National College of Ireland

Implementation of Advance Encryption Techniques to Protect Sensitive Financial Data from Cyber Threats

MSc Research Project
Cybersecurity

Salman Ahmed
Student ID: x23189801

School of Computing
National College of Ireland

Supervisor: Jawad Salauddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Salman Ahmed .....

Student ID: x23189801 .....

Programme: Msc Cyber Security ..... **Year:** 24-25 .....

Module: Practiccum2 .....

Supervisor: Jawad Salauddin .....

Submission Due Date: 12 Dec 24 .....

Project Title: Practiccum2 .....

Word Count: ..... **Page Count**.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Salman Ahmed .....

Date: 12 Dec. 24 .....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Implementation of Advance Encryption Techniques to Protect Sensitive Financial Data from Cyber Threats

Salman Ahmed
x23189801

Abstract

This research mainly focus to analyse and examine the effectiveness of advance encryption techniques (mainly cryptographic) in protecting the sensitive financial data from cyber threats within accounting and banking practices. The research covers the assessment of encryption methods / techniques adequacy and understand the subsequent impact on different aspects of sensitive financial data and related systems. The encryption techniques mostly covered cryptographic methods in this study. A two-pronged analytical methodology is adopted in the research i.e., Structural Equation Modelling (SEM) and matrix analysis. This research provides a technical aspect of cryptographic encryption techniques using matrix analysis concentrating on substitution ciphers including Hill cipher. The study outcome confirm the reliability of these techniques in successfully securing confidentiality and integrity of the sensitive financial data. The SEM analysis also identifies additional important results: first, the use of cryptographic techniques increases perceived level of security namely by 0.23 standardized path coefficients ($\beta = 0.23$, $p = 0.032$); second, regulatory compliance is positively impacted by variables like encryption that have a similar effect size ($\beta = 0.48$, $p < 0.01$). Additionally, an impact on satisfaction of end user is positively observed ($\beta = 0.27$, $p = 0.03$), though challenges persist in implementation, particularly regarding workforce technology infrastructure and training. The study underscores the critical role of strategic implementation in maximizing the efficacy of cryptographic solutions, emphasizing the need for user-centred design and alignment with evolving regulatory frameworks. It highlights the necessity of a balanced cybersecurity approach that integrates advanced encryption techniques with practical considerations for deployment. The research provides valuable insights both qualitative and quantitative to cyber and Information Technology (IT) practitioners, experts, standards and policymakers in establishing comprehensive data protection guidelines and processes in the financial sector[1].

1 Introduction

The financial services sector has seen a dynamic transformation based on advancements in financial technology and engineering, which have made digital platforms and solutions more convenient, accessible, and creative than ever before. Globally, digital financial tools like mobile banking apps and crypto currency exchanges have fundamentally altered how individuals and organizations manage their finances, communicate, and invest. Along with making financial services more accessible to everybody, digital transformation has created new

[1] Keywords: Cybersecurity, Cryptographic, Data Protection, Advance Encryption, Financial Sector, Matrix Analysis, Structural Equation Modelling.

challenges with regard to financial data and the need to protect private information from constantly evolving cyber threats based on more complex and sophisticated methods.

The significance of cyber protection within the financial sector cannot be understated in the current dynamic digitalization financial ecosystem. The increasing digitization of financial data and medium of transaction has made it a prime target for cyber threats such as hacking attempts, unauthorized access, and data breaches. Since the accuracy and linkage of financial data processes are based on these principles, it is imperative to ensure the availability, confidentiality, and integrity of financial data. Financial data loss or leakage has serious repercussions, such as significant monetary losses, reputation risk, and possible legal and regulatory fines and penalties. Considering the same, safeguarding financial data is more than just a technical issue as the same is essential in preserving the integrity of financial systems and sustaining stakeholder trust.

Particularly in the financial industry, where safeguarding or protecting sensitive data is crucial, and encryption is an essential part of cybersecurity to implement the protection. Using algorithms and keys, encryption converts readable data (plaintext) into an unintelligible format (cipher text), guaranteeing that only those with permission can decode and access the data. A few encryption methods were examined, put into practice, and an architecture was suggested to safeguard data on the cloud. Their design was created to use a cryptography technique based on a block cipher to store data in the cloud in an encrypted format (Sugumaran, et al. 2014).

One of the main concerns surrounding the transition to digital financial services is the possibility of financial data breaches. Such breaches may have serious repercussions, including identity theft, monetary loss, a decline in consumer trust, and legal cases. Analysing the critical importance of advanced encryption algorithms in enhancing the security barrier for digital financial applications is the primary goal of this research paper. In order to protect sensitive data, this paper aims to provide an understanding of the advantages, disadvantages, and real-world uses of several encryption types, including symmetric encryption (AES), asymmetric encryption (RSA), end-to-end encryption (E2EE), homomorphic encryption, and blockchain encryption..

The inherently sensitive nature of financial data makes it more vulnerable to data breaches and the consequences of data loss are huge and cascading. Modern data protection techniques such as cryptographic procedures and technologies are required to safeguard the sensitive data from emerging cyber threats with ever-evolving methods. The application of modern techniques also comes with many obstacles considering that there are complex underlying mechanism for encryption techniques. Finance professionals without adequate training related to the encryption techniques may find it very difficult to understand and utilize the same. Moreover, the financial and accounting systems mostly lacks adequate safeguard features and flexibility which makes it more difficult to integrate the advance encryption techniques such as cryptography within the systems. The implementation and integration also requires optimum funding, meticulous design and preparation, system capability and availability of resources. The modern financial systems are often too sophisticated and complex that they overlook end user experience and the integration of encryption techniques may make it more rigid. The application of advance encryption also attracts regulatory and other governing authorities with ever changing rules and regulations which makes it difficult for financial services firms to comply.

As a defence against online threats, spying, and possible breaches, data encryption becomes a crucial method in the cybersecurity toolbox (George et al., 2023). Data encryption is a vital

defence against unwanted access in the constantly changing world of digital communication and information exchange, protecting the integrity and confidentiality of sensitive financial data (Abdel-Rahman, 2023). In a time of unparalleled connectedness and data abundance, safeguarding digital assets has emerged as a critical issue. (Nassar and Kamal, 2021).

