International Journal of Religion
2024
Volume: 5| Number 10 | pp. 4766 – 4782
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/7rfyma13

Examining the Role of Artificial Intelligence in Cyber Security (CS): A Systematic Review for Preventing Prospective Solutions in Financial Transactions

Mahfujur Rahman Faraji[1], Fisan Shikder[2], Md. Hasibul Hasan[3], Md. Mominul Islam[4] and Umme Kulsum Akter[5]

Abstract

Artificial intelligence (AI) is a powerful technology that helps cybersecurity teams automate repetitive tasks, accelerate threat detection and response, and improve the accuracy of their actions to strengthen their security posture against various security issues and cyberattacks. This objective focuses on analysing how AI-based cyber security (CS) solutions improve performance in financial transactions and banking sectors. It also aims to identify the latest advancements in AI-driven CS) research to enhance security and operational efficiency in the financial sector. This article presents a systematic literature review and a detailed analysis of AI use cases for cybersecurity in financial transactions. The review resulted in 800 studies, of which 225 articles remain. This paper will provide readers with a comprehensive overview of the potential of AI to improve cybersecurity in financial transactions. The review also identifies future research opportunities in examining cybersecurity application areas, advanced AI methods, data representation, and the development of new infrastructures for successful adoption in financial transactions. The paper might increase cyber security systems' performance by increasing their defence against cyberattacks. Artificial intelligence approaches improve and enhance cyber security with machine learning and deep learning, fraud and threat detection, and this makes sure a secure and safe financial transaction. This study helps identify how to make transactions safer with cyber security. This study highlights the vital role of evaluation and continuous adaptation in AI. In the near future, this topic should focus on more collaboration among AI, cyber security, and system developers for better and secured outcomes.

Keywords: *Artificial Intelligence, Financial Transaction, Protection, Prospective Solution, Cyber Security, Cyberattack.*

INTRODUCTION

Cyber security (CS) encompasses the application of protective measures to defend networks, programs, and systems from electronic attacks (Baniyounes & Younes, 2024). Cyberattacks commonly aim to gain illegal accessibility, modify or destroy sensitive information, extort money via ransomware infections, or damage normal business activities. A robust cyber security (CS) plan entails the implementation of numerous levels of defense throughout devices, networks, programs, or datasets that require safeguarding (Thakur, 2024). Under consideration of the rising occurrence and intricacy of cyberattacks, along with the escalating intricacy of commercial connections, it is important to use a variety of cyber security (CS) measures to mitigate the likelihood of cyber threats to commercial enterprises (Tetteh & Otioma, 2024).

According to Wai and others (2024) By implementing measures to prevent unauthorized access to resources, systems, and technology, the dangers of cyber assaults are mitigated. The intricacy cyber security (CS) is escalating as a result of the swift proliferation of interrelated gadgets, systems, and networks. The following is exacerbated by progress in the field of technology and facilities leading to an enormous rise in cyberattacks with

[1] Master of Science in Engineering Management, Department of Engineering Management, Westcliff University, Irvine, United States, Email: mahfujurrahmanfaraji@gmail.com, ORCID: https://orcid.org/0009-0004-2312-2622

[2] Department of Management Information Systems, Faculty of Business Studies, Begum Rokeya University, Rangpur., Rangpur-5404, Rangpur, Bangladesh., Email: mdfisan@gmail.com, ORCID: https://orcid.org/0009-0000-1713-0029

[3] Department of Management Information Systems, Faculty of Business Studies, Begum Rokeya University, Rangpur., Rangpur-5404, Rangpur, Bangladesh, Email: hasibul44000@gmail.com, ORCID: https://orcid.org/0009-0004-8679-4928

[4] Department of Management Information Systems, Faculty of Business Studies, Begum Rokeya University, Rangpur., Rangpur-5404, Rangpur, Bangladesh., Email: mominul70989@gmail.com, (Corresponding Author), ORCID: https://orcid.org/0009-0006-4694-9379

[5] Department of Management Information Systems, Faculty of Business Studies, Begum Rokeya University, Rangpur., Rangpur-5404, Rangpur, Bangladesh., Email: uk176983@gmail.com, ORCID: https://orcid.org/0009-0009-2299-9007

profound consequences (Nweke & Yayilgan, 2024). Intelligence-driven cyber security (CS) is being implemented to offer proactive protection against constantly changing threats and to effectively handle large volumes of data. Artificial Intelligence (AI) is an astounding innovation that has the potential to provide sophisticated evaluation and comprehension to counter ever evolving cyberattacks. It achieves this by promptly analyzing numerous occurrences and overseeing a wide array of cyber hazards, enabling it to anticipate and respond as the issue emerges (Hansel & Silomon, 2023).

