Exploring the Impact of AI-Based Cyber Security Financial Sector Management

Shailendra Mishra

Special Issue
Advanced Applications of Artificial Intelligence, Data Analytics and Soft Computing

Edited by
Prof. Dr. Chihhsuan Wang
Exploring the Impact of AI-Based Cyber Security Financial Sector Management

Shailendra Mishra

Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Al Majmaah 11952, Saudi Arabia; s.mishra@mu.edu.sa

Abstract: Cyber threats are attempts to secure unauthorized access to, change, or delete private information, to demand money from victims, or to disrupt business. Cybercrime includes everything from identity theft, malware threats, email and online fraud, to bank fraud. Businesses and individuals use this method to guard their data centers and other digital systems. The lack of scalability, sluggish response times, and inability to spot advanced and insider threats are among some of the problems with conventional approaches to network security. These flaws highlight the need for research to build more efficient and all-encompassing security methods to guard against the expanding variety of network attacks. Cybercriminals use AI and data poisoning, as well as model theft strategies to automate their attacks. A cyber security technique based on artificial intelligence is presented in this study for financial sector management (CS-FSM). In order to map and prevent unexpected risks from devouring a business, artificial intelligence is one of the best technologies. Using the proposed technique, cyberattack problems can be classified and solved. To ensure the security of financial sector information, algorithms such as the Enhanced Encryption Standard (EES) encrypt and decrypt data. By learning from the training data, the K-Nearest Neighbor (KNN) algorithm produces predictions. In the financial sector, it is used to detect and stop malware attacks. The proposed method increases cyber security systems’ performance by increasing their defense against cyberattacks. CS-FSM enhances data privacy (18.3%), scalability (17.2%), risk reduction (13.2%), data protection (16.2%), and attack avoidance (11.2%) ratios.

Keywords: artificial intelligence; enhanced encryption; financial sector; cyber security

1. Introduction

Organizations, communications, applications, objects, and information are protected from cyber threats by cyber security disciplines, systems, and procedures [1]. By preventing unauthorized access to resources, systems, and technologies, cyber assault risks are reduced. Innovating society through the Internet of Things (IoT) is a promising paradigm for the future [2]. In order to protect their clients’ money, banks need to employ a cyber-risk management strategy [3]. Due to its wide variety of opportunities for gain, including intimidation, robbery, forgery, and political and philosophical influence, the financial industry is a target for hackers and advanced persistent threats [4]. As stated in the abstract, this study’s proposed method is an AI-powered cyber security strategy that makes use of the K-Nearest Neighbor (KNN) algorithm and the Enhanced Encryption Standard (EES) cipher and decryption algorithm. The abstract provides support for this approach by elaborating on the necessity for more effective and comprehensive security solutions to prevent the proliferation of network assaults using AI and data poisoning. The proposed approach is offered as a means to improve the efficiency, privacy, scalability, risk reduction, data protection, and attack avoidance ratios of cyber security systems, as well as to better categorize and address the problems associated with cyberattacks. Therefore, the description elucidates the rationale for employing the proposed method and the advantages it may bring to management in the financial sector.
When a customer’s personal information is compromised, it can quickly spiral out of control. As a result, banks and financial institutions place a greater emphasis on cybersecurity due to the sensitive information they store for their customers [5]. Protecting customer assets is the most obvious argument for cybersecurity in banking activities [6]. As customers increasingly forego using cash, more transactions are being conducted via internet checkout pages and physical credit scanners. Consequently, customers and other banking firms have stopped believing in it [7]. Banks use encryption software to protect their digital interactions and private details from hackers [8].

A computerized security program keeps computers safe from attacks from the outside world so that their privacy, reliability, and authenticity are not compromised. A network intrusion presents a threat to the target server’s and the network’s capabilities. A network administrator may respond when an Intrusion Detection System (IDS) detects an intrusion. Internet mistrust has increased in parallel with the regularity of cyberattacks. A successful security attack is a Denial of Service (DoS) attack. When discussing the potential effects of AI-based cyber security on the management of the financial sector, the term “security program” is used to describe a comprehensive set of strategies, policies, procedures, and tools developed to protect sensitive data and critical systems from unauthorized access, use, disclosure, modification, and destruction.

Risk analysis, threat modeling, vulnerability management, incident response preparation, access management, data security, network segregation, monitoring, and reporting are all typical parts of such a program. When properly implemented, a security program may protect an organization from cyber threats, quickly respond to security incidents, limit losses and downtime, and guarantee adherence to all applicable rules and laws. The automation of routine processes, real-time threat intelligence, and improved decision-making speed are a few ways in which AI-based cyber security solutions improve the efficacy and efficiency of security programs.

In addition to the aforementioned, banks use security features and routers to safeguard their servers and data. Protective features such as OTP confirmation, ATM validation, and pre-enrollment with ATM or signatory authorization are available [9]. Using reduced internet devices, all interactions are conducted via a highly secure and encrypted medium, ensuring complete security from the consumer’s point of origin to the end of the destination [10]. Account holders are often compensated with a fixed interest rate for lending their money to banks. The banks earn from the financial performance of commercial banks by making loans to customers at a fixed interest rate [11]. A group’s revenue, flexibility, productivity improvement, and stability can all be gleaned by analyzing its financial measures. Contrasting one organization against another in the same industry or market, ratio analysis can show how a team changes through time [12].

When spotting malicious activity on the Internet, AI can be a helpful tool. Malware and ransomware assaults can be detected in their earliest stages by AI technologies programmed to recognize patterns and to recognize even minor behaviors [13]. With AI, businesses will free up staff while increasing security and ensuring they are headed in the proper technologically sophisticated, inventive direction [14]. Recently, more precise software invention forecasts, automated trades, database administration, poverty alleviation, and new ethical concerns have all been discussed in regard to how artificial intelligence can be applied in finance [15].

Artificial intelligence is more challenging and has a higher job population than cyber security, yet both are equally critical [16]. Cyber security increasingly depends on artificial intelligence (AI) [17]. AI may be utilized for cybersecurity solutions such as spam filtering, malware detection, fraud prevention, creditworthiness, and hacking incident predictions, to name a few [18]. Artificial intelligence (AI) is becoming highly relevant in cybersecurity to combat cyberattacks; the market is predicted to grow at a compound annual growth rate [19]. For effective management of cyber security risks in the financial sector, look no further than the Cyber Security in Financial Sector Management (CS-FSM) approach. This model offers financial organizations with a framework for creating and enforcing robust
security plans, policies, and procedures against cyberattacks on their systems, data, and clients. The foundation of the CS-FSM model is the recognition that cyber security is an essential part of the management of financial institutions.

