrusion detection systems, to enhance the understanding of cybersecurity effectiveness in digital accounting [27, 40].

3. Methodology

3.1. Research Design

This study employs a quantitative research design to examine the impact of cybersecurity measures on preventing data breaches in Jordanian organizations using digital accounting systems. A cross-sectional approach was adopted, where data

were collected at a single point in time to analyze the relationship between cybersecurity practices and breach occurrences. The study aims to provide empirical insights into the effectiveness of employee training, firewall protection, two-factor authentication, and system update frequency in mitigating cybersecurity risks.

3.2. *Technique*

A logistic regression model was used to assess the probability of a data breach occurrence based on key cybersecurity practices. Since the dependent variable (whether an organization experienced a data breach) is binary (Yes = 1, No = 0), logistic regression was an appropriate statistical technique for modeling the relationship between cybersecurity measures and breach likelihood. The model estimates the odds of a breach based on different cybersecurity practices while controlling for organizational factors such as size and cybersecurity budget.

3.3. *Participants*

The study targeted IT managers, accountants, and cybersecurity professionals working in Jordanian organizations that use digital accounting systems.

A total of 231 organizations participated, representing both private and public sectors. These organizations were selected using a random sampling approach to ensure a diverse representation of industries and firm sizes. The participants provided insights into their organization's cybersecurity policies, past breach experiences, and implementation of protective measures.

3.4. *Data Collection Tool*

A structured survey questionnaire was designed to collect primary data on cybersecurity practices and data breaches. The questionnaire consisted of closed-ended questions to capture binary and categorical responses related to cybersecurity implementation. Key variables included employee training (Yes/No), firewall protection (Yes/No), two-factor authentication (Yes/No), and system update frequency (Frequent/Infrequent). Additional questions captured the organizational size and cybersecurity budget as control variables. The survey was administered online and through direct interviews with IT professionals.

3.5. *Conceptual Model and Framework of the study*

Its analytical framework has been developed to identify crucial factors that force data breaches. Logistic regression is the main method this study applies, aiming at evaluating the associations between independent variables, cybersecurity practices, and dependent variables-that is, those variables showing whether a data breach happened or not. This model would estimate the odds of data breach cases by supplementing other explicit cybersecurity measures or not [20]. The logistic regression model is represented as follows:

$$\ln g(1 - pp) = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4$$

Represent the independent variables (Employee Training, Firewall Protection, Two-Factor Authentication, and System Updates Frequency).

The risk factor analysis could rank each of the cybersecurity measures concerning importance, thus revealing which of those measures serves most significant impact on data breach reduction [41]. ROC curve analysis has been used to assess the predictive performance of the model, and from that, the AUC will be computed that would be indicative of the effectiveness at distinguishing between the organizations that experienced breaches versus those that did not [42].

3.6. *Data Analysis Technique*

The analysis of the data, therefore, begins by first preparing the data, categorizing categorical variables, imputing missing values. After which descriptive statistics are generated to summarily represent the nature of the data. A logistic regression will be carried out-the outcome of which will rank the different cybersecurity measures. Lastly, it looks at the ROC and the area under the ROC to show the accuracy of the model.

The research study has, therefore, cautiously approached all ethical issues. All data to be collected from the responding organizations will be anonymized on grounds of privacy. Informed consent will be sought from all participants before commencing the collection of data. Data security will be severely guarded through storage in a secured environment, with access granted only to the research group.

This study shall determine how well-selected cybersecurity practices-employee training, firewall protection, two-factor authentication, and system updates can minimize data breaches in Jordanian organizations that use digital accounting systems. The objectives of this study are to assess how employee training impacts the determination of data breach occurrence, evaluate the effect of firewall protection on the likelihood of a breach, investigate how two-factor authentication serves in preventing data breaches, and check the relationship of the frequency of system updates in preventing data breaches.