AI-driven methodologies employ sophisticated machine learning algorithms as well as deep learning techniques to identify, examine, and counteract cyber threats with enhanced velocity and precision. The integration of Artificial Intelligence (AI) into cyber security (CS) systems is more prevalent, as it is utilized to perform automated safeguarding duties or support individual safety personnel in various situation (Abdulhussein, 2024). The fields of AI and cyber security (CS) have prompt extensive research efforts aimed at addressing issues pertaining to the identification, separating, recognition, reaction, and restoration from cyberattacks. The Internet of Things (IOT) has the potential to revolutionize civilization through innovation. Banks must implement a cyber-risk management strategy to safeguard their clients' funds (Pramita & Sardjono, 2024). The financial services sector is a prime target for hackers and advanced persistent threats due to the numerous options it offers for benefit, such as extortion, burglary, forgeries, and political and ideological influence. The field of financial service delivery has not been affected by the transformative effects of AI, which has made banking services more flexible and pertinent. The banking and finance business has adopted technology advancements to enhance efficiency in operations, resulting in improved satisfaction with customers (Almuqrin & Mishra, 2024). Artificial Intelligence solutions primarily focus on two aspects: enhancing the security of corporate operations and improving the efficiency of service delivery by implementing prompt inventions and continual enhancements. Artificial Intelligence technologies have greatly boosted creativity and played a crucial part in delivering tailored and inventive solutions to stakeholders in the present era of digitalization in the banking and financial sectors (Hossain et al., 2024). The utilization of modern techniques such as data mining, forensic accounting and auditing, and digital investigation applications to combat financial frauds is limited due to cost constraints (Bhuiyan et al., 2024). Furthermore, it is noteworthy that the most susceptible small organizations have predominantly been slow to adopt because of the cost-benefit imbalance that frequently works against them (Rahman et al., 2024). Due to advancements in technologies for communication and information, digital and virtual platforms are being increasingly utilized by individuals with disruptive and criminal motives to carry out cybercrimes and cause disturbances online. To address these potential crimes and dangers, banks have little alternatives except to employ artificial intelligence to enhance their security measures (Bhuiya, 2022).

Research Gap

The number of evaluations on the subject of cyber security (CS) and the utilization of artificial intelligence have been published in the past few years (Bhuiya, 2022). As far as we are aware, there is currently no through analysis that encompasses the latest research on using AI approaches to explain cyber security (CS) operations related to financial transactions and the specific ways in which they are implemented (Bhuiyan, 2023). Artificial Intelligence can be utilized to scrutinize vast quantities of transactions with the purpose of detecting discrepancies, identifying patterns of financial misconduct, and uncovering unexpected occurrences (Bhuiyan, 2017). The same can play a crucial part in the through detection and prevention of fraud in immediate effect. There are multiple Artificial Intelligence approaches, channels, and algorithms that are currently accessible (Hossain et al., 2024). These technologies are designed to tackle the various problems and weaknesses that banking and financial organizations face in the virtualized era. Various Artificial Intelligence systems such as, Teradata and Feedzai, are available to effectively mitigate fraud incidents in the financial sector. Thus, the goal of the current research project is to gain an understanding of the several Ai-based solutions that are available to safeguard cyberspace, with a focus on banking and financial transactions (Bhuiyan, 2023).

OBJECTIVE

RO 1: To examine the role of artificial intelligence-based cyber security (CS) solutions on the overall performance in the financial transactions and banking sectors.

RO 2: To determine the most recent developments in artificial intelligence-driven cyber security (CS) research concerning financial transactions.