Risk management, governance, security operations, incident response, and regulatory compliance are only some of the primary areas of emphasis in the CS-FSM paradigm. In order to formulate a strategy for managing risk, financial institutions must first determine what resources are most important to the institution and what threats those resources face. In order to govern effectively, it is necessary to define roles and duties, develop rules and procedures, and keep these documents under constant review and revision. Firewalls, encryption, and other forms of access control are only some of the technical measures that can be implemented as part of a security operation. The goal of incident response is to have a plan in place to deal with cyberattacks as soon and efficiently as possible.

A significant amount of points that are involved in cybersecurity can benefit from artificial intelligence because AI is all about data clustering, classification, and analysis [20]. While artificial intelligence (AI) is a powerful concept, it cannot be set up and run independently [21]. For this definition, “artificial intelligence” means a computer’s ability to act intelligently independently and independent of human input. Thus, AI security is about using AI to identify and stop cyber threats with little involvement than conventional security methods are usually assumed or required. The suggested CS-FSM framework has been adapted to the financial industry with the goal of enhancing data security, privacy, and risk mitigation. Financial institutions confront a unique set of cyber security concerns, and the researcher’s strategy is designed to help them meet those challenges head-on. Financial organizations that deal with large amounts of sensitive data might benefit greatly from the employment of the Enhanced Encryption Standard Technique (EES) and the KNN algorithm for more effective prediction and prevention of cyberattacks [22].

Although this model has been created with banking in mind, it has potential for use in other areas of network safety as well. The CS-FSM model’s use of AI techniques such as the KNN algorithm can be generalized to boost cyber security in various sectors. One size does not fit all when it comes to cyber security; different sectors face different threats and have different needs. Therefore, prior to adapting this model or its underlying algorithms for use in other sectors, it would be necessary to conduct extensive research into those sectors’ unique requirements and cyber security hurdles [23].

It has been noteworthy to see the amount and diversity of network attacks increase in recent years, despite a lot of research in this field [24]. As a result of AI-powered systems decreasing the number of wrongful convictions, security professionals can allocate resources better. Financial institutions can use innovative surveillance footage to watch numerous places with a small staff of faraway analysts [25]. Cyber threats can bring down entire corporate networks and access confidential data, even if high-tech security protocols and systems protect those networks. Various types of attacks can be carried out on the Internet of Things due to vulnerabilities. Additionally, security issues such as confidentiality, privacy, and accessibility pose a threat to important information [26].

The researcher’s main contributions to this research work are as follows:

- The researcher developed a Cyber Security in Financial Sector Management (CS-FSM) model, with the help of artificial intelligence, to analyze all the intrusions.
- The proposed CS-FSM method is formed to find the black holes in the cyber security system.
- The proposed CSFM model is compared with other existing approaches to validate the results.
- The researcher compared the risk reduction ratio with the existing approach.
- The results of the tests, carried out using effective systems based on the proposed methodology, show a significant improvement in data security.

The remainder of the paper proceeds in this manner: Section 2 discusses background information on cybersecurity and artificial intelligence. Section 3 presents the artificial intelligence approach to Cyber Security in Financial Sector Management (CS-FSM). A
mathematical model and analysis are shown in Section 4, and a conclusion and future scope are illustrated in Section 5.

2. Related Work

Cyberattacks have been prevented in many studies by securing data, money, and other valuables from hackers. In order to fill in the gaps left by previous studies, this study was conducted, the results of which are summarized below.

Brunner et al. examine the present status of risk management strategies used in the region’s Information Security Management System (ISMS) (Germany, Austria, and Switzerland) [27]. The research obtained data from 26 firms using an anonymous online poll targeting strategy, operational data security, and risk management. The research investigates general procedures, documentation artifacts, stakeholder communication patterns, tool categories, and collection methods used by businesses to perform data safety management tasks.

The goal of the Cyber-Physical System (CPS) Ecosystem task is to build an Internet of Things (IoT) architecture that can be used to study and teach in a wide range of CPS-IoT-related fields [28]. The main goal is to provide real architecture and allow students and researchers to explore how it could be used in the real world.

Zhang et al. look into whether, and how, the eXtensible Business Reporting Language (XBRL) requirement changes how investors think about the risk of a company going bankrupt in the future [29]. The goal is to learn more about how this important disclosure rule affects the economy. Using the slope of the implied volatile grin as a substitute for ex-ante prediction of accident rates, the research discovers that the projected crash risk decreases after XBRL implementation. The research also shows evidence that the effect is worse for companies with more opaque accounting, volatile earnings, and different analyst estimates.

These concerns also have an impact on cyber Digital Manufacturing (DM) processes. This challenge may be addressed by developing the meta-architecture [30]. In this work, the Explorer tool created by Industrial Engineering and Systems Engineering is used to create a scenario that highlights the worry over a hypothetical banking cybersecurity issue. A conceptual is generated by using the Genetic Algorithm (GA) with a fuzzy assessor as the fitness value to select permutations of defensive mechanism parts.

Al Hammadi et al. describe an insider risk analysis method as a fitness-for-duty safety assessment that integrates Electroencephalogram (EEG) brainwave patterns with Explainable Artificial Intelligence (XAI) and machine learning techniques to categorize anomalous EEG signals suggesting a possible insider danger and assess fitness for work [31]. The system is supposed to be cost-effective by utilizing a five-electrode EEG device from Emotiv Insight. In this investigation, information was obtained from 17 individuals with varying emotional responses.

Cybersecurity Awareness Training Model (CATRAM) looks at a variety of factors related to older people’s desire to learn cybersecurity skills as well as their actual level of cyberspace proficiency [32]. Using a web-based survey and a scenario-based program called MyCyberSkillsTM, Blackwood-Brown et al. examine the components of interest before and during cybersecurity awareness.