This study focused to mitigate and address these challenges by analysing and examining the application of advance encryption technique i.e., cryptographic techniques over the financial services sector and field. In the study investigation of various cryptographic techniques will be conducted which are suitable for sensitive financial data protection covering strength, weakness and suitability of these techniques. Both technical and functional implementation perspective of cryptographic encryption techniques will be explored in this research. The balance between sustaining strong security and guaranteeing the effectiveness and usability of financial systems will also be discussed in the research. It will also provide insights on the ethical and regulatory issues pertaining implementation of advance techniques like cryptography to protect sensitive financial data, emphasizing the necessity of handling sensitive financial data in an ethical manner and according to international data protection regulations.

The research aims to offer a detailed understanding by examining and analysing the current state of encryption techniques and cybersecurity protection related to financial data and systems. The study will provide valuable knowledge and practical aspects of enhancing the security of sensitive financial data in this dynamic digital age. It will help the finance professionals, IT and cyber experts and policymakers to update and adjust the guidelines and procedures accordingly.

1.1 Research Question

The underlying research question investigates and makes a hypotheses in order to identify pertinent solutions for safeguarding sensitive financial data from cyber threats. This research is based on the following question “How does the implementation of advanced encryption techniques protect sensitive financial data from cyber threats?” It is a worthwhile, feasible, and understandable research topic to analyse and examine how sophisticated encryption methods protect sensitive financial information from online attacks covering cyber attempts. By providing useful advantages for financial institutions and influencing regulatory procedures, it is anticipated that the study make a significant contribution to the field of cybersecurity (Arokiam and Monikandan, 2012). Ethical and regulatory guidelines adherence is of prime importance to conduct this research and the paper complies to it adequately.

The prime target of cyber-attacks is the financial services sector considering the large amount of data processing and huge volume of transaction conducted every day. Protecting sensitive financial data from these emerging threats requires adequate use of advance and complex encryption techniques. It is beneficial to analyse and examine the subject for a number of justifiable reasons, including the rise in cyber threats, the laws and standards guiding encryption methods, technological developments, and the financial consequences of data breaches. By carefully examining encryption tools for data protection, the financial services sector and its associated stakeholders can make well-informed decisions about advanced encryption strategies that meet user expectations for data privacy and protection, comply with legal and regulatory compliance standards, and strengthen security. Additionally, the research will analyse and investigate the emerging trends and parameters of encryption techniques applied to cyber space. The emerging trends covers robust data protection methods from cyber

threats e.g., Artificial Intelligence (AI) implementation, post-quantum encryption, cryptographic etc.

The existing studies does not provide adequate evidence or insights covering the underlying mechanisms of advance techniques deployed by hackers and cyber oriented criminal organizations for the purpose of stealing sensitive financial data. Additionally, the lack of pertinent data and knowledge has prevented a thorough study of the latest developments in cryptography and artificial intelligence (both static and generative). More than the proper application of advanced data protection measures, researchers mostly concentrated on examining the cybersecurity implementation issues in different fields. More rules pertaining to sensitive and personal data, including the General Data Protection Regulation (GDPR), also highlight the importance of using complex and advance methods in businesses worldwide to safeguard client and customers data in the financial services sectors.

This research paper is based on the following structure:

1. Introduction: provides background and initial context of the study and research questions covering hypothesis.
2. Literature Review: Provides detailed insight into the previous work related to cybersecurity and implementation of advance encryption techniques to protect sensitive financial data. The review also cover gaps and potential areas of target for this research.
3. Methodology and Design Specifications: The section covers description of methodology and research design along with techniques used to generate results.
4. Implementation and Results: The section covers the findings and outcome of the selected research methodology for the purpose of examination.
5. Discussion and conclusion: Interpret results of the analysis and examination with adequate comparisons. The section will also cover limitations to the study and suggestions for utilization.
6. References: The section will provide a list of all cited and related papers utilized for conducting the research.

2 Literature Review

There has been an increase in research and studies on the topic of protecting sensitive financial data by implementing advance encryption techniques especially from a perspective of finance and accounting sector (Haapamäki and Sihvonen, 2022). Financial and accounting data has been the most vulnerable sector considering the more sophisticated cyber threats and there is a more stringent need for adequate security measures such as encryption. The complexity and targeting of cyber-attacks on financial institutions has increased, underscoring the need for improved security protocols. (Gulyás and Kiss, 2023).

The evolution of digital age leads to free flow of information and data through internet and sophisticated financial systems, the need for safeguarding sensitive financial data is of more significance than ever before. Encryption is one of the key techniques currently used to safeguard sensitive financial data (Akimova et al., 2022). Several examination / studies were conducted on how financial institutions are increasingly integrating zero-trust architectures alongside encryption to mitigate internal threats. This shift responds to the recognition that insider attacks are just as harmful as external ones, especially within large organizations. The studies found that combining symmetric encryption techniques with zero-trust frameworks enhances protection against unauthorized access, even for employees with elevated privileges. This aligns with the global trend of prioritizing endpoint security in financial institutions to complement traditional encryption measures (Zhang et al., 2022).

The challenges related to the implementation of the advance cryptographic techniques such as symmetric and asymmetric were highlighted besides their usage to protect the sensitive financial data focusing on the confidentiality and integrity of data. The implementation of these techniques also comes with limitations and issues which needs to be focused accordingly (Ruba and Khadir, 2023). Building on earlier research in the topic, recent studies are examining increasingly sophisticated cryptography approaches used in protecting the financial data. The potential of homomorphic encryption to safeguard financial information has been examined and by enabling calculations to be done on encrypted data without first decoding it, this technique presents a new paradigm in safe data processing. One possible obstacle to this method of covering processing costs was also looked into as a potential bottleneck to its application in a dynamic financial services environment (Dhiman et al., 2023).

Several studies focuses on the key aspect of application of decentralized and irreversible properties of blockchain that might enhance and improve security of sensitive financial data. Some of the very pertinent issues were also discussed covering the dynamic regulatory requirements and scalability during the integration phase of blockchain with financial systems for cyber protection (Gupta and Jain, 2023). The balance between security and experience of the customer in the lending practices was analysed from a mortgage perspective where literature does not provide any detailed insights (Gan and Lau, 2024;Berdik et al. 2021). As part of their research, they covered the user interface and experience of financial systems and softwares questioning on their performance and flexibility due to integration of complex cryptographic solutions. Their research outcome stipulates that integration of encryption techniques for enhancing security of financial data should not impact the usability which may lead to ineffectiveness and human errors. Furthermore, it was highlighted that in order for advance encryption techniques to impact positively their underlying linkage should be user-friendly and easily understandable.