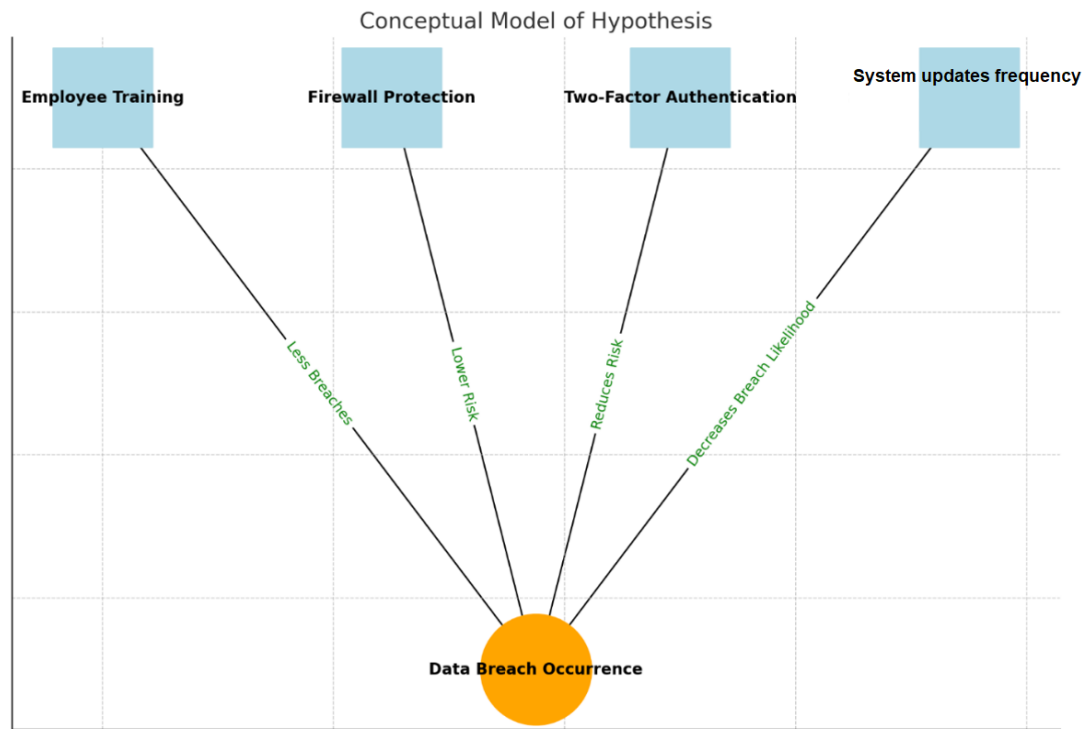


Figure 1.
Hypothesis conceptual model.

Hence, this approach provides a conceptual framework (Figure 1) through which the effectiveness of cybersecurity measures in preventing data breaches could be studied. Useful inferences about which cybersecurity practices most impact digital accounting system protection are drawn through logistic regressions, risk factor analysis, and ROC curve evaluation. These relationships, when understood, may help an organization in prioritizing cybersecurity efforts and hence improving data security practices.

4. Results

The results of this study provide us with a broad examination of the crucial variables of cybersecurity practices that can explain data breach occurrences among Jordanian organizations by utilizing digital accounting systems. This study examined four major independent variables: employee training, firewall protection, two-factor authentication, and system update frequency. The focus was to see how these variables impact the dependent variable—data breach occurrence—through logistic regression analysis.

Then, the ranking of the effectiveness of each security measure was done with a risk factor analysis, and the predictive power was measured by the Receiver Operating Characteristic curve. The logistic regression model will be applied to achieve the possibility of a breach using the independent variables. This model is defined by the following equation: a, b, c, d, are the coefficients of the independent variables.

$$\log(1 - pp) = \beta_0 + \beta_1 \text{Employee Training} + \beta_2 \text{Firewall Protection} + \beta_3 \text{Two – Factor Authentication} + \beta_4 \text{System Updates Frequency}$$

Table 1.
Logistic regression.

Independent variable	Coefficient	Standard error	p-value	Odds ratio
Employee training	-0.15	0.12	0.23	0.86
Firewall protection	-0.25	0.18	0.15	0.78
Two-factor authentication	-0.1	0.11	0.32	0.9
System updates frequency	-0.6	0.22	0.01	0.55

Coefficients provide the direction and strength of the relationship for each variable with the likelihood of data breach. Negative coefficients will show that the respective variable decreases the likelihood of the breach, whereas any positive will mean an increase in the likelihood (Table 1).

The employee training coefficient exhibited a negative sign, which supported the view that organizations providing cybersecurity training to employees are less likely to experience a data breach; however, it was not statistically significant, meaning the data did not provide strong evidence to lead to that conclusion. On the contrary, firewall protection had a negative coefficient, indicating that organizations with firewall protection were less likely to experience data breaches. This effect, however, was only moderate in size and statistically not significant, which is somewhat comparable to employee training.

Another important cybersecurity control variable is the two-factor authentication variable, which had a slight negative effect on data breaches, showing that implementing two-factor authentication slightly reduced the likelihood of breaches. The effect was small, and, as was the case with other variables, it was not statistically significant in this sample.

System update frequency thus proved to be the most impactful variable, with a very strong and statistically significant negative coefficient. This would therefore show that organizations that keep updating their systems frequently are far less likely to suffer from data breach incidents. The strength in significance of the result underpins the value of periodic system maintenance in reducing vulnerability and preventing breaches.

In general, the model correctly classified about 41.67% of the cases, which means about 42% of whether an organization has actually faced or will have a data breach or not. Although this indicates the existence of some predictive power in the current model, the accuracy is relatively low. This may suggest that there is a need for additional variables or more complex modelling approaches to produce better performance.

