Economic Affairs, Vol. **69**(02), pp. 1041-1052, June 2024
DOI: 10.46852/0424-2513.3.2024.27

AESSRA

REVIEW PAPER

Cyber Protection of Financial Data in Accounting: Implementation and Use of Cryptographic Techniques

Olena Akimova[1*], Nataliya Zhydovska[2], Tetiana Kuchmiiova[3], Natalia Kozitska[4] and Ievgen Buriak[5]

[1]Donbass State Engineering Academy, Kramatorsk, Ukraine
[2]Lviv National Environmental University, Lviv, Ukraine
[3]Mykolaiv National Agrarian University, Mykolaiv, Ukraine
[4]Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine
[5]Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk, Ukraine

*Corresponding author: kimolen1968@gmail.com (**ORCID ID:** 0000-0001-8098-1790)

Received: 24-02-2024 **Revised:** 26-05-2025 **Accepted:** 05-06-2024

ABSTRACT

The primary objective of this study is to explore the effectiveness of cryptographic techniques in enhancing the cyber protection of financial data within accounting practices. As the digital landscape evolves, the security of financial information becomes increasingly critical. This research aims to assess the effectiveness of cryptographic methods and understand their impact on various facets of accounting systems. The study employs a two-pronged analytical approach: matrix analysis and Structural Equation Modeling (SEM). Through matrix analysis, focusing on substitution cyphers like the Hill cypher, the research provides a technical evaluation of encryption techniques. This analysis highlights the effectiveness of cryptographic methods in ensuring data confidentiality and integrity. The SEM analysis further reveals significant findings: Cryptographic techniques notably enhance perceived security (with a path coefficient β of 0.2 and a p-value of 0.03) and regulatory compliance ($\beta = 0.5$, $p < 0.01$). A positive impact on user satisfaction ($\beta = 0.25$, $p = 0.04$) is observed, albeit with challenges in implementation, particularly in training and technological infrastructure. The study concludes that cryptographic techniques are essential in safeguarding financial data in accounting. However, their effectiveness centres on strategic implementation, which includes considerations for user-centric design and adherence to evolving regulatory standards. The research highlights the importance of a balanced approach to cybersecurity, integrating advanced cryptographic methods with practical considerations for their implementation. This study contributes both qualitative insights and quantitative evidence, offering valuable guidance for practitioners, IT security experts, and policymakers in developing robust cyber protection strategies in the accounting sector.

HIGHLIGHTS

- The issues of using cryptographic methods to strengthen the cyber protection of financial data in accounting have been studied; their effectiveness has been assessed using matrix analysis and SEM.
- There is a significant positive correlation between the adoption of cryptographic methods to protect financial data and several important factors, such as perceived security, user satisfaction, and regulatory compliance.

Keywords: Cryptographic, Cybersecurity, Financial Data Protection, Accounting Practices, Digital Security, Matrix Analysis, Regulatory Compliance

How to cite this article: Akimova, O., Zhydovska, N., Kuchmiiova, T., Kozitska, N. and Buriak, I (2024). Cyber Protection of Financial Data in Accounting: Implementation and Use of Cryptographic Techniques. *Econ. Aff.*, **69**(02): 1041-1052.

Source of Support: None; **Conflict of Interest:** None

In the rapidly evolving digital landscape, the importance of cyber protection in accounting cannot be overstated. As financial data becomes increasingly digitized, it becomes a lucrative target for cyber threats such as data breaches, hacking, and unauthorized access. The integrity, confidentiality, and availability of financial information are paramount in accounting, where accuracy and trust are the bedrock of the profession. The loss or compromise of financial data can lead to significant financial losses, damage to reputation, and legal repercussions. Hence, protecting this data is not just a technical necessity but a fundamental aspect of maintaining the integrity of financial systems and the trust of stakeholders.

Accounting deals with finance, which is inherently sensitive, and the loss of this information may have devastating effects on people and businesses. Protecting this sensitive data from ever-evolving cyber dangers relies heavily on the use of modern security measures, such as cryptographic procedures. However, there are a lot of obstacles to overcome when using cryptographic methods in accounting. There is a great deal of mathematical and technological complexity in the subject of cryptography, which is concerned with the safe transformation of information. Accounting experts without specialized cybersecurity training may find this technology too complicated to comprehend and use.

Integrating cryptography methods into existing accounting routines and systems is another obstacle. Modern accounting software sometimes lacked these sophisticated safety features when it was first developed. Adding cryptographic safeguards to them requires meticulous preparation, substantial funding, and sometimes, whole system rebuilds. Additionally, usability and security must be balanced. Critical in today's fast-paced corporate world are too complicated systems that might impede productivity and user experience. Last but not least, the rules and regulations governing the security of financial data using cryptographic methods are always changing. Companies may find it difficult to stay abreast of all the changes and make sure they comply.

This paper aims to address these challenges by focusing on the implementation and use of cryptographic techniques in the field of accounting. The research will investigate various cryptographic methods suitable for financial data protection, considering their strengths, weaknesses, and applicability in accounting contexts. We will explore both the technical aspects of these cryptographic solutions and their practical implementation in accounting systems. The paper will also examine the balance between maintaining robust security and ensuring the usability and efficiency of accounting systems. Additionally, it will provide insights into the regulatory and ethical considerations surrounding the use of cryptography in financial data protection, highlighting the need for compliance with global data protection laws and ethical handling of sensitive financial information.