One of the research was conducted covering the integration of cryptographic into the modern financial systems using sensitive data (Kumar et al., 2023). It was highlighted in their study that obsolete or legacy systems are not adequately equipped with latest technologies to integrate

complex data security measures such as cryptographic solutions. Financial services firms face logistical and technical uncertainties during the implementation of advance encryption techniques, which was granularly examined in their research. Financial systems and the related encryption solutions for sensitive data security are also impacted with emerging requirements covering the Environmental, Social and Governance (ESG) objectives established for financial sector by various governing bodies such European Union (EU), Prudential Regulatory Authority (PRA) etc. where cybersecurity requirements are more focused on environmental friendly security solutions (Redko et al., 2023). With an emphasis on strategic planning and regulatory compliance, their study establishes a reliable connection between the need for secure data management in the implementation of environmental rules and digital financial systems.

2.1 Regulatory Landscape for Data Protection

Recent work and studies considers regulatory guidelines and standards around protection of financial data and the related safeguarding techniques as one of the core and crucial area. Regulators and governing authorities around the world pushed towards more establishing stringent and adequate rules and regulations around the use and processing of sensitive data and its protection after some of the major breaches, as the one that resulted in Experian Credit Bureau facing a fine of around $500 million (Twingate, 2024). It was examined that how the use of sophisticated encryption and cryptography methods to safeguard financial data was affected by international data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe and the Middle East. One of the study that has improved the researchers' comprehension of the complex regulatory environment and the difficulties businesses and the financial services sector encounter in upholding compliance was conducted by (Xuereb et al., 2019).

In addition to encryption itself, Regulatory Compliance has also been a critical focus in recent literature. Data privacy regulations were examined, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), are influencing the use of encryption within financial institutions. It was found that encryption has become a crucial tool for maintaining compliance, particularly with regulations that mandate the encryption of personal financial data during both transmission and storage (Navarro and Soler, 2023). Their study suggests that evolving regulatory frameworks are pushing financial institutions to adopt stronger encryption methods, especially as penalties for non-compliance grow stricter.

The practical difficulties faced by financial institutions in managing encryption at a large scale were discussed by (Rashid and Omar, 2022). With the advent of digital banking and mobile transactions, the need to secure massive amounts of real-time data has introduced challenges in key management, particularly for asymmetric encryption methods like Rivest-Shamir-Adleman (RSA). The study proposed the use of key management services (KMS) and hardware security modules (HSMs) to alleviate the operational burden of securely managing cryptographic keys across distributed networks, further supporting the scalability of encryption in financial environments.

The existing research does not sufficiently discuss or analyse granularly the case studies examining the use of encryption techniques in financial services and related facets. An analysis of the steps taken by several global financial institutions to integrate data protection methods specifically, advanced encryption solutions into their technology infrastructure and digital divisions for improved security offers important insights into the difficulties encountered and the methods associated with overcoming them. The use of cutting-edge encryption techniques and their integration with digital financial systems for data security objectives are extensively covered in the paper, which may be a very helpful and informative topic for researchers that

are interested (Abad-Segura et al., 2021). According to another study, encryption meets the standards for financial data security and regulatory compliance considering the latest financial systems infrastructure and underlying processing core. The findings demonstrated how difficult it is for businesses and financial institutions to continue to comply with data protection regulations when they incorporate and use highly complex and advance technologies like encryption. The study also looked at business practices and ethics, highlighting how important it is for financial institutions to protect sensitive financial data considering both ethical and legal reasons (Aldboush and Ferdous, 2023).

2.2 Encryption Techniques

Encryption by using the same key for both encrypting and decrypting the data is considered to the one of the common and fundamental technique used in data protection (Bokhari and Shallal, 2016). Large volumes of data and transactions can be processed by using this techniques with adequate efficiency. Basically, the technique revolves around sharing a coded key with involved parties i.e., the sender and the recipient to communicate in a private environment without involving the bureaucratic and regular management communication techniques. Among various sophisticated and known encryption techniques, the following two i.e., Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are prominently popular symmetric encryption methods used in the financial data protection across various sectors. Most of the digital financial systems and online platforms processing financial data use AES considering that it performs as per expectations while encrypting the sensitive financial data and has strong security features (Sathya and Banik, 2020).

Furthermore, the application of blockchain technology to improve encryption techniques was examined, especially with regard to protecting international financial transactions. The study demonstrated how blockchain-integrated encryption methods, such as Merkle trees and SHA-256, provide improved transaction data security. For global financial institutions, where transaction integrity and transparency is crucial, these findings are particularly pertinent. Blockchain is becoming a more and more popular alternative for high-value financial transactions because it securely encrypts every block of data, lowering the possibility of tampering or unauthorized change (Dhawan et al., 2023).

The application of quantum-resistant algorithms in protecting the sensitive financial data were examined and analysed (Anwar et al., 2022). With quantum computing posing a potential future threat to current encryption standards, algorithms such as lattice-based encryption and hash-based signatures are being tested for their viability in securing financial information. This research indicates that while post-quantum cryptography is still in its infancy, it is crucial for financial institutions to begin considering these encryption techniques to future-proof their security infrastructure. This shift is particularly relevant for institutions managing long-term contracts or financial agreements vulnerable to future decryption by quantum computers.

Further exploration of symmetric encryption techniques has also been prominent in recent research. The efficiency of the Advanced Encryption Standard (AES) with newer algorithms like ChaCha20, focusing on performance in processing large-scale financial transactions were examined and compared for data protection purposes (Liu et al., 2023). Their findings suggest that while AES remains the gold standard for financial encryption due to its balance of speed and security, ChaCha20 offers an alternative in environments where faster encryption times are essential without compromising security levels. Such studies highlight the ongoing effort to optimize encryption methods for the high-volume data processing typical of financial systems.

The implementation of encryption was investigated with relation to the expanding importance of multi-party computation (MPC) in protecting financial data. MPC is particularly helpful in

environments like financial audits, where sensitive data must be encrypted at all times, because it provides a platform to many parties to collaborate and calculate a function over their inputs while maintaining the privacy of these inputs. The underlying research demonstrated how asymmetric encryption in MPC frameworks can dramatically lower the danger of data breaches during cooperative financial operations, such mergers or acquisitions, where several organizations need to exchange sensitive information.

Hybrid encryption combines the finest aspects of symmetric and asymmetric encryption methods to improve security and performance in data protection. With hybrid encryption, a randomly generated symmetric key is exchanged via asymmetric encryption, followed by the encryption of additional data using a symmetric encryption algorithm such as AES or cryptography. This method, which blends high-performance symmetric encryption with the safe key exchange and delivery capabilities of asymmetric encryption, is used to process large volumes of data and adequately secures it from cyber threats and potential breaches (Sajay, Babu and Vijayalakshmi, 2019).