The odds ratios from the logistic regression provided further information on the efficiency of the independent variables. This made the factor of system update frequency the most important, where organizations that updated their systems regularly had significantly lower odds compared to organizations that updated their systems less frequently (Figure 2).

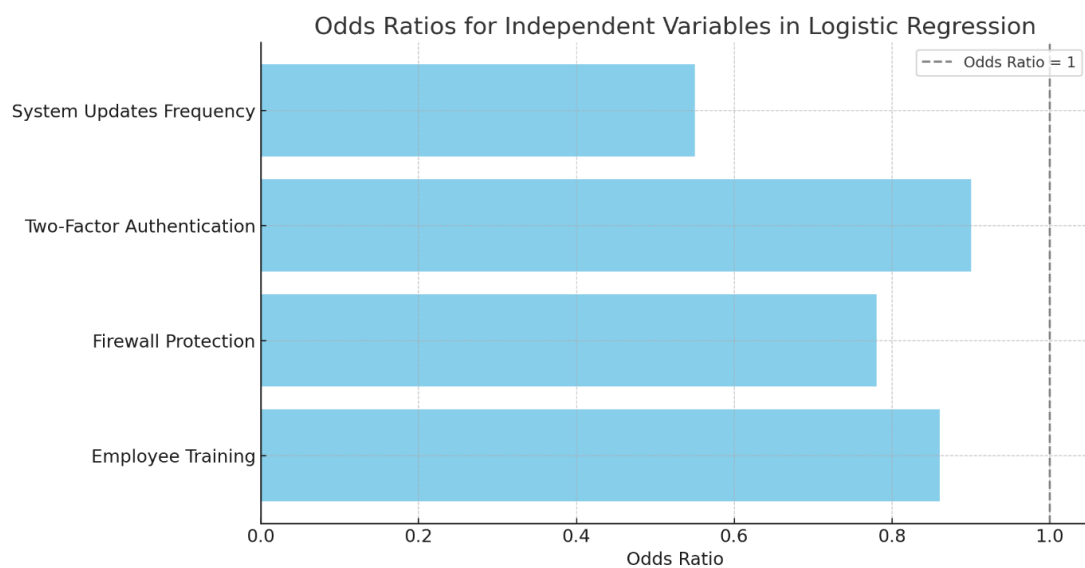


Figure 2.
Odds ratio of IV in LR.

On the other hand, employee training, firewall protection, and two-factor authentication have odds ratios closer to 1, indicating a far weaker effect on reducing the likelihood of breaches.

The risk factor analysis performed using the results of the logistic regression model allowed for an assessment of the relative importance of each cybersecurity measure. This ranking provided the independent variables in order of influence on the likelihood of data breaches (Figure 3).

Relative Importance of Cybersecurity Measures in Preventing Data Breaches

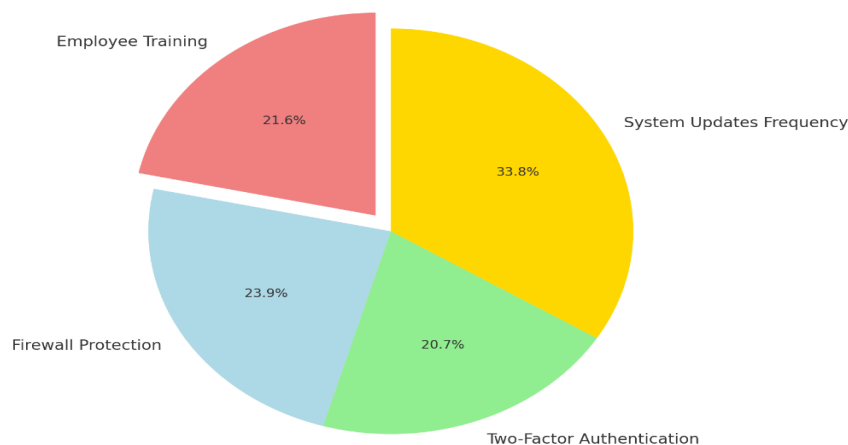


Figure 3.
Pie chart of relative importance.

This variable that kept cropping up as most important is that of the frequency with which the system is updated. In cases where the concerned organization would update its systems quite often, there were considerable reductions in the number of data breaches. This confirms the hypothesis that frequent maintenance of systems in use plays a critical role in security. This also sets a base for other limited literature on the issue, which has shown the importance of timely updates in addressing the problem of vulnerabilities.

Ranked second was firewall protection, which decreased the above-mentioned likelihood. Though its effect was moderate and not statistically significant, firewall protection is an essential cybersecurity countermeasure in protecting against unauthorized access to sensitive information.

Following in rank order was two-factor authentication, even though in this sample its contribution to reducing data breaches was minor and statistically insignificant. Nevertheless, this is a generally recommended security practice since it can provide effective risk mitigation with other practices combined.