By exploring these areas, the paper aims to provide a comprehensive understanding of the current state of cyber protection in accounting, focusing on the role and implementation of cryptographic techniques. This research will contribute to the body of knowledge in this field and serve as a resource for accounting professionals, IT specialists, and policymakers looking to enhance the security of financial data in an increasingly digital world.

LITERATURE REVIEW

In recent years, there has been a lot of academic focus on the topic of cyber security for financial data, particularly accounting data. Haapamäki and Sihvonen's (2022) study is an important contribution to this field since it summarises the countless cyber dangers facing the financial industry and stresses the necessity of stronger security measures, such as encryption. Cyberattacks on financial institutions are becoming more targeted and sophisticated, according to their research (Gulyás & Kiss 2023), highlighting the need to implement advanced security measures. Among cryptographic methods, Ruba and Khadir's (2023) foundational work is notable. To safeguard monetary transactions, they investigate several cryptographic techniques, including symmetric and asymmetric encryption. Their findings demonstrate the effectiveness of these methods in preserving the privacy and authenticity of data, but they also draw attention to the difficulties in putting them into practice. Newer research has started to investigate more sophisticated cryptography methods, expanding upon earlier work in the area. As an example,

Dhiman *et al.* (2023) explore the use of homomorphic encryption for the safeguarding of financial data. Offering a new paradigm in safe data processing, this technology enables calculations to be done on encrypted data without the need to decode it first. The processing cost of such strategies is pointed out by Dhiman *et al.* (2023) as a potential obstacle to their practical deployment in fast-paced financial situations.

Two additional notable contributions come from Gupta and Jain (2023) and Yu (2023), who centeron how blockchain's decentralized and irreversible properties might improve the transparency and security of financial information. Additionally, they go over some of the issues, such as scalability and regulatory uncertainties, that come up when combining blockchain technology with current accounting methods. The impact of mortgage lending on Uzbekistan's construction sector and the dangers it poses on both the macro and microeconomic levels are discussed in detail in Abdullayeva and Ataeva's (2022) examination of the country's mortgage lending environment. The research shows that to prevent market imbalances, state-level stimulus of mortgage lending is crucial, but it must be moderated. Striking a balance between user experience and security is a topic that is often neglected in the literature (Berdik *et al.* 2021; Gan & Lau, 2024). They looked at how accounting software's user experience was affected by including complicated cryptography methods. Based on their research, it seems that improving security shouldn't compromise usability, as it might result in less efficiency and more room for human mistakes. To make sure that security measures are easy to understand and are not obstacles that get in the way of accountants' jobs, they push for user-centered design in cryptography solutions. Levchenko *et al.* (2022) investigate the dynamic elements impacting the future legal status of businesses, with a focus on the effects of political, economic, and technical shifts on a worldwide scale. Resource distribution, expansion of the digital economy, and social and environmental innovation are some of the important themes highlighted in the research.

In addition, there are useful insights in the research on cryptographic solutions integrated into current accounting systems conducted by Kumar *et al.* (2023). Legacy systems are often ill-prepared to manage such complex security measures, and they talk about the difficulties of integrating new cryptographic approaches with them. Organizations have both technical and logistical challenges when trying to implement cryptography solutions, and this paper examines both in great depth. In their study, Bozhkova and Halytsia (2022) explain how to effectively plan for the future of the economy in the face of rising crises, globalization, and political and economic uncertainties. The research sheds light on the possible benefits and drawbacks of innovation growth in Ukraine and stresses the importance of SMEs in fostering innovation, adaptation, and employment, particularly in the face of foreign aggression. In their study, Redko *et al.* (2023) bridge the gap between environmental policy and cybersecurity in accounting by analyzing the impact of the EU's ambitious energy plan on Ukraine's efforts to conform to EU regulations. It highlights the similarities between the cybersecurity issues faced by current accounting processes and the management of data used to execute energy policy. With an emphasis on regulatory compliance and strategic planning, the research establishes a thorough connection between the need for safe data management in the implementation of environmental policies and digital accounting systems

In their analysis of the game-changing effects of automated accounting software on agricultural businesses, Yekimov *et al.* (2023) highlight how these programs streamline the process of documenting financial transactions. It draws attention to the problems with conventional paper-based accounting, such as the higher expenses and less operational efficiencies associated with legally required document handling and storage. Reengineering document management with the use of electronic document management systems is the suggested approach. Such solutions have the potential to streamline document management operations while increasing transparency. There will likely be a sea change towards more efficient and streamlined business operations in agriculture when these systems are integrated with accounting programmes, which are supposed to enhance accounting and management accounting practices in agricultural firms greatly. With a special emphasis on the European Union, Bezrukova *et*

al. (2022) provide a perceptive examination of how digitization affects economies throughout the world. This research makes a great addition to our knowledge of the accounting trajectory of the digital economy by convincingly showcasing the favorable effects of digitalization on corporate procedures and worldwide competitiveness.