2.3 Research Niche

The topic related to cybersecurity and related safeguarding techniques has been examined and studied profoundly but there are still certain areas of improvement remained due to dynamic and fast evolution of technology. Considering the dynamic and emerging nature of cyber threats, there is very less research which focuses on the linkage and connection of real-life implementation of advance cryptography techniques with its theoretical aspects such as governance, management and monitoring. Most studies on various encryption techniques, like blockchain and cryptography, focus on either their technical aspects or their uses without effectively connecting the two. Furthermore, new studies must be conducted in light of the most recent developments in emerging encryption techniques and their possible uses in safeguarding data and financial information.

Given the scarcity of real-world case studies illustrating the successful integration of advanced encryption techniques into financial systems, the research would be highly beneficial to practitioners in the financial sector. Additionally, the literature and related work that is currently available and published usually overlooks how crucial it is to strike a balance between the security of the financial system and its usability whether it can be integrated with human skills of navigating the same. Since the broad adoption of financial systems heavily depends on these aspects, it is imperative to look at ways to provide strong encryption protection without compromising either usability or efficiency. By carefully examining advanced encryption techniques from a theoretical and practical perspective and keeping in mind the most recent technological advancements in the field of financial data protection, this study aimed to close the gaps.

2.4 Research Objective

The purpose of the research article is to investigate and evaluate the effectiveness of cryptographic techniques for protecting sensitive financial information and data stored and utilized in the financial systems, with a focus on how these encryption techniques could provide safeguard against cyber-attacks and strengthen the security of financial practices.

2.4.1 Objectives

1. **Current state assessment of financial sector from cybersecurity purposes:** During this step, the research will focus on assessing the current financial services environment from cyber security aspect covering data breaches and phishing along with existing security solutions implemented.

2. **Cryptographic techniques implementation:** The research will cover merits and demerits of various encryption (cryptographic) techniques such as encryption algorithms and public key infrastructure in financial systems.

3. **Effectiveness of encryption techniques:** The research methodology will be based on matrix analysis and Structural Equation Modelling (SEM**)** for the purpose of evaluating the effectiveness of the encryption techniques i.e., cryptographic.

3 Research Methodology

To conduct this research, matrix analysis has been selected to evaluate the cryptographic techniques resilience and security effectiveness. Matrix analysis is a well-known and powerful method to evaluate and examine the efficiency and strength of the advance encryption techniques such as cryptographic algorithms. The approach uses the matrices to describe the encryption algorithms covering detailed analysis of features which includes linearity, confusion and diffusion. This study employs matrix representations to model cryptographic processes, where each element corresponds to a specific algorithmic operation. For instance, the matrix may represent the transformation of plaintext into ciphertext, as seen in a basic substitution cipher. These matrices are subsequently analysed for critical attributes such as the avalanche effect and non-linearity. Non-linearity is a vital property for ensuring resistance against linear cryptanalysis, while the avalanche effect ensures that minor alterations in the input produce substantial changes in the output (Cheong et al., 2021).

For the purpose of real application and implementation in today's financial environment, the study also measures the cost of computation for each matric operation involved. The real-world application is important because it covers the amount of related encryption and decryption operations involved. The typical cryptographic algorithm from a matrix representation perspective can equated as:

$C = E_k (P)$

Where,
C = ciphertext
P = plaintext
E_k = encryption function

The encryption function E_k under key K can be represented as a matrix operation where P elements are transformed into C elements during the execution of methodology. For clarity, if we examine a straightforward example of a Caesar cipher, which is represented by the matrix M which moves each letter a predetermined number of locations. For a 26-letter alphabet, the matrix M might be a 26 × 26 matrix with each row denoting a shift of the plaintext character if the shift is 3.

3.1 Design – Structural Equation Modelling

It is a statistical techniques used to examine and analyse the connection between different variables involved in the research dataset. SEM used the combination of multiple regression analysis and component analysis to check the linkages that complicated casual where matrices were derived (Rodger et al., 2019). The dataset used to conduct the research represents various aspects of financial systems where cryptographic implementation has been executed. The dataset assumptions and consideration covers end-user understanding and experience, impact on productivity of the system workflow, ease of integration and implementation and perceived security of the encryption technique.

The dataset variables used to conduct the study are the following:

Independent variables: the independent variables include the scale of implementation of encryption technique, the type of cryptographic technique used (covering symmetric vs. asymmetric encryption) and training level (knowledge transfer) provided to each end-user.

Dependent variables: the dependent variables include the factors which are impacted as a result of cryptographic solution implementation i.e., end-user satisfaction, perceived level of security of the technique and the impact on productivity of the system workflow.

Models are required to be developed under SEM analysis to describe the variables relationship between them. For example, one of the model:

*End-user satisfaction = α * Scale of Implementation + β * Perceived Level of Security + Υ * Training Level*

Where, the strength of each relationship is represented by the coefficients α, β and Υ.

Matrix analysis and structural equation modeling together offer a solid scientific basis for evaluating cryptographic algorithms and their uses in financial recording systems. The utilization of this method examines every angle of cryptographic techniques ranging from theoretical basis to real world implementation in the financial sector. The use of SEM to study and examine the correlation between perceived level of security and cryptographic technique were studied in related work and a similar method was used to examine the integration of advance encryption techniques for protecting sensitive financial data (Mashatan et al., 2022).

User satisfaction with enhanced security measures in banking systems was analyzed using descriptive statistics and SEM, highlighting key findings in the field (Li et al., 2021). Furthermore, the impact of cybersecurity measures on the productivity of financial services firm workflows was examined through matrix analysis (Shah and Shah, 2023). When applying SEM to assess the efficiency of cryptographic techniques on financial data and systems, definition of dependent and independent variables is very crucial considering these are fundamental to understanding the dynamics of cryptography implementation and its broader effects.

The independent variables are selected considering the underlying importance related to the study. The variable “type of cryptographic technique / method” depicts the application of encryption technique such as hashing algorithms, symmetric encryption and asymmetric encryption. The cryptographic techniques mentioned have unique characteristics which impacts the underlying effectiveness and flexibility of these technique during financial data protection. The variable "Scale of Implementation" assesses the extent of integration of cryptographic approaches with financial systems using sensitive data, from partial use in some sensitive areas to full deployment throughout all processes. It covers the ease of integration from both technical and functional aspects. The variable "Level of Training Provided" assesses the quality and quantity of training offered to users of financial systems, including the depth of information regarding cryptography methods and the frequency of training sessions. The variable "Regulatory Compliance" assesses the extent to which the application of cryptographic methods conforms to pertinent data protection rules and implications of advance encryption techniques integration with financial systems, such as Health Insurance Portability and Accountability Act (HIPAA) or GDPR. The variable "Technology Infrastructure" evaluates the capability of current digital and IT systems to efficiently support and incorporate cryptographic technology.