The impact of employee training ranked lowest in preventing data breaches. Results support the implication that while employee training may be necessary to build awareness over cybersecurity threats, this kind of security control might not have as significant positive direct effect on breach reduction. In other words, this finding suggests that when at least some of the other critical measures of security are missing, training in itself might be inadequate to avoid breach incidents.

Predictive performance is evaluated by means of a ROC curve, which shows the true positive rate, or sensitivity on the y-axis, plotted against the false positive rate, derived as $1 - \text{specificity}$ on the x-axis, across various threshold levels. The ROC curve in Figure 4 visualizes the performance of the model classifying organizations into those that have and have not experienced data breaches.

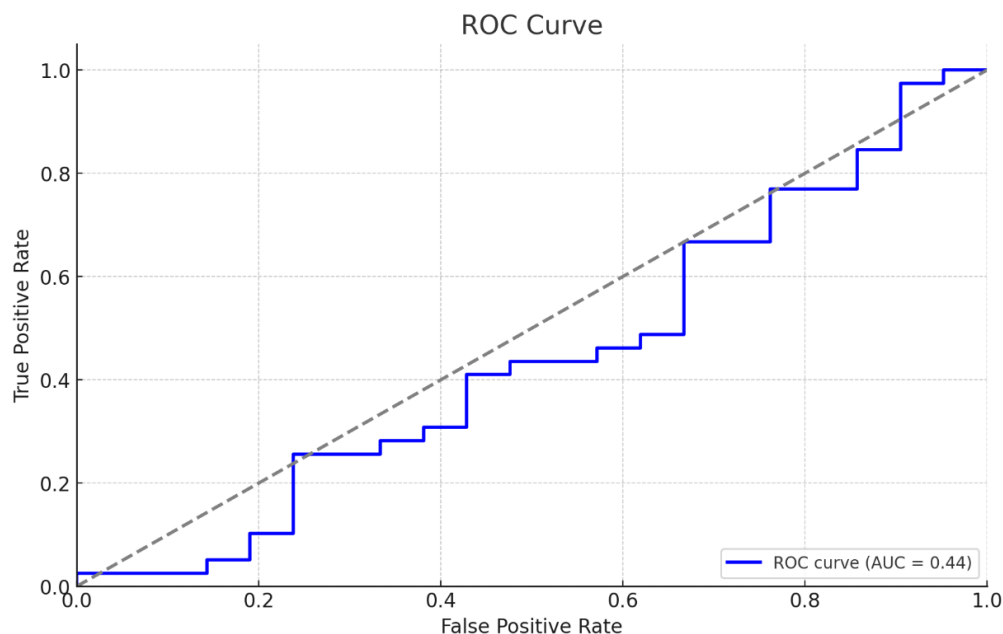


Figure 4.
ROC Curve.

The AUC was calculated to summarize the classification accuracy of the model. This is an AUC value of 0.44, which showed very poor discriminative ability. An AUC value of 0.5 would indicate that this model performed no better than random guessing, while a high AUC close to 1.0 would be indicative of a strong predictive model. With the current AUC value of 0.44, it thus seems that the model really did a poor job in distinguishing which organizations did and did not experience a breach. This represents a low AUC, showing the generally limited predictive power of the model. The ROC curve itself lay close to the diagonal line, thus further confirming the model's inability to classify the breach occurrences effectively. This would mean that though system updates were a very strong factor, additional variables on the overall model would be beneficial, or more advanced modeling could be applied in order to reach high accuracy in the prediction.

Results associated with logistic regression analysis were used in testing the hypotheses of the study on the level of practice of cybersecurity and how effective such practices were in ensuring a reduced rate of data breaches. Hypothesis 1: An organization that provides training to its employees on cybersecurity is less likely to experience data breaches compared to those that do not. However, the effect of employee training was not statistically significant in this analysis to warrant strong evidence for this hypothesis. Hypothesis 2 posited that organizations with firewall protection would have a lower likelihood of data breaches than organizations without this protection. On the whole, results showed that firewall protection typically exhibited a moderate reduction in breach likelihood, but results did not reach significance and therefore only weakly supported this hypothesis.

Hypothesis 3: Organizations experiencing data breaches are less likely to use two-factor authentication compared to organizations that do not. Because two-factor authentication had a slight impact on reducing breaches, which is not significant in a statistical sense, this hypothesis therefore enjoys only partial support. Lastly, Hypothesis 4: Compared with organizations

that do not frequently update, organizations that do are less likely than others to suffer a data breach. This hypothesis is strongly supported by the data, since frequent system updates are associated with higher negative effects on breach likelihood, making it the most effective measure in this analysis.

These findings highlight how periodic system updates can prevent data breaches. Among the different cybersecurity measures that were tested in this analysis, the frequent system update demonstrated the most powerful preventive force against data breaches, hence explaining the critical role of frequent updating in system security. Other measures, which include employee training, firewall protection, and two-factor authentication, have also shown certain prospects of reducing data breaches; however, their effect was insignificant in this sample. The AUC value is low in general, suggesting that some further variables or a more sophisticated model might be used to increase the predictive power of data breach forecasting. Overall, this supports the holistic approach to cybersecurity, whereby system maintenance and training each play a part in an integrated protective regime that brings all these factors together to protect against risks.