LITERATURE REVIEW

According to Milon (2023), a thorough literature analysis offers significant insights into the current research, theories, and practices related to the incorporation of artificial intelligence (AI) techniques for enhancing cybersecurity in financial transactions. This study examines significant studies and publications that provide insight into the possible advantages, difficulties, and consequences of applying integrated techniques. Multiple studies have emphasized the significant capacity of AI to improve cybersecurity in financial transactions (Mishra, 2023). Research highlight the significant of artificial intelligence (AI) in enhancing fraud detection and prevention by utilizing sophisticated analytics and machine learning techniques. Furthermore, a study highlights the capacity of AI to improve cybersecurity through the automation of threat detection and response procedures (Bhuiyan, 2022). These findings emphasize the significance of AI in strengthening banking security through the implementation of real-time monitoring, anomaly detection and predictive analysis (Akter et al., 2024).

Artificial Intelligence

Arificial intelligence refers to computer systems that are capable of performing tasks commonly associated with human intelligence, including predicting, object recognition, speech interpretation, and natural language generation (Garg, 2021). AI systems acquire this ability by analyzing vast quantities of data and identifying patterns that they can use as templates for their own decision- making processes (Bhuiyan, 2019). Often, people will oversee the learning process of an AI, strengthening favorable choices and discouraging unfavorable ones (Li et al., 2023).

However, certain AI systems are specifically built to acquire knowledge without any supervision. Over time, artificial intelligence (AI) systems enhance their proficiency in particular activities, enabling them to adjust to new inputs and make judgements without requiring explicit programming (Gil et al., 2021). Artificial intelligence involves instructing robots to emulate human thinking and learning processes, with the aim of streamlining tasks and enhancing problem-solving capabilities (Bhuiyan et al., 2023).

Cybersecurity

Cybersecurity establishes policies, procedures, and technical measures to protect against damage, unauthorized entry, modification, or misuse of information and communication systems and their contents (Chitadze, 2023).

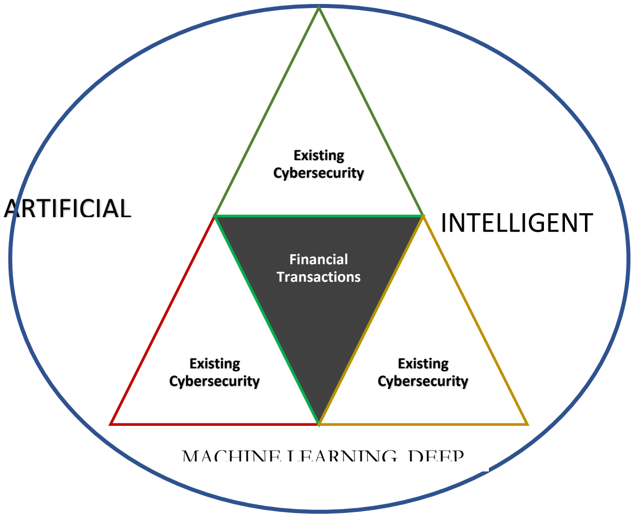

Figure 1: Extra Layer of AI for Protecting Financial Transactions in Cyberspace

Source: (Ozkan-Okay et al., 2024)

The rapid pace of technical breakthroughs and innovation, along with the constantly evolving landscape of cyber threats, adds extra complexity to the problem. AI-powered cybersecurity tools have evolved to address this unique issue, aiding security teams in effectively reducing risks and enhancing security (Costa & Coelho, 2024). To effectively analyze the literature on using AI for cybersecurity, it is necessary to have a universally agreed-upon and integrated classification system due to the diversity of AI and cybersecurity (Bhuiyan et al., 2023). Th This systematic classification system will aid scholars and professionals in achieving a mutual understanding of the particular methodologies (Mani, 2024) and utilities that require enhancement through the utilization of artificial intelligence for the successful execution of robust cybersecurity measures (Sarker et al., 2024).