Using the fuzzy Decision-Making Trial And Evaluation Laboratory (DEMATEL) approach with neural network prediction, a unique reputation regeneration method is developed [33]. Initially, they use a fuzzy multi-criteria decision-making framework, dubbed the fuzzy DEMATEL technique, to examine the fundamental causal linkages between relevant elements and to find the key success factors for reputation estimation. Finally, the research uses a neural network using backpropagation to generalize the relationships to the original reputation score.

Distributed Denial of Service (DDoS) attacks mess up online services and make digital services less accessible. Singh et al. look at how blockchain technology, one of the newest and most promising new ideas, can be used to protect against DDoS attacks [34]. As a result of its robust, decentralized, and secure design, blockchain technology is quickly...
gaining traction in applications that range from finance to gaming. Blockchain-based DDoS mitigation is still in its infancy, with some systems providing only architecture specifications and ignoring implementation details.

For the sake of the system’s security, Aghili et al. [35] look at a secure and lightweight RFID authentication protocol for Medical IoT (SecLAP) and demonstrate its vulnerability to attacks such as secret exposure, reader impersonation, and tag tracing. In addition, it cannot guarantee that both the label and the recipient will remain anonymous. Second, the study introduces a new technique for protecting the privacy and security of IoT devices using secure and lightweight reciprocal RFID identification (SecLAP). The SecLAP technique guarantees the privacy of both forward and backward data flow, as shown by the privacy research, and it is resistant to desynchronization, replaying, reader/tag impersonators, and tracing threats.

Protection at all levels requires functional technology-based protection. Using IEC 61850’s Sampled Value (SV) messages, this study designs an intrusion identification solution for smart grids to satisfy this demand [36]. Using artificial intelligence (AI), the technology can analyze the communication flow of a specific power network and differentiate between regular data observations and maliciously inserted data, i.e., assaults.

This research presents KiRTi, a deep-learning-based payment system for public blockchain, to enable smart lending activities between Potential Borrowers (PB) and Potential Lenders (PL) to eradicate the requirement to use third-party Credit Rank Agencies (CRAs) for Credit-Score (CS) creation [37]. Consequently, PB receives secured, approved, and computerized loan grants from PL to speed up the distribution procedure. On a blockchain network, KiRTi records its past transactions, financial assets, and obligations as time-series declarations to that effect. A Long-Short-Term Memory (LSTM) system retrieves sequencing information from the blockchain and provides CS for loan suggestions based on suggested lending methods for PB and PL.

The rise of cyberattacks, which target the weaknesses of networked devices, has had a negative effect on the productivity of businesses in the manufacturing sector, prompting the introduction of Artificial Intelligence-Based Cyber Security (AI-CS) [38] by A. J. G. de Azambuja. Attack plans for targeted cyberattacks are evolving and becoming more sophisticated all the time, with an emphasis on the use of artificial intelligence in their implementation. In order to help the research community better prepare for future risks, this study will analyze the relevant literature to better understand the effects of this new danger. The findings can be used to direct the analysis of AI-backed cyberattacks.

The study found that the privacy, scalability, risk reduction, data protection, and attack avoidance ratios of several existing ISMS, CPS-IoT, XBRL, DM, XAI, and CATRAM technologies must be improved. As a result, this research proposes the CS-FSM model, which can help the finance sector comply with personal data protection. Table 1a shows the research gap with the state of arts techniques and Table 1b. Previous Findings.

<table>
<thead>
<tr>
<th>Citation</th>
<th>Limitation</th>
<th>Features</th>
<th>Computation Type</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>[25]</td>
<td>Yes</td>
<td>No</td>
<td>Risk management strategies</td>
<td>ML</td>
</tr>
<tr>
<td>[26]</td>
<td>Yes</td>
<td>Yes</td>
<td>Malicious uses of machine learning in the cybersecurity and CPS areas</td>
<td>ML</td>
</tr>
<tr>
<td>[27]</td>
<td>Yes</td>
<td>No</td>
<td>Reducing expected crash risk, Provides insight into data safety management</td>
<td>Statistical</td>
</tr>
</tbody>
</table>

Table 1. (a) Research gap in previous findings. (b) Previous Findings.
<table>
<thead>
<tr>
<th>Citation</th>
<th>Limitation</th>
<th>Features</th>
<th>Computation Type</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>[28]</td>
<td>Yes</td>
<td>Yes</td>
<td>SoS Explorer tool solves banking cybersecurity problem</td>
<td>Genetic Algorithm (GA)</td>
</tr>
<tr>
<td>[29]</td>
<td>Yes</td>
<td>No</td>
<td>Risk assessment system for duty security evaluation Impact of XBRL requirement on economy Determines effect on crash risk</td>
<td>ML and DL</td>
</tr>
<tr>
<td>[30]</td>
<td>Yes</td>
<td>No</td>
<td>Increasing the cybersecurity skill level of the senior citizens</td>
<td>Statistical</td>
</tr>
<tr>
<td>[31]</td>
<td>Yes</td>
<td>No</td>
<td>Reputation System for e-commerce systems Integrates EEG brainwave patterns with XAI and machine learning techniques to categorize anomalous EEG signals</td>
<td>Fuzzy logic</td>
</tr>
<tr>
<td>[32]</td>
<td>Yes</td>
<td>No</td>
<td>Blockchain-based DDoS solutions, Examines factors related to older people’s desire to learn cybersecurity skills</td>
<td>Blockchain</td>
</tr>
<tr>
<td>[33]</td>
<td>Yes</td>
<td>Yes</td>
<td>Radio-Frequency Identification (RFID) based security solutions for MIoT</td>
<td>RFID in IoT</td>
</tr>
<tr>
<td>[34]</td>
<td>Yes</td>
<td>Yes</td>
<td>Intrusion detection system for smart grids, Provides robust, decentralized, and secure design for DDoS mitigation</td>
<td>ML</td>
</tr>
<tr>
<td>[35]</td>
<td>Yes</td>
<td>Yes</td>
<td>Deep-learning-based credit-recommender scheme for public blockchain, Secure and ultralight reciprocal RFID identification (SecLAP) method</td>
<td>Statistical Method</td>
</tr>
</tbody>
</table>

(b)

<table>
<thead>
<tr>
<th>Author</th>
<th>Proposed Technique</th>
<th>Advantages</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brunner et al. [27]</td>
<td>Risk management strategies in ISMS</td>
<td>Provides insight into data safety management</td>
<td>Examined general procedures, documentation artifacts, stakeholder communication patterns, tool categories, and collection methods used by firms</td>
</tr>
<tr>
<td>Zhang et al. [29]</td>
<td>Impact of XBRL requirement on economy</td>
<td>Determines effect on crash risk</td>
<td>Found that the projected crash risk decreases after XBRL implementation</td>
</tr>
</tbody>
</table>
Table 1. Cont.