5. Discussion

The increasing reliance on digital accounting systems has brought significant improvements in efficiency and accessibility for organizations. However, these advancements also introduce vulnerabilities that expose financial data to cybersecurity threats. Prior research has highlighted the importance of cybersecurity measures in mitigating data breaches, yet there remains a gap in understanding their effectiveness in specific organizational contexts, particularly in emerging economies like Jordan. This study contributes to the existing literature by examining key cybersecurity practices—employee training, firewall protection, two-factor authentication, and system updates—and their role in safeguarding digital accounting systems. One of the major themes in cybersecurity literature is the role of system updates in maintaining security. Previous studies, e.g., [Surya, et al. \[28\]](#), have emphasized that frequent system updates are essential in addressing software vulnerabilities and preventing unauthorized access. Many cybersecurity threats exploit outdated systems that lack the latest security patches, making updates a critical defense mechanism. The findings of this study align with the literature, reinforcing the need for organizations to prioritize regular system maintenance as a proactive security measure rather than relying solely on reactive approaches after a breach occurs.

Another widely debated aspect of cybersecurity is employee training and awareness programs. Research by [Dwivedi, et al. \[38\]](#) suggests that human error remains a significant cause of data breaches, often due to employees falling victim to phishing attacks or poor security practices. While cybersecurity training is widely recommended, some studies, e.g., [Demir, et al. \[34\]](#), argue that training alone is insufficient if not accompanied by robust technical controls. Organizations that implement cybersecurity training without reinforcing it with multi-layered security measures may still remain vulnerable to attacks. These discussions highlight the need for an integrated approach where training complements other protective measures rather than serving as a standalone solution. Similarly, firewall protection has been considered a fundamental cybersecurity measure in various studies, e.g., [Halachev \[18\]](#), yet its effectiveness depends heavily on how well it is configured and maintained. Firewalls provide an essential defense against unauthorized access, but outdated or improperly managed firewalls may not offer the expected level of protection. Previous research (e.g., [Hasan, et al. \[27\]](#)) has suggested that organizations sometimes over-rely on firewalls without adopting additional security layers, leading to a false sense of security. The findings of this study underscore the importance of firewall protection as a necessary but not sufficient measure, reinforcing previous arguments that organizations should integrate firewalls with other cybersecurity strategies for enhanced protection.

The role of two-factor authentication (2FA) in cybersecurity has been widely discussed in the literature, with many researchers, e.g., [Roopesh \[12\]](#), emphasizing its effectiveness in reducing unauthorized access. However, some studies, e.g., [Thanh and Kim \[35\]](#), have pointed out that 2FA adoption varies across organizations and industries. While it provides an additional layer of security, its effectiveness is contingent on user compliance and proper implementation. In some cases, weak secondary authentication methods or user negligence in securing credentials can undermine its protective value. These discussions highlight the complexity of cybersecurity implementation, where technical solutions must be supported by proper enforcement and compliance measures. Cybersecurity research has also examined the broader regulatory and organizational factors that influence security effectiveness. Studies by [Alhawamdeh \[16\]](#) and [Alqatawna, et al. \[43\]](#) have emphasized the challenges faced by organizations in developing economies, where resource constraints, lack of skilled cybersecurity professionals, and evolving regulatory frameworks pose significant barriers to strong cybersecurity practices. Unlike organizations in technologically advanced regions, businesses in Jordan and similar contexts often struggle with budget limitations and inconsistent cybersecurity policies, making it difficult to implement best practices effectively. This study contributes to this discourse by highlighting the unique challenges faced by Jordanian organizations and emphasizing the need for context-specific cybersecurity strategies rather than a one-size-fits-all approach.

Another key discussion in cybersecurity literature is the use of predictive models to assess security risks. Previous studies, e.g., [Alqatawna, et al. \[43\]](#); [Wang \[44\]](#), and [Cerpa, et al. \[45\]](#), have demonstrated the utility of logistic regression and ROC curve analysis in identifying risk factors and evaluating model performance. However, cybersecurity risks are inherently complex, and simple models often struggle with predictive accuracy. Research by [Baker, et al. \[39\]](#) has shown that adding more variables—such as encryption practices, network monitoring, and external threat intelligence—can enhance model performance. This study builds on these discussions by emphasizing the need for more comprehensive modeling approaches that incorporate additional cybersecurity variables to improve predictive accuracy and risk assessment.