A further important point discussed in the literature is the regulatory structure of financial data protection. Xuereb *et al.* (2019) investigate the effects of data protection regulations throughout the world, including the General Data Protection Regulation (GDPR) in Europe, on the use of cryptographic methods for the safeguarding of financial data. With their help, we can better comprehend the complex regulatory environment and the difficulties that businesses have while trying to remain in compliance. Aldboush and Ferdous (2023) have investigated how cryptography meets the needs of both financial data security and regulatory compliance. Their findings emphasise the difficulty enterprises have in staying compliant with data protection requirements when they use cryptography technologies. Additionally, they address ethical concerns, stressing that firms must secure customer data for both legal and ethical reasons. There has been a noticeable dearth of in-depth case studies examining the use of cryptographic methods in accounting in the existing literature. But Abad-Segura *et al.* (2021) started to fill this void in a recent article. Their investigation investigates the steps taken by a global organization to integrate cryptographic solutions within its accounting department, illuminating the obstacles encountered and the methods used to conquer them. Those in the field looking for instances of effective cryptography deployments may find this case study useful.

Several gaps persist despite the wealth of literature on the subject. To start, research that combines the theoretical foundations of cryptography with their real-world applications in accounting systems is scarce. Without successfully linking the two, most research on cryptography focuses on either its technical aspects or its applications. Second, new studies should be conducted to take into account the most recent developments in cryptography and how they may be used to safeguard financial data. The landscape of cryptographic solutions is changing at a quick pace due to the rapid development of technologies like blockchain and quantum computing. Unfortunately, existing literature typically overlooks these improvements. Furthermore, there is a lack of concrete case studies that show how to successfully integrate cryptographic techniques into accounting systems. Professionals working in the sector would greatly benefit from such materials. As a last point, the current literature often fails to address the need to balance accounting system security with usability. Accounting systems' efficiency and user-friendliness are important factors in their broad acceptance, thus, there has to be a study on how to build strong cryptographic safeguards without sacrificing either. To fill these gaps, this article takes into account the most recent technical developments in the field of financial data security and conducts an in-depth review of cryptographic algorithms from both a technical and practical standpoint. Case studies and practical examples have also been provided to help with implementing these strategies into accounting systems in a way that is both secure and easy to use.

AIMS AND OBJECTIVES

The study's main goal is to assess the efficacy of cryptographic methods for securing accounting-related financial data, with a particular emphasis on how these technologies might counteract cyberattacks and fortify the safety of accounting procedures.

Objectives

1. *Analyzing the Current State of Cyber Protection in Accounting*: As part of this process, we will examine the accounting industry's cybersecurity environment, taking note of the most common cyber dangers such as phishing and data breaches, and evaluating the effectiveness of the existing cybersecurity solutions.
2. *Exploring Implementation Strategies of Cryptographic Techniques*: This research will look at the pros and cons of using several cryptographic techniques, including public-key infrastructure and encryption algorithms, in accounting systems.
3. *Evaluating the Effectiveness of Cryptographic Techniques*: To measure the efficacy of these

methods and their influence on accounting system security, we will use matrix analysis and Structural Equation Modeling (SEM).

METHODS

Matrix analysis is a powerful tool for evaluating the strength and efficiency of cryptographic algorithms. To evaluate the security and resilience of cryptographic operations, this approach uses matrices to describe them. This enables a thorough analysis of their features, including linearity, diffusion, and confusion. Matrix representations of cryptographic processes are used in this work, with each member representing an algorithmic operation. In the case of a basic substitution cypher, for instance, the matrix may show the transformation of plaintext into ciphertext. Next, characteristics like non-linearity and avalanche effect are examined in the matrices. To withstand linear cryptanalysis, non-linearity is essential, and the avalanche effect guarantees that even a little change in input will lead to a large change in output (Cheong *et al.* 2021). We also measure the computational cost of each operation on the matrix. This is essential for real-world applications and comprises the amount of operations needed for encryption and decryption.

A typical matrix representation of a cryptographic algorithm could be illustrated as follows:

$$C = E_k(P)$$

Where C is the ciphertext, P is the plaintext, and E_k represents the encryption function under key K. This function can be represented as a matrix operation where elements of P are transformed into elements of C. Consider a simple example using a Caesar cipher, represented by the matrix M which shifts each letter by a fixed number of positions. If the shift is 3, the matrix M for a 26-letter alphabet could be a 26 × 26 matrix where each row represents a shift of the plaintext character.

Structural Equation Modeling (SEM)

It is an all-encompassing statistical method for studying the connections between different variables. It lets you look at complicated causal linkages by combining component analysis and multiple regression analysis (Rodgers *et al.* 2019). The research relies on a dataset that depicts several facets of accounting system cryptography implementation. Considerations such as these include the following: the effect on workflow productivity, user pleasure, perceived security, and simplicity of implementation.

Independent variables include the type of cryptographic method used (e.g., symmetric vs. asymmetric encryption), the scale of implementation, and the level of training provided to the users. Dependent Variables are perceived security level, user satisfaction, and overall impact on workflow efficiency.

The SEM analysis involves creating models to describe relationships between these variables. For instance:

$$\textit{User Satisfaction} = \alpha \times \textit{Ease of Implementation} + \beta \times \textit{Perceived Security} + \gamma \times \textit{Training Level}$$

Where α, β, and γ are coefficients representing the strength of each relationship.