<table>
<thead>
<tr>
<th>Author</th>
<th>Proposed Technique</th>
<th>Advantages</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al Hammadi et al.</td>
<td>Insider risk analysis method</td>
<td>Integrates EEG brainwave patterns with XAI and machine learning techniques to categorize anomalous EEG signals</td>
<td>Provides a cost-effective method to assess insider danger and fitness for work using a five-electrode EEG device</td>
</tr>
<tr>
<td>[31]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blackwood-Brown et al.</td>
<td>Cybersecurity Awareness Training Model (CATRAM)</td>
<td>Examines factors related to older people’s desire to learn cybersecurity skills</td>
<td>Explored the components of interest before and during cybersecurity awareness using a web-based survey and MyCyberSkillsTM</td>
</tr>
<tr>
<td>[32]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Singh et al.</td>
<td>Blockchain technology for DDoS protection</td>
<td>Provides robust, decentralized, and secure design for DDoS mitigation</td>
<td>Explored the potential for blockchain technology to protect against DDoS attacks</td>
</tr>
<tr>
<td>[34]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aghili et al.</td>
<td>Secure and ultralight reciprocal RFID identification (SecLAP) method</td>
<td>Ensures safety and privacy preservation for IoT devices</td>
<td>Presents a novel method resistant to various attacks and assures the safety of both forward and reverse data flow</td>
</tr>
<tr>
<td>[35]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The main research gap addressed in this proposed work is highlighted below:

An analysis based on both intelligent systems (CPS) and computational methods will be applied to the proposed work.

- The proposed work will have an impact on both computational and CPS-based analysis.
- The developed framework architecture of the proposed CS-FSM model is based on AI and AES.
- The proposed CS-FSM method is formed to find the black holes in the cybersecurity system.
- The proposed CSFM model is compared with other existing approaches.

3. Cyber Security in Financial Sector Management (CS-FSM)

Cybersecurity is necessary to safeguard a system, network, and technology against illegal access. In today’s technologically advanced world, a company must have a dedicated cybersecurity team to monitor potential cyber threats and devise strategies for countering them. Figure 1 depicts the essential elements of cybersecurity. Cybersecurity mainly includes secure payment, the online privacy of the user, an antivirus firewall, mobile security, security padlock, data protection, computer protection, and a specific global shield. For any company that processes electronic payments or transactions, payment security is critical to information security.; keeping abreast of the most recent developments in e-commerce and secure transaction methods, and seeking guidance on implementing them in their business. A cyber security methodology based on artificial intelligence, in particular the K-Nearest Neighbor (KNN) algorithm and the Enhanced Encryption Standard (EES) encryption and decryption algorithm, has been used to accomplish the research’s goals.
Figure 1. Essential elements of cybersecurity in financial management.

Banks must put cyber risk management plans in place to keep their networks safe and safeguard the safety of their consumers. Trust in financial organizations can be eroded by data breaches, which is a big concern for banks. They could lose a large chunk of their consumer base if they have a weak cybersecurity system.

Using Padlock, organizations can connect with independent cybersecurity consultants, have access to on-demand cyber security knowledge, and security measures for mobile devices include laptops, smartphones, tablets, wearables, and other electronic devices that hold and send sensitive data. The principal objective of smartphone safety is to avoid additional entry into the enterprise network. Online privacy refers to an individual’s privacy protection while using the Internet. The level of online security provided protects legal and economic information, conversations, and choices. Data security is the process of preventing the loss, and alteration or tampering with sensitive information. In light of the ever-increasing volume of generated and stored data, it is more critical than ever to safeguard data.

Additionally, there is a low tolerance level for downtime, making it impossible to retrieve vital documents or other data. Data protection aims to ensure that data can be recovered quickly in case of a data breach or loss. Protecting the integrity of data and the privacy of those whose data is being watched are critical considerations in data protection.

Antivirus software protects a computer against viruses by scanning for, detecting, and removing them. Most security software is set up to run in the background and defend from virus attacks as soon as they occur. Users should feel protected from known dangers if they have an antivirus product regularly updated and scanned. Antivirus software is an essential component of a user’s overall cybersecurity hygiene. The fundamental purpose of digital safety, known as cybersecurity, is to take the appropriate actions to prevent networks and information from damage, fraud, and illegal usage. Identification numbers, locking, and sirens protect sophisticated or pricey computer equipment. An intruder on a computer network can be a targeted attacker or opportunistic malware. Software and device security is the emphasis of application security. If an application is hacked, the data it should safeguard could be accessed. Businesses that will not take proper precautions against cybercrime face considerable losses. Regulations are beginning to take note of the rising threat of cyberattacks. Cybersecurity is not addressed explicitly in financial rules and regulations, although securing IT systems for operational assurance, data protection, and correct reporting is often an implied necessity.

Cybersecurity Principles, an introductory security course, covers the basics of information security. It allows pupils to identify information security threats that impact an organization’s security posture and establishes general security policies to protect against
these threats. Secrecy, authenticity, and accessibility are the three pillars of data security. Every aspect of an organization’s information security program (and every security measure it implements) must be built around achieving at least one of these three goals. Identifying and communicating cybersecurity threats is essential in developing a comprehensive cybersecurity approach and program. An entity that behaves or can act in a way that causes or contributes to risk. Professionals such as system development, information, and attackers are all possible risk areas.

3.1. AI in Cybersecurity

Figure 2 illustrates how artificial intelligence is used in cybersecurity. Artificial intelligence’s spam filtering flags inappropriate content in every incoming communication. Malware can be detected due to its ability to learn and adapt.

![Image of AI in Cybersecurity](image)

Figure 2. AI in cybersecurity.