The Role of Artificial Intelligence in Cybersecurity

Artificial intelligence is vital in the subject of cybersecurity since it improves the effectiveness of cybersecurity defense measures (Azambuja et al., 2023). Artificial intelligence employs data analysis to anticipate and avert cyber threats by examining extensive quantities of information (Islam & Bhuiyan, 2022). To avoid cyberattacks, it is vital to use a comprehensive and multi-dimensional approach that incorporates many security measures at different levels of an organisation's infrastructure. Presented comprehensive examination of age technique employed to prevent cyberattacks (Ghiasi et al., 2023). The significance of AI is cybersecurity stems from its capacity to offer sophisticated threat detection automate responses, adjust to emerging threats, and extensive data analysis (Hossain, 2024). Given the ever-changing nature of Cyber threats, it is becoming more and more crucial to incorporate artificial intelligence (AI) into cybersecurity strategies in order to preserve strong and efficient defenses (Arif et al., 2024).

Table 1: The role of artificial intelligence in cybersecurity

Core concepts	Explanation	Reference
Advanced Threat Detection	Artificial intelligence facilitates the implementation of Advanced and resize thread detection. Machine learning algorithms have the capability to examine large data sets and detect trends, abnormalities and potential threats in real time. This proactive strategy enables the timely identification of developing risks, including novel and sophisticated attacks.	(Labu & Ahammed, 2024)
Behavioral Analytics	Artificial intelligence demonstrates exceptional proficiency in behavioral analytics, which compasses the examination of user behaviour patterns and network activity. AI systems can identify security threats by comparing current activity to a standard baseline and detecting any abnormal security procedure may overlook.	(Awaludin et al., 2024)
Automated Incident Response	Artificial intelligence enables the streamlining of incident response procedures. AI possess the capacity to acquare knowledge from past data and adjust their response based on new information, enabling them to promptly and efficiently address required to discover, contain, and resolve a security breach.	(Sontan et al., 2024)
Reducing False Positives	Artificial intelligence (AI) has the capability to decrease the occurrence of incorrect identification in security alerts. Conventional security systems frequently provide erroneous alerts, resulting in a state of exhaustion from excessive warnings and the possibility of disregarding genuine dangers. The capacity of AI to contextualize data and comprehend typical behavior patterns aids in differentiating authentic threats from false alarms.	(Bhuiyan, 2022)

Financial Transactions in Cybersecurity

According to Alom and others (2023) AI has being increasingly utilize in the financial industry across five key domains: compliance, fraud and anti-money laundering (AML) detection, lending and credit evolutions, cybersecurity, and trading and investment strategies (Uddin et al., 2024). The advent of technology has given rise to the creation of digital banking, online investment platforms, electronic payment systems, and other financial service that function via the internet (Bhuiyan er al., 2023). The emergence of digital transformation has improved the accessibility and convenience of financial services (Hossain et al., 2024). However, the shift to digital platforms has also introduced new challenges, particularly in regard to cybersecurity (Hossain et al., 2024).

Additional investigation is required to examine the obstacles and optimal methods for incorporating these technologies in the cybersecurity measures for financial transactions. By tackling these obstacles and harnessing the capabilities of AI, organizations may enhance their cybersecurity measures and guarantee the durability of the financial ecosystem (Azeez et al., 2024).

METHODOLOGY

Artificial intelligence merging with existing technologies has effectively advanced financial transaction security in cyberspace (Bhuiyan, 2023). The methodical investigation and extensive examination of qualitative data guided this research whose goal is to identify, evaluate, and interpret all the searches in the area of research gaps, objectives, and answers to the research questions (Molla et al., 2023). The methodical research starts with a robust data sourcing phase whose motive is to find a wide range of scholarly databases, journals, industry reports, white papers, and conference proceedings such as Web of Science, SCOPUS, Scholar Google, and TRID that are essential to the study of artificial intelligence, financial transactions, and cybersecurity (Alam, 2020).This wide range of sources guarantees a deep diversity of viewpoints, covering technological developments, real-world applications, and the multidisciplinary character of financial transaction innovation (Bhuiyan et al., 2023).

Following the search phase, the identified studies underwent a filtering process to eliminate any study that was not relevant (Islam et al., 2024). The studies collected during the initial phase were evaluated based on specific criteria to identify significant publications that discuss the study themes. At this point, it is crucial to ensure a significant, yet attainable, selection of studies (Islam, et al., 2024). The search was conducted without any time restrictions, and early papers were included to ensure that no important research findings were overlooked. 800 Papers were extracted from the Web of Science, SCOPUS, Scholar Google, and TRID database and refined using the inclusion and exclusion criteria (Akter et al., 2023). After excluding papers written in languages other than English, posters, reviews, surveys, non-scientific publications, books, chapters, summaries of workshops and symposiums, duplicates, guideline documents, and comparative studies, there were 225 articles remaining (Masum et al., 2024).