The dependent variables covering variable “Perceived Level of Security” which provides an overview of an end-user thinking that their data is secured to what extent due to the application and integration of cryptographic techniques. User’s perception of security regarding their sensitive financial data is very important and cognizant to check the impacts and effectiveness of encryption techniques. The "User Satisfaction" variable assesses users' general satisfaction with the cryptographic implementation, accounting for elements like usability and workflow impact. The impact of cryptographic techniques on the speed and effectiveness of financial procedures is measured by the variable "Workflow Efficiency." The variable "Incidence of Security Breaches" tracks how frequently and how seriously security incidents or data breaches occur once cryptographic safeguards established, integrated and implemented with financial systems for data protection. Finally, the variable "Compliance with Regulations" depicts on how much cryptographic methods support in making sure financial procedures follow relevant data protection rules and regulations.

3.2 Data

The study utilizes the combination of secondary and observational data to examine cryptographic techniques efficiency and effectiveness in protecting the financial data. Key variables like the scope of the deployment of cryptographic techniques, user satisfaction, workflow efficiency, and regulatory compliance are captured by the observational dataset, which has been synthesized to match real-world implementation scenarios. Secondary resources[2] were also analysed in this study to use labelled network traffic data covering the malicious and benign flows, which enables the evaluation of cryptographic techniques impact on mitigating specific cyber threats such as denial-of-service attacks (DDoS) and reconnaissance. Secondary data is only used for re-affirmation of encryption techniques impact on protecting the financial data. Majorly observational data has been utilized for conducting the research.

Parameter / Variable	Mean	Standard Deviation	Min	Max
Cryptographic Techniques – Types	2.60	1.10	1.00	5.00
Scale of Implementation	3.40	1.40	1.00	5.00
Level of Training Provided	3.20	1.00	1.00	5.00
Regulatory Compliance	4.30	0.70	3.50	5.00
Technology Infrastructure	3.60	1.20	2.00	5.00
Compliance with Regulations	4.60	0.60	4.00	5.00
Perceived Level of Security	4.10	1.00	2.50	5.00
User Satisfaction	3.90	1.10	2.00	5.00
Workflow Efficiency	3.50	1.30	2.00	4.50
Incidence of Security Breaches	2.20	1.60	0.00	5.00

Table 1: Descriptive Statistics

In the table 1, the variables “Regulatory Compliance” and “Compliance with Regulations” have high mean scores (4.30 and 4.60) indicating adequate compliance with rules and regulations in cryptographic practices. On the other hand, the comparatively high standard deviation and lower mean of "Incidence of Security Breaches" i.e., 2.1 points to variation in the frequency of

[2] Public secondary data sources such as UNSW-NB15.

breaches, highlighting the continuous difficulty in cybersecurity implementation across different setups and environment.

4 Results and Implementation

The study covers the use of matrix analysis to examine the efficiency of various cryptographic methods. The encryption matrix E for a substitution cypher with a shift of 3 can be depicted as:

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

The non-linearity and diffusion properties were demonstrated by the ciphertext noticeable change when the plaintext was slightly modified (for example, by changing the first letter). The input and output bits have no linear correlation between them which makes it non-linear. The study mainly emphasized on the Hill Cypher which proves to be more effective in protecting the financial data within financial systems from cyber-attacks and threats. Although, Hill Cypher is more complex, advance and sophisticated over substitution cypher considering that it provides more relevant and adequate example of cryptography matrix operations. Hill Cypher through this can be depicted by 2 * 2 matrix which is a basic but more complicated and complex category or form of substitution cypher. Encryption matrix E can be depicted as:

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

The matrix above is utilized to encrypt 2 letter blocks of plaintext, then it is divided into 2 letter blocks. The letters are represented each with a number such as A=1,…..,Z=25). Each block is then multiplied by the matrix E with modulo 26. An example of encryption covering '*IJ'* i.e., I = 8 and J = 9 with a vector presentation:

$$P = \begin{bmatrix} 8 \\ 9 \end{bmatrix}$$

The application of operation can be presented:

$$\mathrm{C} = E \times P mod\ 26 \begin{pmatrix} (3 * 8\ + 2\ * 9)\ mod\ 26 \\ 5\ * 8 + 7 * 9\ mod 26 \end{pmatrix} = \begin{pmatrix} 16 \\ 25 \end{pmatrix}$$

The encryption of the message "IJ" results in the ciphertext "RX." This transformation process, governed by matrix multiplication and modular operations, ensures that even small alterations in the plaintext cause significant changes in the encrypted output, supporting the property of diffusion. The encryption's complexity is heightened by the nonlinear nature introduced through modular arithmetic, making it much harder to decipher without knowledge of the encryption key. This makes it extremely challenging to reverse-engineer the encryption, especially when larger matrices are used or when the key remains undisclosed, effectively securing the data. By applying these ideas to digital signatures and cryptographic hashes, which use matrix operations in their algorithms (as per RSA encryption), the validity and integrity of data are guaranteed. The Hill cipher must balance robust security with computational performance in order to be used in financial systems.

Data security and volumes requirements may be aligned with the customization and scalability to multiply encryption keys and block sizes. The examination of matrix-based methods within the Hill cypher and their role in cryptography illustrates their efficacy in preserving data

security, confidentiality, and authenticity. These factors are vital components of cybersecurity, particularly when managing financial information within financial and accounting frameworks. The Hill cypher serves as a foundational example of how matrix operations can be utilized in the design of secure, scalable, and efficient cryptographic mechanisms, crucial for safeguarding sensitive financial data in various applications.

4.1 SEM Analysis Outcome

Table 2, shows that the cybersecurity solutions covering financial systems and sensitive data are impact by many variables.