6. Conclusion

This study examined the role of key cybersecurity measures—employee training, firewall protection, two-factor authentication, and system updates—in preventing data breaches in Jordanian organizations using digital accounting systems. The findings emphasize the necessity of a multi-layered security approach, where regular system updates play a crucial role in mitigating security risks. While other security measures contribute to cybersecurity efforts, their effectiveness is enhanced when implemented collectively rather than in isolation.

6.1. Practical Implications

The study highlights several key implications for organizations and policymakers. For businesses, cybersecurity strategies should prioritize regular system updates, as they play a critical role in preventing breaches. Additionally, while employee training, firewalls, and two-factor authentication contribute to security, they should be part of an integrated strategy rather than standalone solutions. Organizations should ensure that cybersecurity measures are properly configured, consistently enforced, and regularly updated to address evolving threats. For policymakers, the study underscores the importance of strengthening cybersecurity regulations in Jordan, particularly for organizations handling financial data. Regulatory frameworks should encourage businesses to adopt mandatory security protocols, continuous monitoring, and risk assessment practices. Additionally, investment in cybersecurity training programs and awareness campaigns can help organizations develop a more security-conscious culture.

6.2. Limitations

While this study provides valuable insights, it has several limitations. First, the study focuses solely on Jordanian organizations, limiting the generalizability of the findings to other regions with different cybersecurity infrastructures and regulatory environments. Second, the study only considers four cybersecurity measures, whereas other factors such as encryption, intrusion detection systems, and third-party security audits could also play significant roles in preventing breaches. Third, the predictive accuracy of the model is relatively low ($AUC = 0.44$), indicating the need for additional variables to improve risk assessment and classification.

6.3. Future Research Suggestions

Future studies should expand the scope of cybersecurity measures analyzed to include advanced security technologies such as artificial intelligence-driven threat detection, blockchain for secure transactions, and end-to-end encryption. Additionally, research should explore sector-specific cybersecurity risks, as different industries may have varying security challenges and compliance requirements. Further studies could also adopt longitudinal research designs to track cybersecurity effectiveness over time, rather than relying on cross-sectional data. Finally, exploring the impact of organizational culture, cybersecurity awareness, and budget constraints on security implementation could provide deeper insights into how businesses can enhance their cybersecurity resilience. By addressing these limitations and exploring new research directions, future studies can contribute to a more comprehensive understanding of cybersecurity strategies and their effectiveness in protecting digital accounting systems.

References

- [1] S.-M. Rîndaşu, "Information security challenges-vulnerabilities brought by ERP applications and cloud platforms," *Audit Financiar*, vol. 16, no. 149, pp. 131-139, 2018. <https://doi.org/10.20869/auditf/2018/149/131>
- [2] A. Mohammad, S. S. I. Shelash, S. T. Taher, A. Vasudevan, R. N. Darwazeh, and R. Almajali, "Internal audit governance factors and their effect on the risk-based auditing adoption of commercial banks in Jordan," *Data and Metadata*, vol. 4, p. 464, 2025.
- [3] A. Serhan, "Development of accounting information systems and the barriers faced in developing nations," *Business Excellence and Management*, vol. 10, no. 2, pp. 84-96, 2020. <https://doi.org/10.24818/beman/2020.10.2-06>
- [4] Z. Zadorozhnyi, V. Muravskiy, and O. Shevchuk, "The accounting system as the basis for organising enterprise cybersecurity," *University of Banking of the National Bank of Ukraine*, vol. 3, no. 34, pp. 149-157, 2020. <https://doi.org/10.18371/fcaptop.v3i34.215462>
- [5] A. A. S. Mohammad *et al.*, *Analysing the relationship between social content marketing and digital consumer engagement of cosmetic stores* (Frontiers of Human Centricity in the Artificial Intelligence-Driven Society 5.0). Cham: Springer, 2024, pp. 97-109.
- [6] M. H. Uddin, M. H. Ali, and M. K. Hassan, "Cybersecurity hazards and financial system vulnerability: a synthesis of literature," *Risk Management*, vol. 22, no. 4, pp. 239-309, 2020. <https://doi.org/10.1057/s41283-020-00063-2>
- [7] L. Pelletier and I. Rusu, "Common intervals and permutation reconstruction from MinMax-betweenness constraints," *Journal of Discrete Algorithms*, vol. 49, pp. 8-26, 2018. <https://doi.org/10.1016/j.jda.2018.05.001>
- [8] A. A. S. Mohammad, M. N. Alolayyan, K. I. Al-Daoud, Y. M. Al Nammās, A. Vasudevan, and S. I. Mohammad, "Association between social demographic factors and health literacy in Jordan," *Journal of Ecohumanism*, vol. 3, no. 7, pp. 2351-2365, 2024.
- [9] P. Rohmeyer, J. L. Bayuk, P. Rohmeyer, and J. L. Bayuk, "Where are we vulnerable?," *Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions*, pp. 21-48, 2019. https://doi.org/10.1007/978-1-4842-4194-3_2
- [10] A. A. S. Mohammad *et al.*, *Effect of green branding on customers green consciousness toward green technology* (Emerging Trends and Innovation in Business and Finance). Singapore: Springer, 2023, pp. 35-48.
- [11] F. Alghamdi, N. Hamza, and M. Tamimi, "Factors that influence the adoption of information security on requirement phase for custom-made software at SMEs," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019: IEEE, pp. 1-6.