It was evident from the title and abstract if the study was outside the purview of the review and may be disregarded. In cases where the study's contribution or application domain were not evident from the title or abstract, the complete text of the paper was scrutinized in later rounds of the review process (Bhuiyan & Akter, 2024). 115 studies were selected from a total of 225 research based on a study of the titles and abstracts (Hossain et al., 2024). Following a comprehensive review of the complete publications, 52 more studies were excluded. This means that the foundation for this research study was provided by a total of 63 original studies.

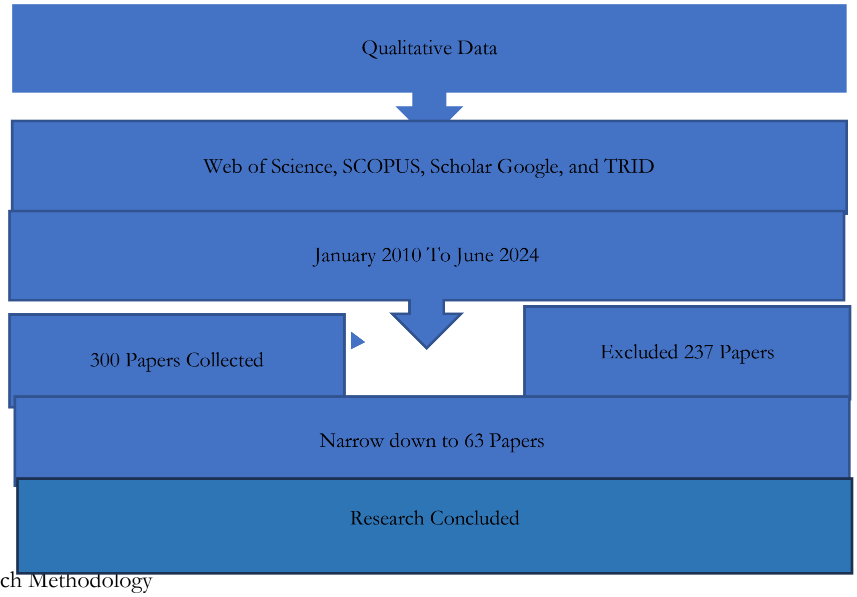

Figure 2: Research Methodology

Source: Author's work

DISCUSSION

Artificial Intelligence in Cybersecurity

zAccording to akter and others (2023) the escalating dependence on technology in the contemporary world has heightened the imperative of safeguarding confidential data to an unprecedented degree. Cyberthreats have the potential to disrupt organizations and affect individuals worldwide, ranging from personal data breaches to financial transaction disruptions (Ali et al., 2023). There is no text provided. Cybersecurity is a field that comprises a range of procedures and activities aimed at protecting computer systems and networks against unwanted access, damage, or theft. It involves the implementation of robust security protocols, sophisticated encryption technologies, and proactive countermeasures (Bhuiyan & Akter, 2024). According to the IMF global financial stability report April, 2024, the banking sector is particularly vulnerable to cyber danger. Financial institutions, due to their handling of substantial quantities of sensitive information (Poli et al., 2024).