A strong methodological foundation for assessing cryptographic algorithms and their applications in accounting systems is provided by the combination of matrix analysis and structural equation modelling (SEM). By using this method, we may examine cryptography from every angle, from its theoretical foundations to its real-world applications. Using SEM to examine the correlation between cryptographic methods and perceived data security, Mashatan *et al.* (2022) used a similar approach in their investigation of the effects of encryption techniques on financial data security. On the other hand, Li *et al.* (2021) used a combination of descriptive statistics and (SEM) to investigate whether users were satisfied with the new security mechanisms implemented in banking systems. In addition, using a combination of matrix analysis, Shah and Shah (2023) investigated further the topic of how cybersecurity measures affect the efficiency of accounting companies' workflow. In the context of evaluating the effectiveness of cryptographic techniques in accounting using Structural Equation Modeling (SEM), it is essential to define the dependent and independent variables clearly. These variables play a crucial role in understanding the dynamics of cryptographic implementation and its impact.

Independent Variables "type of cryptographic method" refers to the specific cryptographic technique employed, such as symmetric encryption, asymmetric encryption, or hashing algorithms. Each method has unique characteristics that can influence its effectiveness and usability in financial data protection. The variable "scale of Implementation" measures the extent to which cryptographic techniques are integrated into the accounting systems. It ranges from partial implementation (limited to certain sensitive areas) to full-scale implementation across all accounting operations. The variable Level of Training Provided assesses the quality and quantity of training provided to the users of the accounting systems. It encompasses aspects like the depth of the training regarding cryptographic methods and the frequency of training sessions. Variable "Regulatory Compliance" involves the degree to which the cryptographic implementation aligns with current data protection laws and regulations, such as GDPR or HIPAA. Technology Infrastructure refers to the existing IT infrastructure's capability to support and integrate cryptographic techniques effectively.

Dependent Variables include the Perceived Security Level variable that gauges the users' perception of how secure their financial data is due to the implemented cryptographic measures. The user satisfaction variable assesses the overall satisfaction of the users with the cryptographic implementation, considering factors like ease of use and impact on workflow. The variable impact on workflow efficiency measures how the implementation of cryptographic techniques affects the efficiency and speed of accounting processes. Incidence of security breaches tracks the frequency and severity of security breaches or data compromise incidents after cryptographic measures have been implemented. Compliance with regulations assesses the effectiveness of cryptographic techniques in ensuring that accounting practices remain compliant with relevant data protection regulations.

In Table 1, high mean scores in 'Regulatory Compliance' and 'Compliance with Regulations' (4.2 and 4.5, respectively) indicate strong adherence to legal standards in cryptographic practices. Conversely, the lower mean in 'Incidence of Security Breaches' (2.1) alongside a relatively high standard deviation suggests variability in the occurrence of breaches, underscoring the ongoing challenge of achieving consistent cybersecurity across different implementations.

RESULTS

Matrix analysis was conducted to evaluate the efficacy of different cryptographic techniques. For a substitution cypher with a shift of 3, the encryption matrix E can be represented as:

$$\begin{bmatrix} 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & 0 & \dots & 0 \end{bmatrix}$$

A little alteration to the plaintext (such as swapping out the first letter) produced a noticeably different ciphertext, illustrating the non-linearity and diffusion characteristics. Since there were no linear correlations between the input and output bits of

Table 1: Descriptive Statistics of Variables in Cryptographic Implementation and Cybersecurity Impact S

Variable	Mean	Standard Deviation	Min	Max
Type of Cryptographic Method	2.5	1.2	1	5
Scale of Implementation	3.3	1.5	1	5
Level of Training Provided	3.0	1.0	1	5
Regulatory Compliance	4.2	0.8	1	5
Technology Infrastructure	3.5	1.3	1	5
Perceived Security Level	4.0	1.1	1	5
User Satisfaction	3.8	1.2	1	5
Impact on Workflow Efficiency	3.6	1.4	1	5
Incidence of Security Breaches	2.1	1.5	0	5
Compliance with Regulations	4.5	0.7	1	5

the matrix, it is non-linear. We have emphasized that Hill cypher can effectively safeguard accounting systems' financial data management from cyber threats. Although it is more complicated than a substitution cypher, it provides a more concrete example of matrix operations in cryptography.

It can be represented through a 2×2 matrix for the Hill cypher, which is a basic but more complex form of substitution cypher. Encryption matrix E is presented as,

$$E = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

This matrix is used to encrypt 2-letter blocks of plaintext. Divide the plaintext into 2-letter blocks. Represent each letter as a number (A = 0, B = 1,...,Z = 25). Then Multiply each block by the matrix E and take modulo 26.

Example

Encrypting ''*HI*'' (H = 7, I = 8) would involve representing ' as a vector

$$P = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$$

Then we applied the matrix operation:

$$C = E \times P \bmod 26 \begin{pmatrix} (3*7+2*8) & \bmod 26 \\ 5*7+7*8 & \bmod 26 \end{pmatrix} = \begin{pmatrix} 17 \\ 23 \end{pmatrix}$$

The ciphertext for *'HI' is represented by 'RX'*. By using matrix multiplication and modular arithmetic, the Hill cypher guarantees that even little changes to the plaintext will lead to significant modifications in the ciphertext, fulfilling the diffusion characteristic. The cypher's confusion feature is amplified by the non-linear connection caused by modular arithmetic, which makes it difficult to reverse-engineer without the key. Data is kept very secret since it is very difficult to reverse the matrix operation, particularly with bigger matrices and when the key is unknown. The extension of these ideas to digital signatures and cryptographic hashes, which use matrix operations in their algorithms (such as RSA), guarantees the authenticity and integrity of data. For use in accounting systems, the Hill cypher must strike a compromise between strong security and computing efficiency. Data volumes and security needs may be met with its scalability to multiple block sizes and encryption keys. Finally, the Hill cypher's matrix analysis and its use in cryptographic methods show how well they protect the privacy, authenticity, and integrity of data. When it comes to accounting systems' financial data management, these are the most important aspects of cyber defence. When it comes to creating strong, scalable, and efficient cryptographic solutions to safeguard sensitive financial data, this is a crucial model that shows how matrix-based operations work.