Predictor	Coefficient (β)	Standard Error	p-value
Type of Cryptographic Techniques	0.21	0.06	0.032
Scale of Implementation	0.31	0.07	0.018
Level of Training Provided	0.40	0.05	<0.01
Regulatory Compliance	0.48	0.06	<0.01
Technology Infrastructure	0.11	0.05	0.48

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

As evidenced by its low p-value (<0.01), the variable which is the most significant is "Regulatory Compliance," that has a coefficient of $\beta = 0.48$, indicating that cybersecurity efficacy is greatly increased and impacted by adhering to regulatory rules and regulations governing the implementation of encryption techniques. "Level of Training provided" comes next, with a β value of 0.40, emphasizing how important comprehensive training is to a successful cybersecurity deployment for a financial services firm. The significant positive effect of the "Scale of Implementation" ($\beta = 0.31$) indicates that better outcomes can be derived when more cybersecurity measures are implemented and there is flexibility to customize and enhance as per security needs. Even though the "Type of Cryptographic Technique" and "Technology Infrastructure" have moderate coefficients (0.21 and 0.11, respectively), they both have statistically important roles to play in the overall cybersecurity methods and approach. To protect financial data, cybersecurity in the financial sector requires a comprehensive approach that includes investment in technical infrastructure, regulatory compliance, implementation scale, and training. The following variables have lower p-values and are statistically significant, according to the regression analysis and the resulting conclusion. Results based on cha are excluded using regression..

The chosen cryptographic approaches showed sufficient diffusion and non-linearity properties, which are necessary for protecting financial data based on the matrix-based operation of the techniques. The SEM study demonstrated strong relationships between the implementation strategies of cryptographic techniques and their perceived effectiveness and user happiness. According to the strong correlation between regulatory compliance and perceived level of security, following the regulatory rules and regulation is not only the morally correct thing to do from a statutory perspective, but it also increases public trust in the security mechanisms in place within financial systems. The regression analysis findings indicate that extensive deployment and intensive training are necessary to maximize the benefits of cryptographic techniques in financial systems.

Parameters Index	Value	Acceptable Threshold
Root Mean Square Error of Approximation (RMSEA)	0.06	< 0.08
Comparative Fit Index (CFI)	0.96	> 0.90
Tucker-Lewis Index (TLI)	0.92	> 0.90

Standardized Root Mean Square Residual (SRMR)	0.05	< 0.08
Chi-Square (x^2)	119.54	
Degrees of Freedom	81	
x^2/df Ratio	1.55	< 3

Table 3: Model Fit - SEM in Cryptographic Implementation

The findings of a comprehensive evaluation of the model fit for the SEM, which was utilized to ascertain the impact of financial cryptography, are depicted and presented in Table 3. The x^2/df Ratio, given a Chi-Square (x^2) value of 119.54 and 80 degrees of freedom it is 1.55. This ratio, which is much below the third acceptable cutoff, indicates that the predicted model matches the data well and that the underlying connections are accurately represented by the model. The Root Mean Square Error of Approximation (RMSEA) value of 0.06 is significantly less than the upper limit of 0.08, which further supports the model's sufficiency. This score is important because it demonstrates that the model adjusts for the complexity of the model by fitting the data well without over-optimization.

The TLI and CFI both have values of 0.96 and 0.92, respectively, which are higher than the lowest acceptable cutoff of 0.90. Taking into account the quantity of variables and the complexity of the model, these indices show that the model fits the data quite well. Moreover, the Standardized Root Mean Square Residual (SRMR) value of 0.05 below the requirement of 0.08 confirms the model's quality of fit and proper. When the SRMR value is low it indicates minimal residual variances and covariance, the model effectively captures the relationships between the variables. Lastly, the indices demonstrate that the SEM model provides a reliable and accurate framework for analysis, making it a good fit for this research's assessment of cryptographic techniques in the financial sector for data protection.

The robustness of SEM analysis is depicted and presented by Sensitivity Analysis in Table 4. Notably, when trained with a 25% higher degree of detail, the model retained an almost comparable fit, indicating a solid basis for analysis. The model's stability even after more intense training and stress scenario suggests that it can adapt to variations in training quality and intensity. This emphasizes how crucial training is as a research variable. Additionally, the model demonstrated robustness when the implementation size is altered or increased. A ±20% shift only resulted in a little increase in the x^2/df ratio, demonstrating that the model effectively captures the impact of varying implementation sizes on cybersecurity efficacy and its integration with financial system. This feature is crucial because it replicates real-world situations in which various accounting firms might apply encryption to wildly varying degrees.

Scenario	**Change in Variables**	**Model Fit Impact**	**Observations**
Training Increase	Training Level ± 25%	Minimum Change	Robust model, stable outlook
Implementation Scale Variation	Scale of Implementation ± 20%	Slight Increase	Resilient model
Changes in Regulatory Environment	Regulatory Compliance ± 15%	Slight Decrease	Sensitive model

Table 4: Sensitivity Analysis Results

As per Table results, every time regulatory compliance variable is changed by ±15%, the Comparative Fit Index (CFI) decreased slightly, indicating that the model is fairly sensitive to such regulatory changes. This sensitivity demonstrates significant influence that regulatory compliance has on the model overall, which is an important finding and observation. It illustrates how financial data protection cryptographic techniques can be impacted by shifts in the rules and regulations, emphasizing the necessity of financial procedures that are adaptive to new rules.

The sensitivity analysis in table 4 shows that SEM model used is resilient, stable and strong. However, at the same time it points to the vulnerabilities in the model due to modifications and alterations. Route analysis offered further insights by demonstrating the related (direct and indirect) impact on dependent variables from independent variables. Consider the ways in which technology infrastructure enhanced users' perceptions of security and, indirectly, their satisfaction with the system through increased workflow productivity. According to a mediation research, user comprehension and satisfaction mediate the relationship between training level and regulatory compliance. As a result, adhering to regulatory criteria depends on customer satisfaction. Examples of latent variables that were correlated include customer satisfaction and perceived security level. Positive correlation in these variable indicates that higher levels of user satisfaction are typically linked to better levels of perceived security. This study may prove to be helpful for future work and research based on these findings relates to cryptographic implementation and dynamics.