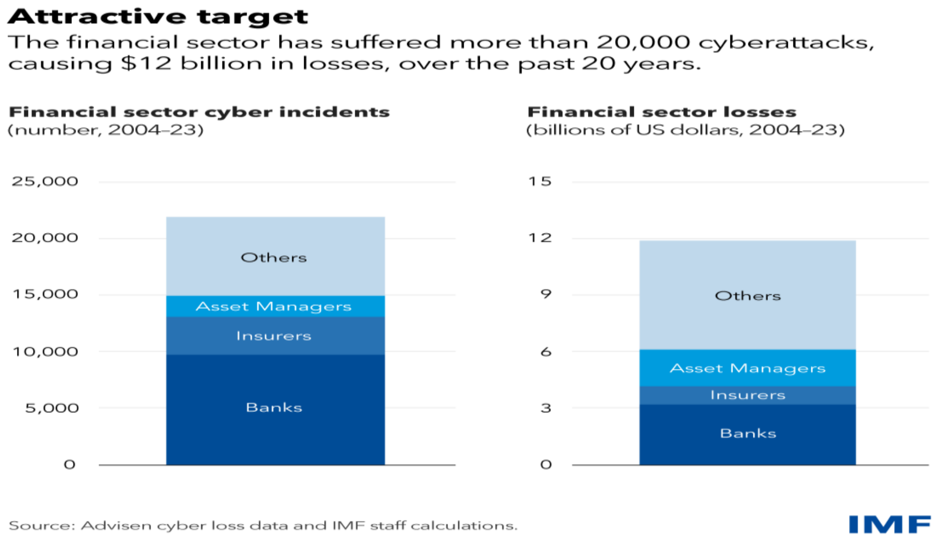

Figure 3: The IMF Global Financial Stability Report April 2024

Source: Advisen cyber loss data and IMF staff calculation

and financial transactions, are frequently targeted by criminals with the intention of stealing funds or disrupting economic operations (Bhuiyan et al., 2024). Nearly 20% of all attacks target financial firms, with banks being the most vulnerable. Instances of cyber disruptions that cause significant disruptions to essential services (Kabir et al., 2024).

Concerning present evidence ensuring cybersecurity becomes more significant in the financial sector as well as financial transactions (Khan, 2023). AI-powered solutions enhance analysts' efficiency by speeding up AI threat identification and mitigation, expediting replies, and safeguarding user identity and datasets. These solutions also ensure that cybersecurity teams remain informed and in control (Sontan et al., 2024).

Financial Transaction in Cyberspace

A financial transaction refers to the process of buyers and sellers engaging in a conversation or agreement to trade assets, services, or goods in return for money on an internet platform (Javaid et al., 2023). It entails the use of at least one asset, such as money or a valued commodity like silver or gold, to be exchanged in the digital realm (Mia et al., 2024).

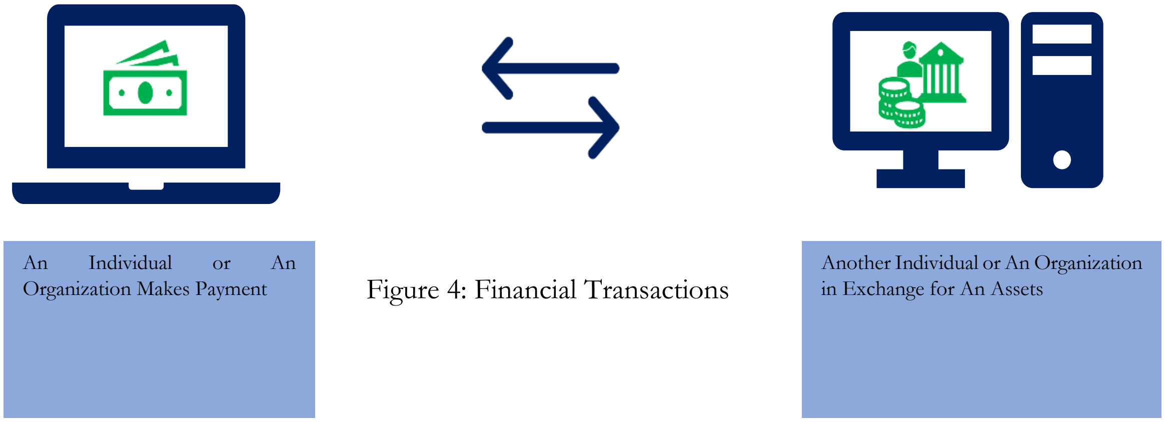
An Individual or An Organization Makes Payment
Figure 4: Financial Transactions
Another Individual or An Organization in Exchange for An Assets

Figure 4: Financial Transactions

A financial transaction can occur when there is a change in the financial situation of two businesses or individuals' financial situations change. Financial transactions occur when an individual decides to provide payment in return for an asset. In the field of accounting, a transaction is classified as a financial transaction if it exclusively involves the exchange of money, rather than a transaction where money is traded for a tangible item or service (Mulherin et al., 2021). Instances of this category of financial transaction encompass acquiring a loan and placing funds into a checking or savings account (Khanom et al., 2022).