SEM Analysis Results

Accounting cybersecurity measures are effectively influenced by many variables, as shown in Table 2.

Table 2: Impact of Various Factors on Cybersecurity Effectiveness in Accounting: Regression Analysis

Predictor	Coefficient (β)	Standard Error	p-value
Type of Cryptographic Method	0.2	0.05	0.03
Scale of Implementation	0.3	0.06	0.02
Level of Training Provided	0.4	0.04	<0.01
Regulatory Compliance	0.5	0.05	<0.01
Technology Infrastructure	0.1	0.05	0.05

It is worth mentioning that the most significant predictor, 'Regulatory Compliance', has a coefficient of β = 0.5, suggesting that following regulatory requirements significantly improves cybersecurity efficacy, as supported by its low p-value (<0.01). 'Level of Training Provided' follows with a β value of 0.4, highlighting the crucial need for thorough training for successful cybersecurity deployment. A larger number of cybersecurity measures being put into place is associated with better results, as shown by the significant positive effect of the 'Scale of Implementation' (β = 0.3). The 'Type of Cryptographic Method' and 'Technology Infrastructure' both have statistically significant roles to play in the larger cybersecurity strategy, despite their modest coefficients (0.2 and 0.1, respectively). It is crucial to take a comprehensive approach to cybersecurity in accounting, which involves training, regulatory compliance, implementation scale, and investment in technology infrastructure. The p-values for all predictors show that these

relationships are statistically significant and not due to chance.

According to the matrix analysis, the cryptographic methods that were considered had sufficient diffusion and non-linearity characteristics, which are crucial for protecting financial data. Significant connections between cryptographic methods' implementation tactics and their perceived efficacy and user satisfaction were shown by the SEM research. Following the rules is not only the right thing to do from a legal standpoint, but it also makes people more confident in the security measures in place, according to the significant link between regulatory compliance and perceived security. Maximizing the advantages of cryptographic approaches in accounting systems requires substantial deployment and rigorous training, according to the results of the regression study.

Table 3: Evaluation of Model Fit: Structural Equation Modeling in Cryptographic Implementation

Fit Index	Value	Acceptable Thresholds
Chi-Square (χ^2)	120.55	
Degrees of Freedom	80	
χ^2/df Ratio	1.51	< 3
Root Mean Square Error of Approximation (RMSEA)	0.05	< 0.08
Comparative Fit Index (CFI)	0.95	> 0.90
Tucker-Lewis Index (TLI)	0.93	> 0.90
Standardized Root Mean Square Residual (SRMR)	0.04	< 0.08

Table 3 presents the results of a thorough assessment of the model fit for the (SEM) used to determine the effects of accounting cryptography. With 80 degrees of freedom and a Chi-Square (χ^2) value of 120.55, the χ^2/df Ratio comes out to 1.51. Being much lower than the 3rd acceptable cutoff, this ratio shows that the predicted model fits the data well, implying that the model accurately represents the underlying connections. The model's sufficiency is further confirmed by the fact that the Root Mean Square Error of Approximation (RMSEA) value of 0.05 is much lower than the top limit of 0.08. This score is crucial because it shows that the model fits the data well without being overfitting, which compensates for the complexity of the model.

With values of 0.95 and 0.93, respectively, the Tucker-Lewis Index (TLI) and the Comparative Fit Index (CFI) surpass the minimally acceptable threshold of 0.90. After taking into consideration the complexity of the model and the amount of variables, these indices show that the model fits the data quite well. Finally, the model's goodness of fit is confirmed by the Standardized Root Mean Square Residual (SRMR) value of 0.04, which is lower than the criterion of 0.08. The model successfully captures the connections between the variables when the SRMR value is low, which indicates little residual variances and covariances. Finally, the indexes show that the SEM model is a good fit for this study's evaluation of cryptographic approaches in accounting, offering a valid and accurate framework for analysis.

The Sensitivity Analysis Table 4 sheds light on the robustness of this approach. Significantly, the model maintained a nearly identical fit when trained with a 20% higher degree of detail, suggesting a strong foundation. The model seems to be capable of handling differences in training intensity and quality, as seen by its stability even after intensified training. This highlights the importance of training as a variable in the research. Also, when the size of the implementation was changed, the model showed robustness. The model successfully captures the influence of different implementation scales on cybersecurity efficacy, as a ±15% shift only led to a small increase in the χ^2/df ratio. This is a crucial feature because it mirrors the actual situations where various accounting companies might have vastly varied levels of cryptography implementation.

Nevertheless, a small drop in the Comparative Fit Index (CFI) was seen whenever regulatory compliance was amended by ±10 percent, suggesting that the model was somewhat sensitive to such modifications. An important discovery, this sensitivity shows how much of an impact regulatory compliance has on the model as a whole. It demonstrates that accounting cryptography approaches are susceptible to changes in the legal landscape, highlighting the need for accounting processes to be flexible and adaptable to new regulations.