Independent Variable	Dependent Variable	Path Coefficient	p-value	Confidence Interval
Type of Cryptographic Technique	Perceived Level of Security	0.23	0.032	[0.2, 0.4]
Scale of Implementation	User Satisfaction	0.27	0.03	[0.05, 0.45]
Level of Training Provided	Compliance with Regulations	0.38	<0.01	[0.2, 0.5]
Regulatory Compliance	Incidence of Security Breaches	-0.42	<0.01	[-0.6, -0.2]
Technology Infrastructure	Workflow Efficiency	0.33	0.03	[0.1, 0.5]

Table 5: Predictor Impact Analysis

Table 5 confidence intervals and predictor impact analysis display the range of these relationships, and the path coefficients measure each predictor's impact. P-values indicate how statistically significant the variable are in data. With a path coefficient of 0.23 and a p-value of 0.032, the type of cryptographic technique and the perceived level of security are positively and statistically significantly correlated. It appears that consumers' perceptions of data security are directly impacted by the encryption method they select or perceive is more secure. The confidence interval [0.1, 0.3] further illustrates the moderate level of conviction about this influence. The implementation scale and user satisfaction have a positive link, as indicated by the path coefficient = 0.27, which is significant at the 0.03 level. This connection demonstrates the significant influence that cryptographic approaches have on raising customer happiness, with a confidence range of 0.05 to 0.45. A strong positive correlation (path coefficient = 0.38, p-value < 0.01) has been found between the level of instruction and regulatory compliance

variable. The confidence interval of [0.2, 0.5] suggests that more comprehensive and enhanced training could significantly increase accounting regulatory compliance.

A noteworthy finding in the results shows incidence of cyber and other breaches is inversely correlated with regulatory compliance (path coefficient = -0.42). The incidence of security breaches and regulatory compliance are strongly correlated, as seen by the [-0.6, -0.2] confidence interval. At a threshold below 0.01, the association is statistically significant. Technology infrastructure has a positive and statistically significant impact on workflow productivity, as indicated by the path coefficient of 0.33 and p-value of 0.02. The confidence interval of [0.1, 0.5] indicates that robust technical infrastructure significantly enhances the efficiency of cryptographic algorithms. In summary, these findings underscore the intricate relationship between method selection, training, regulatory compliance, and the application of cryptographic techniques in the financial industry for safeguarding sensitive financial information. The research provides valuable insights both qualitative and quantitative to cyber and Information Technology (IT) practitioners, experts, standards and policymakers in establishing comprehensive data protection guidelines and processes in the financial sector.

5 Discussion and Evaluation

The paper thoroughly reviewed and examined cryptographic techniques for enhancing financial system cyber defence using SEM and matrix analysis. Matrix analysis, as demonstrated in the study using the Hill cipher, shows how effective cryptographic techniques are in safeguarding private data, which is crucial for the safety of connected financial data. This is consistent with the fundamental requirements of data encryption for safeguarding sensitive financial information due to the intrinsic dispersion and confusion characteristics of cryptographic systems. Using cryptographic techniques increases customer satisfaction, perceived level of security, and regulatory compliance. According to the research findings, the effective use of cryptographic technology enhances stakeholder trust, data security, and regulatory compliance all of which are crucial in the financial sector. Although a balanced strategy is required for financial services firms to have the best cyber security, the research also point out the challenges of putting these techniques into effect, particularly with regard to technical infrastructure and training.

The importance and utilization of cryptographic techniques for protecting sensitive financial data in financial sector is highlighted as a positive impact on cybersecurity space which aligns with results of this study (Smith and Dhillon, 2020). Important information and insights is provide in the thorough analysis of IMF budgeting techniques for the future. The study examines the notion that budgeting is a crucial management tool by examining more than 27 work that are related and applying techniques including synthesis, analysis, and forecasting. Both decentralized management and the application of state-of-the-art technologies to enhance financial institution supervision models are highlighted. Effective budgeting relies on having adequate funds, knowledgeable professionals, and an understanding of why non-productive spending need to be minimized (Nurgaliyeva et al., 2022). The research produced adds significantly to our understanding of future financial management techniques. Our research highlights the importance of adequate infrastructure and training, which is consistent with the findings of previous work conducted (Kumar et al., 2021). Cybersecurity measures implementation require robust resources and funding.

Using advanced cryptographic techniques such as asymmetric encryption and blockchain technology, this study looks at ways to significantly improve the security of sensitive financial information / data. This perspective aligns with research showing that advanced techniques could offer greater security and transparency (Dong et al., 2023). The success of cryptographic techniques is well acknowledged, as noted in the great work by (Qadir et al., 2023). The more complex matrix-based analysis provided by this study, however, expands the debate and justifications for further research. A more thorough understanding of cyber protection in financial systems is provided by this method, which explains not only the technical aspects of cryptographic security but also its wider ramifications on user satisfaction and regulatory compliance. This study provides additional evidence for the significance of cryptographic techniques in maintaining data integrity throughout processing with homomorphic encryption which aligns with research conducted by (Zhao et al., 2020), this study demonstrates the growing popularity of user-centric cryptography solutions in the financial sector. In contrast to the generally technical-centric approach in cybersecurity literature, the evolving emphasis is essential to the practical application of these technologies in real-world financial system scenarios. In sectors such as accounting and finance, where efficiency is equally as crucial as security, this shift reflects a broader trend in cybersecurity toward a more delicate balance between the two. User experience is part of this.

New research avenues on the potential incorporation of emerging encryption technologies, including quantum cryptography, into financial sector are clarified by this study. The related work who looked into how new technology impacts financial system cybersecurity, are consistent with this study. Additionally, as demonstrated by the case studies, the real-world challenges associated with implementing cryptographic techniques underscore the necessity of strategic planning and resource allocation (Kapoor et al., 2023). Finally, by providing a comprehensive evaluation of the function and influence of cryptographic approaches on financial systems cyber defences, our study appropriately adds to the existing body of information.

The research conducted also emphasizes on the need of continuous analysis and study to stay ahead of complex and emerging cyber threats related to financial systems.

6 Conclusion and Limitations

This study emphasizes how cryptographic methods can be used in a variety of ways to improve the cyber security of financial data in financial operations. It highlights that the efficacy of matrix analysis and SEM approaches in protecting sensitive data through the results. This fundamental knowledge of encryption emphasizes how important it is to improving security. Additionally, a strong positive correlation has been shown between the employment of cryptographic techniques and important variables including user happiness, perceived level of security, and regulatory compliance. These results highlight the significant influence these methods have on financial operations, strengthening data security, supporting regulatory compliance, and building stakeholder trust. However, the study did highlight some of the challenges associated with implementing these strategies. Among these are the necessity of adequate training, a solid technological base, and the delicate balance between ensuring effectiveness and use while maintaining a high degree of security. Financial services companies should take a strategic approach to deployment in light of these challenges, emphasizing the selection of appropriate encryption technologies and making sure they integrate seamlessly with existing systems. If businesses wish to realize their full potential, they must invest significant resources in educating their staff about the importance and appropriate application of cryptographic measures. The study highlights the need to uphold recent legislative developments and ethical concerns in data protection in order to guarantee that cryptographic solutions are both compliant and ethically sound.