According to Alam (2022) suppose when a person uses his debit or credit card to pay at a grocery store for goods, the person has conducted a cyber transaction. To ensure the transaction is secure and authentic a security path has been followed. The path starts from identification, authentication to authorization (Meah & Hossain, 2023).

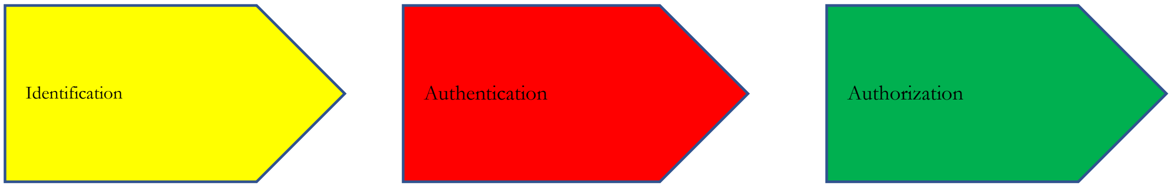

Figure 5: Basic Meacham of Financial Transactions

Table 2: Basic Meacham of Financial Transactions

Concept of cybersecurity	Description	Reference
Identification	Identification is the initial stage in cyber transactions and involves a user submitting their personal information, such as their name, email address, phone number, or username, in order to establish their identity (Mani, 2019). This refers to the act of an individual affirming their identity as a specific person. Identities can be authenticated by providing additional information, typically in the form of a government-issued identification document. The verification process often occurs just after the initial account creation or site access. Following this, your identification will undergo authentication, typically through the establishment of a password that corresponds to your username.	(Chawki & Abdel Wahab, 2006)
Authentication	Authentication, in the context of information security, refers to the collection of techniques employed to verify the validity of an identity assertion. Authentication just verifies the accuracy of the claimed identity. Authentication does not entail or suggest anything about the permissions or actions that the authenticated party is granted; this is a distinct process referred to as authorization. Authentication can be done using a password, a hardware token, or other proof. Authorization verifies the user's or device's permission to access data or resources, while authentication is distinct. Access control and cyber security require authentication.	(Saqib & Moon, 2023)
Authorization	Authorization defines the permissions and restrictions for users, systems, or applications once they have been verified via the authentication procedure. Usually, an administrator or system owner grants those access and privileges. The allocated privileges govern the user's actions,	(Mohamed et al., 2023)

	including their ability to read and write, utilize specified services, access networks, databases, other applications, or sensitive data. The authorization privileges dictate the extent of access or functionality that a user or system can have within a network, system, or program.	

Identification, authentication and authorization seem like basis, but all of the security software or system focuses on securing this security financial security path.

Contemporary Methods of Cyberattacking and Preventing Financial Transaction Security Path

Several methods of attacking have been developed to weaking the cybersecurity. Moreover, there operational techniques are different which make difficult to spot and mitigate them. On the other hand, several prevention methods also have been developed to secure cybersecurity.

Table 3: Contemporary Cyberattack

Cyberattacking Methods	Description	Reference
Denial-of-Service (DoS) Attacks	A denial-of-service (DoS) attack is a type of cyberattack that targets devices, information systems, or other network resources with the intention of preventing legitimate users from accessing the services and resources they expect to use. Typically, this is achieved by inundating the intended host or network with a high volume of data until the target becomes unresponsive or has a system failure.	(Haseeb-ur-rehman et al., 2023)
Identity-Based Attacks	Identity-based attacks target and compromise the digital identities of individuals, organizations, or entities. These attacks exploit vulnerabilities in identity and cybercriminals can exploit access management systems to illicitly acquire, modify, or exploit valuable information, including login passwords, domain names, personal data, and digital certificates.	(Wang et al., 2024)
Malware	Malware, an abbreviation for malicious software, encompasses any invasive program created by cybercriminals (often known as hackers) with the intention of pilfering data and causing harm or destruction to computers and computer systems. Common types of malware encompass viruses, worms, Trojan viruses, spyware, adware, and ransomware.	(Alaeiyan et al., 2023)
Code Injection Attacks	Code injection refers to the act of maliciously inserting code into an application. Subsequently, the program proceeds to interpret or execute the code, thereby influencing the performance and functionality of the application. Code injection attacks commonly target pre-existing data vulnerabilities, such as insecure manipulation of data from untrusted sources.	(Lee et al., 2023)
Insider Threats	An insider threat refers to a cyberattack that is initiated by an individual who is employed by an organization or has authorized access to its networks or systems. An insider threat refers to an individual who poses a risk to an organization's security and can include current or former employees, consultants, board members, or business partners. This threat can arise from intentional, unintentional, or malevolent actions.	(Renaud et al., 2024) (Shaw, 2023)