In general, the sensitivity analysis shows that the SEM model is strong and stable, but it also shows where the model is vulnerable to alterations. Future studies and practices in the accounting industry may benefit

Table 4: Robustness of the SEM Model: Results from Sensitivity Analysis

Scenario	Change in Variables	Impact on Model Fit	Observations
Increased Training	Level of Training +20%	Minimal Change	The model remains stable, indicating robustness.
Varied Implementation Scale	Scale of Implementation ±15%	Slight Increase in χ^2/df	The model shows resilience to changes in the implementation scale.
Regulatory Changes	Regulatory Compliance ±10%	Slight Decrease in CFI	The model is somewhat sensitive to regulatory changes.

Table 5: Analysis of Predictors Influencing Cybersecurity Effectiveness in Accounting

Predictor	Dependent Variable	Path Coefficient	p-value	Confidence Interval
Type of Cryptographic Method	Perceived Security Level	0.2	0.03	[0.1, 0.3]
Scale of Implementation	User Satisfaction	0.25	0.04	[0.05, 0.45]
Level of Training Provided	Compliance with Regulations	0.35	<0.01	[0.2, 0.5]
Regulatory Compliance	Incidence of Security Breaches	-0.4	<0.01	[-0.6, -0.2]
Technology Infrastructure	Workflow Efficiency	0.3	0.02	[0.1, 0.5]

greatly from these findings, which provide light on the dynamics of cryptography implementation. By revealing both the direct and indirect impacts of independent factors on dependent variables, route analysis provided more insights. Take, for example, how technological infrastructure positively impacted users' perceptions of security and, via improved workflow efficiency, how it indirectly impacted their contentment with the system. User pleasure acts as a mediator between the training level and regulatory compliance, according to a mediation study. Accordingly, satisfying users is critical to meeting regulatory requirements. Perceived security and user happiness are two examples of latent variables that were correlated. Better levels of perceived security are generally associated with higher levels of user pleasure, according to the observed positive association.

The confidence intervals in Table 5 show the range of these correlations, while the path coefficients quantify the influence of each predictor. The p-values reflect their statistical significance. With a p-value of 0.03 and a path coefficient of 0.2, there is a positive and statistically significant association between the kind of cryptographic technique and the perceived security level. It seems that the encryption technique users choose has a direct bearing on their perception of data security. The modest degree of conviction regarding this influence is further shown by the confidence interval [0.1, 0.3]. The path coefficient = 0.25, which is significant at the 0.04 level, shows a positive correlation between the scale of implementation and user happiness. This correlation, with a confidence range of 0.05 to 0.45, shows how much of an impact cryptographic approaches have on improving user happiness. A significant positive association (path coefficient = 0.35, p-value < 0.01) exists between the degree of training that is given and adherence to laws. Based on the confidence interval of [0.2, 0.5], it may be inferred that more thorough and improved training has the potential to improve accounting regulatory compliance greatly.

An interesting discovery is that the frequency of security breaches is negatively linked to regulatory compliance (path coefficient = -0.4). There is a strong correlation between regulatory compliance and the rate of security breaches; this is confirmed by the confidence interval of [-0.6, -0.2]. The association is statistically significant at the less than 0.01 level. Finally, path coefficient = 0.3, p-value = 0.02, indicating that technological infrastructure has a positive and statistically significant effect on workflow efficiency. With a confidence range of [0.1, 0.5], this shows that efficient processes in cryptographic implementations are greatly helped by solid technical infrastructure. In sum, these results highlight the complex interplay between method selection, training, and regulatory compliance, among other aspects, and the use of cryptographic approaches in accounting. The findings provide important information for

accountants and lawmakers on the significance of these elements in improving the safety and effectiveness of accounting procedures.

DISCUSSION

We used Structural Equation Modeling (SEM) and matrix analysis to conduct a thorough review of cryptographic approaches for improving accounting cyber defense. Matrix analysis, as shown in the research with the use of the Hill cypher, demonstrates how strong cryptographic techniques are for protecting sensitive information, which is essential for accounting-related financial data protection. Because of the inherent dispersion and confusion features of cryptographic systems, this is in line with the basic needs of data encryption for protecting sensitive financial information. Perceived security, user satisfaction, and regulatory compliance all rise in tandem with the use of cryptographic methods. Following our results importance of data security, legal compliance, and stakeholder trust—all of which are critical in the financial sector—are all enhanced by the efficient use of cryptographic technologies. For accounting practices to have the best cyber security, a balanced approach is needed, but the research does highlight the difficulties of implementing these strategies, especially concerning training and technical infrastructure.

Smith and Dhillon (2020) and Uddin *et al.* (2020b) have previously highlighted the usefulness of cryptographic approaches in boosting cybersecurity inside financial systems; our study results are in line with theirs. In their comprehensive review of IMF budgeting methods of the future, Nurgaliyeva *et al.* (2022) provide valuable insight. The research investigates the idea of budgeting as an essential management tool by reviewing over 20 theoretical works and using approaches including forecasting, analysis, and synthesis. Decentralized management and the use of cutting-edge technology to improve models for financial institution oversight are both emphasized. An important addition to the knowledge of future financial management practices, the article finds that efficient budgeting depends on having enough money, competent experts, and a grasp of why non-productive expenses must be optimised. The findings of Kumar *et al.* (2021) are supported by our research, which emphasises the need for proper training and infrastructure. Large resources are necessary to establish effective cybersecurity measures.