This harmful software is immediately recognized, and users are warned not to open any emails that include it. Utilizing data layering, deletion, and backup storage, companies can protect their software and platform activities through folder security. Encryption, tokenization, biometric verification, and essential control are other options. Protecting a financial institution’s architecture by avoiding a wide range of dangerous threats from entering or spreading within a network is the goal of network security and can be accomplished by way of a collection of approaches. To preserve network safety, users need various types of network security (endpoint, online, wireless) and network security (firewalls, VPN encryption). Behavior analysis uses multiple techniques including machine learning, artificial intelligence, big data, and statistics. Individual behavior is the focus of behavior analysis, a branch of natural science. As a result of their work, behavior analysts try to understand how a person’s or an animal’s biology, pharmacology, and environment influence their behavior. A subset of business intelligence employs machine learning to detect new patterns, discover linkages, and uncover insights. Artificial intelligence is used to automate much of the labor traditionally performed by data analysts.

3.2. Cyber Security in Financial Sector Management (CS-FSM)

The proposed model, Cyber Security in Financial Sector Management (CS-FSM), with the help of artificial intelligence, analyzes all the intrusions and allows individuals to determine when it is safe. Otherwise, it stops the entry and reports to the control room or accessing persons. Figure 3 illustrates the overall systematics of the proposed system.
All the customers’ financial information, banking sector, and other data are stored in the database secured by cyber security. The firewall blocks untrusted entry when one person, client, or threat enters to access those data. Genuine entries are allowed to store the data. These data are encrypted using a private key or a public key. Once encrypted, they will be held in the database, assuring that the data will be safer when cyberattacks happen. Artificial intelligence makes the best prediction model with trusted and untrusted data using the KNN algorithm. This algorithm designs a model based on the information given by authorized persons. After creating a successful prediction model, information access is thoroughly checked. Suppose an unknown entry or a virus tries to use the information stored in the database, in this case, the prediction model will analyze them, stop their entry, and notify the authorized person. The financial data are safer using this proposed model.

![Figure 3. The architecture of the proposed CS-FSM model.](image)

People and organizations can obtain various payment options and products from the financial services industry. Depositors, investment groups, lenders, credit institutions, real estate agents, and health insurers make up this economy sector. Financial and commercial banks cannot share confidential information or execute transactions without a firewall. The Crystal Act of 1933 prohibited banks and brokerage businesses from working together and served as a firewall. In addition, computers can check each packet for malware using comprehensive security techniques. In addition to serving as load balancers, proxies can act as filters, preventing viruses from infecting the web servers they sit next to.

Predictive analytics for private motives, such as production process, marketing and revenue positioning, efficiency and better security, and fraudulent monitoring, are a perfect fit for banks. Resources, debts, ownership, revenue, expenditures, and working capital are all important types of financial data. Obligations are the debts owed by the firm. At the same time, equity is the money that the stakeholders keep after subtracting the value of the business’s liabilities from the value of its assets. All private details are encrypted to prevent cyber criminals from readily obtaining them. The use of encryption libraries and critical recovery services is required for application encryption. At the application level, encryption implies encrypting data before it can be stored and decrypting it when something is retrieved from a database or completely based.

Artificial intelligence can be used to assess consumer and micro-enterprise loan candidates’ default risk. The platform uses investment information and algorithms to identify patterns and determine which applications are excellent or poor. Predictive analytics can help uncover fraudulent activity by studying the most efficient operating ways for transactions, sales, and transactions. Patterns can be discovered by analyzing organized and unstructured data (emails, reviews, and forum posts). The Enhanced Encryption Standard
and K-Nearest Neighbor are the algorithms used for the prediction process. Financial institutions should re-evaluate their present back-office and front-end tools and procedures in secure information as it travels around the organization. They should implement extra verification layers and security systems with multilevel checks to ensure safe transactions across several channels. Banking security is a serious issue in the present day and age. A cybersecurity threat is one of the issues to be aware of. Fraud and other malpractices result from these security vulnerabilities. Every year, more and more people fall victim to bank fraud. The objective of financial safety net programs is to lessen the frequency and consequence of credit crises that have economic consequences. Whether private or state offered, the threat finance sector frequently associated parties without expenditures.

3.3. Enhanced Encryption Standard Technique

EES is not a Feistel cipher but an iterative one. ‘Substitution–permutation network’ is the underlying concept. Many different processes are linked together in this way. Some are simple substitutions of one input for another, while others entail bit shuffles (permutations). Figure 4 shows the transformation of information into the EES model. Clients or authorized persons want to store their data in a safer way so that they cannot be found or stolen; their financial information is encrypted using a security key, which is then changed into a cipher text. The data are stored in the database. Again, the same person can use those data by decrypting the information with the same security key they use to encrypt; in this way, their information is safer from cyberattacks. The financial statements are designed to offer details on an organization’s strategy, financial condition, and profitability, among other things. Readers of financial accounts use this data to understand better how to allocate resources. Network security keys are just another name for the enabled device’s password. To access the communication network, one must enter a network security key, a type of network passcode signature which safeguards a system and its devices from unauthorized intrusions.

![Figure 4. Working of Enhanced Encryption Standard Technique.](image-url)

The financial sector is being held more and more liable for the security, confidentiality, and integrity of private consumer data (NPI). Businesses in the banking and financial services sector can safeguard private information such as client financial records, social security numbers, income, and account numbers by safeguarding nonpublic personal information and personally identifiable information (PII). If unencrypted data are lost after a data breach, an organization may be subject to fines that can reach millions of dollars, in addition to indirect expenses such as diminished brand value, legal fees, and lost business. Nowadays, almost all commercial databases offer some kind of database-level encryption. A clear benefit of database layer encryption is the integration with other database access control services, resulting in fewer security gaps and it is tailored for database speed.

The encryption method may incorporate encryption key management more effectively. Keeping the encryption keys distinct from the data they protect and managing them
throughout their entire lifecycle are two of the key duties of a key management solution. In this study, the researcher used advanced encryption standard (AES) algorithms. The researcher used Python 3.8.10 for this. Python AES offers three distinct key lengths: 128, 192, or 256 bits long, with a fixed block size of 128 bits (16 bytes). Using pycryptodome, we can use AES-128 to encrypt some data, store the data in a file, read the same data again, and then decrypt the data.