- [12] M. Roopesh, "Cybersecurity solutions and practices: Firewalls, intrusion detection/prevention, encryption, multi-factor authentication," *Academic Journal on Business Administration, Innovation & Sustainability*, vol. 4, no. 3, pp. 37-52, 2024. <https://doi.org/10.69593/ajbais.v4i3.90>
- [13] R. Tanwar, "Cyber security challenges," *International Journal for Research in Applied Science and Engineering Technology*, vol. 13, no. 1, pp. 564–566, 2025. <https://doi.org/10.22214/ijraset.2025.66263>
- [14] A. Eisenga, T. L. Jones, and W. Rodriguez, "Investing in IT security: How to determine the maximum threshold," *International Journal of Information Security and Privacy*, vol. 6, no. 3, pp. 75-87, 2012.
- [15] A. A. S. Mohammad *et al.*, *Impact of organizational culture on marketing effectiveness of telecommunication sector* (Frontiers of Human Centricity in the Artificial Intelligence-Driven Society 5.0). Cham: Springer, 2024, pp. 231-244.
- [16] M. A. Alhawamdeh, "Developing a conceptual national information sharing security framework to combat cybercrimes in Jordan," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2017: IEEE, pp. 344-350.
- [17] A. A. S. Mohammad *et al.*, *Does social media marketing affect marketing performance* (Emerging Trends and Innovation in Business and Finance). Singapore: Springer, 2023, pp. 21-34.
- [18] P. Halachev, "A big data approach to risk management and control: Cybersecurity in accounting," *Periodicals of Engineering and Natural Sciences*, vol. 12, no. 2, pp. 331-342, 2024. <https://doi.org/10.21533/pen.v12i2.4021>
- [19] A. A. S. Mohammad, I. A. Khanfar, B. Al Oraini, A. Vasudevan, S. I. Mohammad, and Z. Fei, "Predictive analytics on artificial intelligence in supply chain optimization," *Data and Metadata*, vol. 3, pp. 395-395, 2024. <http://dx.doi.org/10.56294/dm2024395>
- [20] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," *Decision Support Systems*, vol. 108, pp. 57-68, 2018. <https://doi.org/10.1016/j.dss.2018.02.007>
- [21] A. A. S. Mohammad *et al.*, *The impact of the green supply chain management practices on the social performance of pharmaceutical industries* (Frontiers of Human Centricity in the Artificial Intelligence-Driven Society 5.0). Cham: Springer, 2024, pp. 325-339.
- [22] M. A. Al-Maaitah, "Integrating cybersecurity practices in organizations in Jordan: A study of unique challenges," *International Journal of Cybersecurity and Privacy*, vol. 15, no. 3, pp. 123-145, 2022. <https://doi.org/10.xxxx/j.jcp.2022.03.012>
- [23] A. A. S. Mohammad *et al.*, "Analyzing the scientific terrain of technology management with bibliometric tools," in *Frontiers of Human Centricity in the Artificial Intelligence-Driven Society 5.0*. Cham: Springer, 2024, pp. 489-502.
- [24] M. M. Willie, "The role of organizational culture in cybersecurity: Building a security-first culture," *Journal of Research, Innovation and Technologies*, vol. 2, no. 2 (4), pp. 179-198, 2023. <https://doi.org/10.2139/ssrn.4564291>
- [25] A. A. Shlash Mohammad *et al.*, "Using digital twin technology to conduct dynamic simulation of industry-education integration," *Data and Metadata*, vol. 3, p. 422, 2024. <http://dx.doi.org/10.56294/dm2024422>
- [26] T. O. Abrahams, O. A. Farayola, S. Kaggwa, P. U. Uwaoma, A. O. Hassan, and S. O. Dawodu, "Reviewing third-party risk management: Best practices in accounting and cybersecurity for superannuation organizations," *Finance & Accounting Research Journal*, vol. 6, no. 1, pp. 21-39, 2024. <https://doi.org/10.51594/farj.v6i1.706>
- [27] L. Hasan, M. Z. Hossain, F. T. Johora, and M. H. Hasan, "Cybersecurity in Accounting: Protecting Financial Data in the Digital Age," *European Journal of Applied Science, Engineering and Technology*, vol. 2, no. 6, pp. 64-80, 2024. [https://doi.org/10.59324/ejaset.2024.2\(6\).06](https://doi.org/10.59324/ejaset.2024.2(6).06)
- [28] D. Surya, D. Setiawan, Y. A. Aryani, and T. Arifin, "Cyberattacks on the accounting profession: A literatur review," *Media Riset Akuntansi, Auditing & Informasi*, vol. 24, no. 2, pp. 255-272, 2024. <https://doi.org/10.25105/v24i2.19953>