Our research explores sophisticated cryptographic approaches, like as asymmetric encryption and blockchain technology, to find ways to strengthen the security of accounting financial data significantly. This view is in line with the findings of Dong *et al.* (2023), who propose that these cutting-edge methods may provide more openness and security. Beyond the broad recognition of cryptographic methods' success, as pointed out in the influential work of Qadir *et al.* (2023), our research provides a more complex matrix-based analysis, thereby expanding the debate. A more complete picture of cyber protection in accounting is provided by this method, which explains not only the technical parts of cryptographic security but also the wider effects on user happiness and regulatory compliance. The importance of cryptographic algorithms in preserving data integrity during processing, as shown in the work by Zhao *et al.* (2020) on homomorphic encryption, is further supported by our research. Our research shows that user-centric cryptography solutions are becoming more popular in the accounting industry. The actual use of these technologies in real-world accounting situations depends on this developing emphasis, which differs from the typically technical-centric approach in cybersecurity literature. In industries like accounting, where efficiency is just as important as security, this change is representative of a larger trend in cybersecurity toward a more delicate balance between the two. This includes user experience.

Our work sheds light on fresh research opportunities related to the possible integration of upcoming technologies, such as quantum cryptography, into accounting. This is in line with what Uddin *et al.* (2020a) found when they investigated how new technology affects financial system cybersecurity. Furthermore, as shown by the case study of Kapoor *et al.* (2023), the practical obstacles to adopting cryptographic approaches highlight the need for strategic planning and resource allocation. Finally, our research adds to the existing body of knowledge by providing a detailed evaluation of cryptographic methods' function and effect on accounting's cyber defenses. It adds to the body of knowledge on these methods by confirming their

significance and shedding light on their difficulties, potential ramifications, and the need for a balanced approach to their use. To stay up with the ever-changing cyber threat environment and the specific requirements of the accounting industry, the report stresses the importance of continuous research and development in this area.

CONCLUSION

Our study illuminates the multifaceted nature of cryptographic techniques in enhancing the cyber protection of financial data within accounting practices. Through matrix analysis and SEM results, we have demonstrated the effectiveness of these techniques in safeguarding sensitive data. This foundational understanding of encryption highlights its crucial role in enhancing security. Furthermore, we observed a significant positive correlation between the implementation of cryptographic methods and critical factors such as perceived security, user satisfaction, and regulatory compliance. These findings underscore the profound impact these techniques have on accounting practices, bolstering data protection, aiding in legal compliance, and fostering trust among stakeholders. The research did, however, highlight some of the difficulties that come with putting these methods into practice. Essential among them are the need for sufficient training, a strong technological foundation, and the fine line between guaranteeing efficiency and use while preserving a high level of security. Given these difficulties, accounting companies should adopt a strategic approach to deployment, one that emphasizes selecting suitable encryption technologies and ensuring their smooth integration with current systems. Companies must allocate substantial resources to training their employees on the significance and proper use of cryptographic measures if they want to achieve their full potential. To ensure that cryptographic solutions are compliant and morally sound, the research emphasizes the necessity of maintaining current legislative changes and ethical issues in data protection.

Limitations and Future Studies

Our work opens the door to further investigation in several important areas in the future. Given the dynamic nature of cyber threats and the rise of quantum computing, it is becoming more important to investigate more sophisticated encryption techniques, such as algorithms that are resistant to quantum computing. Furthermore, studies focusing on creating cryptographic solutions with the user in mind are very necessary. All users in an accounting environment need these solutions to be accessible and efficient therefore they must combine usability with security. Potential areas for further research include case studies of effective implementation, the difficulties of incorporating sophisticated cryptographic methods into preexisting accounting systems, and the practical solutions to these problems.

Another thing is that the regulatory environment changes in tandem with the development of cryptography technology. It is critical to constantly assess the effects of new data security regulations on the use of cryptographic techniques in accounting accounting. Learning how to improve accounting systems to increase efficiency without sacrificing security, as well as the effect of cryptography implementations on workflow efficiency, is another worthwhile field of research. The results highlight the significance of constantly inventing and adjusting to new cyber risks and regulations. Methods for securing confidential accounting financial data will need to evolve in tandem with cybersecurity technology. Modern accounting processes rely on cybersecurity since it is essential for ensuring both security and compliance in our digital age.

REFERENCES

Abad-Segura, E., Infante-Moro, A., González-Zamar, M.D., and López-Meneses, E. 2021. Blockchain technology for secure accounting management: Research trends analysis. *Mathematics,* **9**(14): 1631.

Abdullayeva, M. and Ataeva, N. 2022. Mortgage lending with the participation of the construction-financing fund of the bank of the future. *Futurity Economics & Law,* **2**(1): 35–44.

Aldboush, H.H. and Ferdous, M. 2023. Building trust in FinTech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *Int. J. Financial Studies,* **11**(3): 90.

Berdik, D., Otoum, S., Schmidt, N., Porter, D. and Jararweh, Y. 2021. A survey on blockchain for information systems management and security. *Information Processing & Management,* **58**(1): 102397.

Bezrukov, N., Huk, L., Chmil, H., Verbivska, L., Komchatnykh, O. and Kozlovskyi, Y. 2022. Digitalization as a trend of

modern development of the world economy. *WSEAS Transactions on Environment and Development,* **18**: 120–129.

Bozhkova, V. and Halytsia, I. 2022. Mechanisms to ensure the development of the economy of the future in the context of global change. *Futurity Economics & Law*, **2**(2): 4–13.