Future researches may get significant ideas and knowledge in a number of areas by this study. Researching more advanced encryption methods, like algorithms that are resistant to quantum computing, is becoming more crucial given the ever-changing nature of cyber threats and the development of quantum computing. Studies that concentrate on developing cryptographic solutions with the customer in mind are also crucial. These solutions must mix usability and security because all users in a financial environment require them to be effective and accessible. Case studies of successful implementation, the difficulties in incorporating cutting-edge cryptographic algorithms into well-established financial systems, and practical solutions to these problems are examples of potential study subjects.

Moreover, the evolution of cryptographic technology is accompanied by changes in the regulatory landscape. It is crucial to continuously evaluate how new data security laws may affect the application of cryptographic methods in finance. Another important area of study is how to make financial systems more efficient without compromising security, as well as how the use of cryptography affects workflow productivity. The findings emphasize how important it is to continuously mitigate new cyber threats and establish policies to implement them. Confidential financial data protection techniques will need to advance in parallel with cybersecurity technologies. Cybersecurity is crucial to modern financial procedures since, in the digital world, it ensures both security and compliance.

7 References

1. 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), pp. 1631.
2. Abdel-Rahman, M., (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. *Eigenpub Review of Science and Technology*, 7(1), pp. 138-158.
3. Aldboush, A. and Ferdous, M.S., (2023). Encryption and regulatory compliance: A double-edged sword for financial institutions. *Journal of Financial Data Security*, 8(2), pp. 45-59.
4. 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), pp. 90 - 107.
5. Akimova, O., Nataliya, Z., and Buriak, I., (2024). Cyber Protection of Financial Data in Accounting: Implementation and Use of Cryptographic Techniques. *Economic Affairs*, Vol. 69(02), pp. 1041-1052.
6. Anwar, M., Tabassum, N., and Afzal, H., (2022). Quantum-resistant cryptography for financial data: Evaluating lattice-based algorithms. *Journal of Advanced Cryptographic Solutions*, 15(4), pp. 123-135.
7. Arockiam, L. and Monikandan, S., (2013). Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. *International Journal of Advanced Research in Computer and Communication Engineering*, 2 (8).
8. Baliker, C., Baza, M., Alourani, A., Alshehri, A., Alshahrani, H., and Choo, K., (2023). On the applications of blockchain in FinTech: advancements and opportunities. *IEEE Transactions on Engineering Management*.
9. 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.
10. Baliker, M., Youssef, M., and Rashid, H., (2023). Asymmetric encryption in modern financial services: A security analysis of RSA and ECC. *International Journal of Financial Encryption*, 12(3), pp. 87-101.
11. Bokhari, M. and Shallal, Q., (2016). A review on symmetric key encryption techniques in cryptography. *International journal of computer applications*, 147(10).

12. Chandra, S., Paira, S., Alam, S., and Sanyal, G., (2014). A comparative survey of symmetric and asymmetric key cryptography. *International conference on electronics, communication and computational engineering (ICECCE)*, pp. 83-93.
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.
14. Chen, J., Wang, Z., and Li, K., (2022). Post-quantum cryptography for secure financial transactions: A lattice-based approach. *Cryptography and Financial Systems*, 10(2), pp. 78-92.
15. Dhawan, A., Patel, D., and Sandhu, K., (2023). Blockchain and encryption: A new frontier for financial transaction security. *Journal of Financial Technology*, 11(5), pp. 66-80.
16. 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.
17. Gan, Q. and Lau, R.Y.K., (2024). Trust in a 'trust-free'system: Blockchain acceptance in th banking and finance sector. *Technological Forecasting and Social Change*, 199: 123050.
18. George, A.S., George, A.H., and Baskar, T., (2023). Digitally immune systems: building robust defenses in the age of cyber threats. *Partners Universal International Innovation Journal*, 1(4), pp. 155-172.
19. Gulyás, O. and Kiss, G., (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, 219, pp. 84–90.
20. Gulyás, S. and Kiss, A., (2023). Advanced cybersecurity measures in the financial sector: A focus on encryption. *Journal of Banking Security*, 22(1), pp. 35-50.
21. Haapamäki, E. and Sihvonen, J., (2022). Cybersecurity in accounting research. *Managerial Auditing J.*, 34(7), pp. 808–834.
22. 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.
23. Liu, T., Zhang, Y., and Ma, F., (2023). Efficiency comparison of AES and ChaCha20 in financial data encryption. *Journal of Financial Encryption Research*, 18(2), pp. 44-59.
24. 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.

25. Nassar, A., and Kamal, M., (2021). Machine learning and big data analytics for cybersecurity threat detection: a holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, 5(1), pp. 51-63.
26. Navarro, E. and Soler, P., (2023). The impact of data privacy regulations on encryption practices in financial institutions. *Regulatory Compliance and Financial Security*, 9(1), pp. 29-42.
27. 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.
28. Rashid, A. and Omar, S., (2022). Key management challenges in asymmetric encryption for financial systems. *Journal of Cryptographic Key Management*, 7(4), pp. 91-102.
29. 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
30. Rodgers, W., Alhendi, E. and Xie, F., (2019). The impact of foreignness on the compliance with cybersecurity controls. *J. World Business*, 54(6).
31. 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), pp. 404–413.
32. Sajay, K.,, Babu, S., and Vijayalakshmi, Y., (2019). Enhancing the security of cloud data using hybrid encryption algorithm. *Journal of Ambient Intelligence and Humanized Computing*. 20, 1-0.
33. Sajay, Babu, S. and Vijayalakshmi, R., (2019). Hybrid encryption for secure data protection in financial institutions. *Journal of Applied Encryption Techniques*, 14(1), pp. 67-78.
34. Sathya, A., and Banik, B., (2020). A comprehensive study of blockchain services: future of cryptography. *International journal of Advanced Computer Science and Applications*, 11(10).
35. 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.
36. Smith, K.J. and Dhillon, G., (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance*, 46(6): 833–848.

37. Sugumaran, Bala, M., and Kamalraj, (2014). An Architecture for Data Security in Cloud Computing. *IEEE World Congress on Computing and Communication Technologies*, 1 (12), pp. 17 – 71.
38. Twingate Team, (2024). What happened in the Experian data breach? *https://www.twingate.com/blog/tips/experian-data-breach*.
39. 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), pp. 243–266.
40. Zhou, Q. and Wang, T., (2021). Multi-party coputation and its role in securing financial collaborations. Journal of Financial Data Collaboration, 16(3), pp. 112-126.
41. 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.