3.3.1. Algorithm (Encryption)

Step 1—Import Cryptodome Cipher and Cryptodome from the library.

Step 2—The term “SECRET DATA” indicates that the data in this instance must be in byte form. The prefix “b” or “B” is always used before a byte literal.

Step 3—The function receives random bytes and returns an N-byte random string. N must be 16, 24, or 32 bytes in length since it is 16 bytes (128 bits) in this scenario. The key is here.

Step 4—To generate our cipher, we utilize AES.new(). It requires two arguments: the mode, which is a constant, and the key in bytes, which we defined in the preceding statement. In this instance, MODE EAX is used. Encrypt-then-authenticate-then-translate, or EAX, is a cryptographic block cipher operation mode.

Step 5—The encryption and digest functions of encrypt and digest(). Remember that while a digest is a fixed-size numeric representation that serves as an identifier for the contents of the data, encryption masks the contents of our data. The encrypt and digest method accepts our data and returns a tuple that includes the ciphertext and the message authentication code (MAC), also referred to as a tag that verifies the data’s legitimacy.

Step 6—Finally, we write our encrypted message, along with the tag and a cipher. To ensure that our data are authentic, the cipher. nonce is an arbitrary value that is used just once. For instance, if multiple portions of the same cipher. nonce are utilized.

3.3.2. Algorithm (Decryption)

Step 1—To read the bytes into the file and decode the message, someone would need access to the file. Following that, one would obtain the ciphertext, tag, and nonce.

Step 2—The researcher created the cipher using AES.new() as previously stated, but this time also add the nonce. The key should typically only be accessible to the person who is decrypting the communication.

Step 3—The decrypted data are delivered after one runs decrypt and verify, pass the ciphertext, and tag.

Step 4—Since the data are in bytes, function decode must be used before print() can be used to display the message in the console.

3.4. Prediction

KNN predicts in real-time by comparing the similarities between an input sample and each training example. The input data can be matched with various distance measurements depending on their structure. When utilizing KNN, it is good to normalize or rescale the data. When using KNN to forecast which class test data should be assigned, all learning values are considered. The KNN method determines which class of ‘K’ training data are most likely to contain the test data. During the training phase, it does not acquire any knowledge and does not use the experimental information in any discriminatory way. However, there is no prerequisite training session.

3.5. Date Privacy and Risk Reduction Ratio

When producing real-time predictions, it draws on the training data stored in the system. Whenever it comes to the Internet, since data are a valuable commodity, one way to protect one’s privacy is through data privacy. Finding out who is looking at our online activity and what they plan to do with it is vital to protecting our privacy. Maintaining data security and safeguarding user privacy go hand in hand. Meeting regulatory obliga-
tions, the safe management of critical material, such as personally identifiable information and other personally identifiable information (such as financial and technological market information), is called data privacy. The following equations calculate the data privacy:

$$\log \frac{D_s(s \in \text{range}(N)|P)}{D_s(s \in \text{range}(N)|P')} \leq \varepsilon$$  \hspace{1cm} (1)

$$D_s(N) \equiv \sup \log \frac{D_s(s|r,P_k)}{D_s(s|r,P_k)}$$  \hspace{1cm} (2)

As shown in Equation (1), and $2D_s$ is denoted as the data privacy ratio, $N$ is characterized as the randomized mechanism that takes input $P$ and outputs $s$, $D_s(s \in \text{range}(N)|P')$ satisfies the differential privacy $\varepsilon$, $D_s(N)$ is denoted as data security based on randomized mechanisms, and $P_k$ is denoted as supplied understanding. Based on Equations (1) and (2), the data privacy ratio is enhanced.

A scalable business can raise overall sales while maintaining or improving profitability; in the capital markets, scalability refers to the ability of financial firms to quicken the rate of consumer demands. Buying the stock at lower prices, a strategy known as “scaling in”, allows investors to take advantage of falling equity prices. When a stock falls below a specific price, scaling in is called. If the price continues to slide or the desired deal size is reached, the purchasing will proceed. Scaling a business entails laying the groundwork for the group’s future growth. To be unhindered in one’s growth is what it means to be flexible. Strategy, individual finance, and the correct procedures, employees, methods, equipment, and partnerships are all needed to complete the job. The equation for scalability is given below,

$$S(a) = 1 - Gp - \partial_{n+1} \times (1 - T_d)$$  \hspace{1cm} (3)

As per Equation (3), $S(a)$ is denoted as the scalability ratio, $Gp$ is denoted as the gap between the desired response time, $n$, $\partial_{n+1}$ is denoted as using a value that is one size larger than the existing value to specify the significance difference, and $T_d$ is denoted as a rising trend in reaction times.

$$Gp = \sum_{i=1}^{u} \partial_{2i}G_{2i}$$  \hspace{1cm} (4)

where $\partial_{2i}$ is denoted as between two predetermined values, and $G_{2i}$ is denoted as the gap between two desired times. The scalability ratio is improved as a result of Equation (3).

Risk reduction aims to lessen the chance and magnitude of future liabilities. Due to oil’s geopolitical and default risk, a risk-averse investor considering buying oil equities may decide not to purchase a stake in the company. Medical treatment, emergency responders, nighttime security personnel, sprinklers, and burglar alarms are all examples of risk reduction. An insurance firm or organization can minimize risks by employing procedures that reduce the economic effect of possible losses.

$$QR = \frac{R_r - C_c}{C_c}$$  \hspace{1cm} (5)

In Equation (5), $QR$ is denoted as the evaluation of the quantified risk, $R_r$ is denoted as the risk reduction ratio, and $C_c$ is denoted as costs associated with management.

$$R_r = A_r \times P_t \times L_r$$  \hspace{1cm} (6)

As per Equation (6), $A_r$ accuracy is denoted as a percentage of total measurement, $P_t$ is denoted as a single event’s projected expenses, and $L_r$ is denoted as a decrease in the likelihood of risk. An increase in the risk reduction ratio can be attributed to Equation (6).