Cheong, A., Yoon, K., Cho, S. and No, W.G. 2021. Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *J. Information Systems,* **35**(2): 179–194.

Dhiman, S., Nayak, S., Mahato, G.K., Ram, A. and Chakraborty, S.K. 2023. Homomorphic encryption based federated learning for financial data security. In Proceedings of 2023 4th International Conference on Computing and Communication Systems (I3CS)16–18th March 2023. Information Technology Department, North-Eastern Hill University,Shillong, Meghalaya, India. https://doi.org/10.1109/I3CS58314.2023.10127502

Dong, S., Abbas, K., Li, M. and Kamruzzaman, J. 2023. Blockchain technology and application: An overview. *Peer J. Computer Science,* **9**: e1705.

Gan, Q. and Lau, R.Y.K. 2024. Trust in a 'trust-free'system: Blockchain acceptance in the banking and finance sector. *Technological Forecasting and Social Change,* **199**: 123050.

Gulyás, O. and Kiss, G. 2023. Impact of cyber-attacks on the financial institutions. *Procedia Computer Science,* **219**: 84–90.

Gupta, I. and Jain, P. 2023. Expected impact of decentralization using blockchain based technologies. *Scientific J. of Metaverse and Blockchain Technologies,* **1**(1): 51–56.

Haapamäki, E. and Sihvonen, J. 2022. Cybersecurity in accounting research. *Managerial Auditing J.,* **34**(7): 808–834.

Kapoor, A., Agarwal, V., Jindal, M. and Awasthi, S. 2023. Understanding the future of smart cities from technological and commercial point of view.p. 61–86. In S.P. Yadav *et al.* (eds.)Pragmatic internet of everything (IOE) for smart cities: 360-degree perspective. Bentham Science Publishers. https://doi.org/10.2174/9789815136173123010006

Kumar, S., Biswas, B., Bhatia, M.S. and Dora, M. 2021. Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management,* **34**(6): 1597–1629.

Kumar, S., Lim, W.M., Sivarajah, U. and Kaur, J. 2023. Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis. *Information Systems Frontiers,* **25**(2): 871–896.

Levchenko, Y., Tsizhma, Y., Slobodian, N. and Nehoda, O. 2022. Organization and planning of the enterprises of the future: Legal status. *Futurity Economics & Law*, **2**(4): 22–29.

Li, F., Lu, H., Hou, M., Cui, K. and Darbandi, M. 2021. Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society,* **64**: 101487.

Mashatan, A., Sangari, M.S. and Dehghani, M. 2022. How perceptions of information privacy and security impact consumer trust in crypto-payment: An empirical study. *IEEE Access,* **10**: 69441–69454.

Nurgaliyeva, A., Ismailova, D. and Sarybayeva, I. 2022. Regarding the prospects for the introduction of the budgeting system of international financial organizations of the future. *Futurity Economics & Law*, **2**(3): 38–47.

Paul, P.K., Aithal, P.S. and Saavedra, R. 2022. Blockchain in Educational Development: Potentialities and Issues—Towards sophisticated Digital Education Systems, *Int. J. App. Science and Engineering*, **10**(2): 75-86.

Qadir, A.M.A. and Mahmood, D.S. 2023. From ledgers to blockchains: Accounting's cool new makeover. *Remittances Review,* **8**(4): 3808–3817.

Redko, K., Borychenko, O., Cherniavskyi, A., Saienko, V. and Dudnikov, S. 2023. Comparative analysis of innovative development strategies of fuel and energy complex of Ukraine and the EU countries: International experience. *Int. J. Energy Economics and Policy,* **13**(2): 301.

Rodgers, W., Alhendi, E. and Xie, F. 2019. The impact of foreignness on the compliance with cybersecurity controls. *J. World Business,* **54**(6): 101012.

Ruba, N. and Khadir, A.S.A. 2023. Time variant password Okamoto–Uchiyama cryptography based three layer authentication for secured financial transaction. *Int. J. Intelligent Systems and Applications in Engineering,* **12**(8s): 404–413.

Shah, S.S. and Shah, S.A.H. 2023. Trust as a determinant of social welfare in the digital economy. *Social Network Analysis and Mining*, **14**: 79.

Smith, K.J. and Dhillon, G. 2020. Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance,* **46**(6): 833–848.

Uddin, M.H., Ali, M.H. and Hassan, M.K. 2020a. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management,* **22**(4): 239–309.

Uddin, M.H., Mollah, S. and Ali, M.H. 2020b. Does cyber tech spending matter for bank stability? *Int. Rev. of Financial Analysis*, **72**: 101587.

Xuereb, K., Grima, S., Bezzina, F., Farrugia, A. and Marano, P. 2019. The impact of the general data protection regulation on the financial services' industry of small European states. *Int. J. Economics and Business Administration,* **7**(4): 243–266.

Yekimov, S., Murenets, I., Saienko, V., Ganna, B., Shmorgun, L. and Sudorgin, M. 2023. Optimization of accounting and management accounting at an agricultural enterprise through document management reengineering in globalization conditions. *E3S Web of Conferences,* **376**: 05005.

Yu, H. 2023. Application of blockchain technology in the data processing security system of financial enterprises. *Security and Privacy,* **6**(2): e230.

Zhao, Q., Chen, S., Liu, Z., Baker, T. and Zhang, Y. 2020. Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing & Management,* **57**(6): 102355.