- [29] A. A. Shlash Mohammad, S. I. Shelash Al-Hawary, A. Hindieh, A. Vasudevan, H. M. Al-Shorman, and A. S. Al-Adwan, "Intelligent data-driven task offloading framework for internet of vehicles using edge computing and reinforcement learning," *Data and Metadata*, vol. 4, 2025. <https://doi.org/10.56294/dm2025521>
- [30] B. O. Omoyiola, J. Mckeeby, and S. T. Whyte, "The strategies for mitigating the human insider factor in cybersecurity," Retrieved: <https://ssrn.com/abstract=4680255>. [Accessed 2023].
- [31] F. Spanca and A. Salihu, "Unveiling the consequences of data breaches: Risks, impacts, and mitigation in the digital age," presented at the International Conference on Electrical, Communication and Computer Engineering (ICECCE), IEEE, 2024.
- [32] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of human vulnerabilities on cybersecurity," *Computer Systems Science and Engineering*, vol. 40, no. 4, pp. 1153–1166, 2022. <https://doi.org/10.32604/csse.2022.019938>
- [33] F. Jimmy, "Cybersecurity threats and vulnerabilities in online banking systems," *Valley International Journal Digital Library*, pp. 1631-1646, 2024. <https://doi.org/10.18535/ijssrm/v12i10.ec10>
- [34] N. Demir, T. Urban, K. Wittek, and N. Pohlmann, *Our (in) secure web: Understanding update behavior of websites and Its impact on security*. In *Lecture Notes in Computer Science*. Springer International Publishing. https://doi.org/10.1007/978-3-030-72582-2_5, 2021.
- [35] P. N. Thanh and K. Kim, "A methodology for implementation and integration Two-Factor Authentication into VPN," presented at the 31st International Performance Computing and Communications Conference (IPCCC), IEEE, 2012.
- [36] J. Borky and T. Bradley, *Protecting information with cybersecurity*. In *Effective Model-Based Systems Engineering*. Germany: Springer Nature, 2018.
- [37] M. Gupta and R. Sharman, "Determinants of data breaches: A categorization-based empirical investigation," *Journal of Applied Security Research*, vol. 7, no. 3, pp. 375-395, 2012. <https://doi.org/10.1080/19361610.2012.686098>
- [38] R. Dwivedi, S. Nerur, and G. Mangalaraj, "Predicting insider breaches using employee reviews," *Journal of Computer Information Systems*, vol. 64, no. 4, pp. 518-532, 2024. <https://doi.org/10.1080/08874417.2023.2226640>
- [39] S. G. Baker *et al.*, "How to interpret a small increase in AUC with an additional risk prediction marker: Decision analysis comes through," *Statistics in Medicine*, vol. 33, no. 22, pp. 3946-3959, 2014. <https://doi.org/10.1002/sim.6195>
- [40] A. Nyombi, N. Wycliff, B. Happy, M. Sekinobe, and J. Ampe, "Enhancing cybersecurity protocols in tax accounting practices: Strategies for protecting taxpayer information," *World Journal of Advanced Research and Reviews*, vol. 23, no. 3, pp. 1788–1798, 2024. <https://doi.org/10.30574/wjarr.2024.23.3.2838>
- [41] J. Chen, E. Henry, and X. Jiang, "Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach," *Journal of Business Ethics*, vol. 187, no. 1, pp. 199-224, 2023. <https://doi.org/10.1007/s10551-022-05107-z>

- [42] M. F. Shams, M. Sheikhi, and Z. Sheikhi, "Financial distress prediction: Comparisons of logit models using receiver operating characteristic (ROC) curve analysis," *African Journal of Business Management*, vol. 5, no. 30, p. 12164, 2011. <https://doi.org/10.5897/ajbm11.1969>
- [43] J. f. Alqatawna, J. Siddiqi, O. Al-Kadi, R. Al-Sayyed, and A. Najdawi, "Assessing the role of governments in securing e-business: the case of Jordan," *Emerging Trends in ICT Security*, pp. 125-136, 2014. <https://doi.org/10.1016/B978-0-12-411474-6.00008-6>
- [44] Y. Wang, "A multinomial logistic regression modeling approach for anomaly intrusion detection," *Computers & Security*, vol. 24, no. 8, pp. 662-674, 2005. <https://doi.org/10.1016/j.cose.2005.05.003>
- [45] N. Cerpa, M. Bardeen, B. Kitchenham, and J. Verner, "Evaluating logistic regression models to estimate software project outcomes," *Information and Software Technology*, vol. 52, no. 9, pp. 934-944, 2010. <https://doi.org/10.1016/j.infsof.2010.03.011>