In Figure 5, the risk reduction ratio is the multiplication of the accuracy percentage of total measurement, the single event’s projected expenses, and the decrease in the likelihood of risk. Removal is the most effective improvement strategy that may be applied to eliminate
risk from the task. This is the ideal control method because it removes the danger and zero risk, little hazard, and no likelihood of harm.

\[
Q_R = R - C \cdot C = R \cdot A \cdot P \cdot L
\]

\[
P_d = \left( \sum_{j=1}^{t} R_i \cdot A_{i,j} \right) - \left( \sum_{j=1}^{t} R_i \cdot F_{i,v} \right)
\]

As shown in Equation (7), \( P_d \) is denoted as the data protection ratio, \( F_{i,v} \) is denoted as dynamic mass gradient rating based on \( i \) th vector, \( v \) is denoted as gradient rating, \( R_i \) is denoted as a danger made possible by the persistence of a potentially harmful outcome, \( A_{i,j} \) is denoted as the export score, and \( t \) is characterized as the time factor. Equation (7) is responsible for an increase in the data protection ratio.

Avoiding a data leak is the best way to keep the information safe. Cybersecurity technology, a virtual private network, and understanding typical attack methods can help people and organizations keep their data safe from hackers. In many cyber threats, hackers exploit weaknesses in a computer system’s defenses to gain access to the system. It may entail looking for security holes in a website’s code to introduce and circumvent authentication procedures. The following calculations denote the attack avoidance ratio:

\[
A_v = \frac{R_s + H_i}{N}
\]

\[
A_{vc} = A_s + A_v
\]

As per Equations (8) and (9), \( A_v \) is denoted as the attack avoidance ratio, \( R_s \) is denoted as the network node’s primary resource, \( H_i \) is denoted as the location of the host, \( N \) is characterized as the period, \( A_{vc} \) is denoted as the likelihood that the first source will be found, and \( A_s \) is denoted as the likelihood of finding a solution. Due to Equation (8), the attack avoidance ratio improves.
Artificial intelligence (AI) is used in this study to provide a cyber security strategy for the financial sector which helps to reduce the risk of illegal access to a corporate system or network by implementing the necessary networking safeguards. It will help to increase stakeholder involvement in data protection procedures. In the preceding section, it is mathematically derived. In the following section, the results and comments are summarised.

4. Experiments and Evaluation

Experimental results presented in this section are based on the CS-FSM method, and its classification performance is compared with that of other algorithms that provide similar results. This experiment was conducted on an Intel Core i7 computer with 2.84 GHz and 64 GB of RAM running Windows 8 64-bit. The Python 3 emulator was loaded, and the testing network’s susceptibility information was examined using the security program. The network structure data were gathered with the ArcGIS toolkit. The researcher used Python to develop the code for the project. During the course of the trial, the investigation analyzed roughly 250 thousand sets of attack and defense strategies. Matlab 2018a was employed for data analysis and visualization.

Various parameters have been used to evaluate the suggested CS-FSM model, such as data privacy ratio, scalability ratio, risk reduction ratio, data protection ratio, and attack avoidance ratio. It analyzes cyber security data with artificial intelligence, and the Enhanced Encryption Standard (EES) secures and decompresses data to keep financial sector information safe. The following dataset is taken from the link [39].

Data privacy refers to individuals’ ability to control their data collection and use. Data security and privacy go hand in hand because protecting customer details and secret materials is the first step in preserving digital information and personal data confidentiality. The results are compared to the latest techniques such as Support Vector Machine (SVM), Principal Component Analysis (PCA), and Linear Discriminant Analysis (LDA). Personal Identifiable Information is a severe danger to data privacy. In an innovative contemporary society, dealing with millions, if not billions, of collected data can be a hardship because of the information’s quality and amount. Figure 6 shows that the financial sector’s data privacy ratio is mathematically confirmed using Equation (2). The innovative CS-FSM method to financial sector cyber security enhances privacy, scalability, risk reduction, data protection, and attack avoidance. EES and KNN are two examples of AI algorithms that can provide a more comprehensive view of cyber security than traditional methods. The proposed method represents a significant improvement over the status standard of cyber security measures in the banking industry. The results in Figure 6 validate the novel nature and practicality of the proposed approach enhancing cyber security in the banking industry.

Preparing the groundwork to enable and support future performance and being able to grow without being inhibited is the goal. Planning, funding, and having the right infrastructure (including people, procedures, tools, and equipment) are essential. This refers to the ability of an organization or company strategy to grow without being constrained by its structure or finances when confronted with higher productivity. In a software organization, scalable pricing is valuable for increasing income. It allows one to take a larger share of the money that customers are ready to pay without alienating smaller customers who cannot afford high pricing. The finance system’s scalability ratio is theoretically verified using Equation (2) in Figure 7.

Financial risk refers to a company’s ability to handle indebtedness and strain, whereas economic exposure refers to the firm generating enough income to cover operating costs. Financial risk refers to a group’s capacity to manage credit and fulfill financial obligations. Volatility in stock prices and bond rates, currency fluctuations, and other variables contribute to this risk type. The simulation results of the proposed CS-FSM system are shown in Table 2. The suggested CS-FSM systems simulation results and the growth rate in risk reduction are compared to existing models using Equation (5).
Data retention is all about protecting critical IT assets with a set of regulations and procedures. Throughout this project, papers, charts, identification, and connectivity were all taken care of. One strategy for identifying and reducing the risk associated with data storage and transportation is data security. Banks have to protect their customers’ financial information against unauthorized access. If cybersecurity is poor, clients can lose necessary time, personal information, and savings. Customers may become uneasy or fearful, and companies may lose the public’s faith in keeping their money and personal information safe. The proposed technique has strengthened data protection based on the data values determined from Equation (7). Figure 6 shows that the CS-FSM method provides better data protection than other methods. Protecting sensitive information is a crucial part of using artificial intelligence for security purposes in the banking industry. Financial institutions
must ensure that they have comprehensive data protection mechanisms in place to secure sensitive data from cyberattacks, comply with data protection legislation, and guarantee the transparency and explication of their AI-based cyber security systems.

Table 2. Comparison of risk reduction ratio.

<table>
<thead>
<tr>
<th>Number of Customers</th>
<th>SVM</th>
<th>CPS-IoT</th>
<th>PCA</th>
<th>DM</th>
<th>LDA</th>
<th>CATRAM</th>
<th>CS-FSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>78.5</td>
<td>82.1</td>
<td>84.8</td>
<td>80.9</td>
<td>90.5</td>
<td>86.3</td>
<td>93.2</td>
</tr>
<tr>
<td>20</td>
<td>76.2</td>
<td>80.2</td>
<td>85.6</td>
<td>82.3</td>
<td>89.3</td>
<td>90.1</td>
<td>95.4</td>
</tr>
<tr>
<td>30</td>
<td>80.4</td>
<td>81.7</td>
<td>89.2</td>
<td>78.6</td>
<td>88.4</td>
<td>91.6</td>
<td>96.1</td>
</tr>
<tr>
<td>40</td>
<td>83.4</td>
<td>82.9</td>
<td>88.7</td>
<td>81.4</td>
<td>87.6</td>
<td>88.4</td>
<td>97.4</td>
</tr>
<tr>
<td>50</td>
<td>72.5</td>
<td>79.6</td>
<td>82.3</td>
<td>80.5</td>
<td>85.4</td>
<td>89.3</td>
<td>94.6</td>
</tr>
<tr>
<td>60</td>
<td>74.6</td>
<td>72.4</td>
<td>80.8</td>
<td>79.8</td>
<td>82.5</td>
<td>87.8</td>
<td>92.4</td>
</tr>
<tr>
<td>70</td>
<td>78.2</td>
<td>76.3</td>
<td>82.5</td>
<td>82.7</td>
<td>86.6</td>
<td>85.6</td>
<td>93.5</td>
</tr>
<tr>
<td>80</td>
<td>82.6</td>
<td>77.5</td>
<td>81.2</td>
<td>86.9</td>
<td>89.4</td>
<td>83.4</td>
<td>96.7</td>
</tr>
<tr>
<td>90</td>
<td>85.4</td>
<td>85.6</td>
<td>86.7</td>
<td>83.6</td>
<td>79.6</td>
<td>91.7</td>
<td>95.4</td>
</tr>
<tr>
<td>100</td>
<td>79.5</td>
<td>87.2</td>
<td>89.6</td>
<td>85.4</td>
<td>88.6</td>
<td>89.8</td>
<td>98.7</td>
</tr>
</tbody>
</table>

Figure 8. Assessment of data protection.

An attack avoidance strategy eliminates challenges, activities, and exposures that could harm a company and its resources. Cybersecurity seeks to minimize the negative consequences and financial costs of potentially harmful situations, whereas avoidance aims to avoid them altogether. The CS-FSM approach, as shown in Figure 9, is more precise than the alternatives. These values are provided by Equations (8) and (9), demonstrating a significant increase in attack avoidance utilizing the researcher’s proposed technique.

Due to data breaches, financial institutions can be tough to convince, which is a significant problem for banks. A shaky protection system can lead to data exposures, quickly leading to customers going elsewhere to spend their cash. The CS-FSM approach enhances the data privacy ratio (18.3%), scalability ratio (17.2%), risk reduction ratio (13.2%), data protection ratio (16.2%), and attack avoidance ratio (11.2%).
The purpose of this section is to discuss an experiment that focused on a suggested CS-FSM method for cyber security utilizing AI and EES. The research’s code was written in Python, and the results were examined in Matlab 2018a. Data privacy, scalability, risk reduction, data protection, and attack avoidance are a few of the metrics used to gauge the success of the suggested approach. Linear discriminant analysis, principal component analysis, and the Support Vector Machine are some of the current methods used to compare the results. To ensure the protection of the financial sector’s data, the experiment assessed cyber security data. The results of the study demonstrated that the CS-FSM method excels over competing approaches in terms of data confidentiality, scalability, risk mitigation, data security, and attack avoidance. The risk reduction ratio for various models is compared in Table 2, and it can be seen that the suggested CS-FSM method results in a higher risk reduction rate. The findings verified the efficacy of the proposed approach in delivering financial sector cyber security.

Artificial intelligence (AI) algorithms such as the Enhanced Encryption Standard (EES) and the K-Nearest Neighbor (KNN) algorithm are used in CS-FSM to provide a holistic approach to cyber security. While the EES method is used to encrypt and decode data in the banking sector, the KNN algorithm is employed to identify and prevent malware threats. The suggested method can classify cyberattack problems and provide solutions through the use of the KNN algorithm, which learns from the training data and makes predictions.

5. Conclusions

Improved privacy, scalability, risk reduction, data protection, and attack avoidance belong to some of the many benefits of the proposed CS-FSM paradigm, which is powered by AI to revolutionize cyber security in the financial sector. Using Enhanced Encryption Standard (EES) and the KNN algorithm, the research demonstrates the efficacy of these tools in foreseeing and averting intrusions. Positive outcomes in terms of data security, privacy, and risk reduction have been observed. This research shows how critical it is to implement AI algorithms into banking sector cyber security solutions. The system has analytical values of 96.1% for data privacy, 97.2% for scalability, 98.7% for risk reduction, 95.4% for data protection, and 94.3% for attack avoidance. Information security can be
improved further by incorporating blockchain technology, which should be the subject of future studies. As a whole, this innovative approach is an improvement over standard cyber security procedures and is effective in strengthening online safety in the banking industry.

CS-FSM provides a revolutionary approach to cyber security in the financial sector, improving privacy, scalability, risk reduction, data protection, and attack avoidance. The usage of EES and KNN, two examples of AI algorithms, offers a holistic perspective on cyber security that is lacking from more conventional approaches. The proposed solution is a considerable upgrade over current cyber security practices for dealing with cyber threats in the banking sector. The overall findings and conclusions prove the originality and usefulness of the proposed method for boosting financial sector cyber security.

There are, however, limitations to this research, such as the small sample size and narrow focus of the analysis. The report also glosses over the feasible consequences and probable costs of the proposed solution. Despite this, the successful use of AI algorithms into banking sector cyber security solutions is warranted due to the favorable results in data security, privacy, and risk reduction.

**Funding:** This research was funded by Deanship of Scientific Research at Majmaah University for supporting this work under Project Number No: R-2023-407.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The author declares no conflict of interest regarding the present study.

**References**


17. Dzhaparov, P. Application of blockchain and artificial intelligence in bank risk management. *Информатика Управление* 2020, 17, 43–57. [CrossRef]


20. Kshetri, N. Economics of Artificial Intelligence in Cybersecurity. *IT Prof.* 2021, 23, 73–77. [CrossRef]


Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.