Contemporary Prevention Methods

In order to secure financial transaction several methods and technologies have been invented to tackle down insecurity in cyberspace.

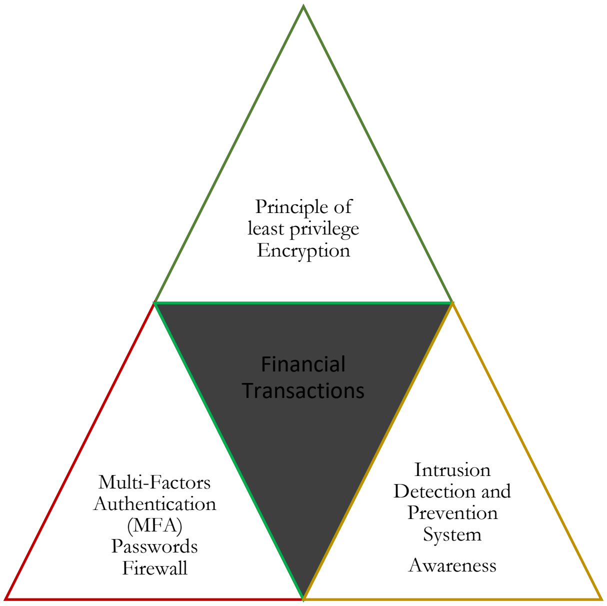
Principle of least privilege Encryption
Financial Transactions
Multi-Factors Authentication (MFA) Passwords Firewall
Intrusion Detection and Prevention System
Awareness

Figure 6: Contemporary Method protecting Financials Transactions in cyberspace

Multi-Factor Authentication (MFA) is a way of verifying a user's identity by requiring them to provide at least two pieces of evidence, such as a password and a temporary passcode.

Intrusion Detection and Prevention System: An Intrusion Prevention System (IPS) is alternatively referred to as an Intrusion Detection and Prevention System (IDPS). This is a network security application that monitors network or system actions to detect any harmful or malicious behaviour. The primary functions of intrusion prevention systems (IPS) are to detect and classify hostile activity, gather relevant information about such activity, generate reports, and make efforts to prevent or halt it (Kizza, 2024).

Network Segmentation: Network segmentation in cyber networks refers to dividing cyber networks into smaller, different parts and making subnetworks, also network segmentation is called network isolation and network segregation. Each segment is made of a different set of devices, resources, and networks which are isolated from other segments of networks by routers, switches, and firewalls (Bhuiyan, 2023).

Principle of least privilege: According to Rashed and others (2024) the principle of least privilege is a concept of restricted access to computer files that ensures people restricted access rights following specific requirements. The principle of least privilege assures that only authenticated individuals with confirmed identities have the right authorizations to exercise tasks within the systems, apps, data, and other resources.

Complex Passwords: complex passwords referred to as password strength which is focused on the difficulty level. when an individual would like to try to guess a user's password, it makes them overwhelmed with guesses (Bhuiyan, et al., 2024).

According to Islam (2024) artificial intelligence operates with massive datasets with sophisticated, looping algorithms to acquire knowledge from patterns and characteristics in the raw data. After each loop of data processing, artificial intelligence evaluates and assesses its self-performance while also gathering more knowledge and skills. Artificial intelligence operates continuously without any breaks, enabling it to rapidly process numerous data, ranging from hundreds to limitless.This allows it to acquire a substantial amount of knowledge within a short period and attain exceptional proficiency in the specific activities it is taught for (Amin et al., 2024).

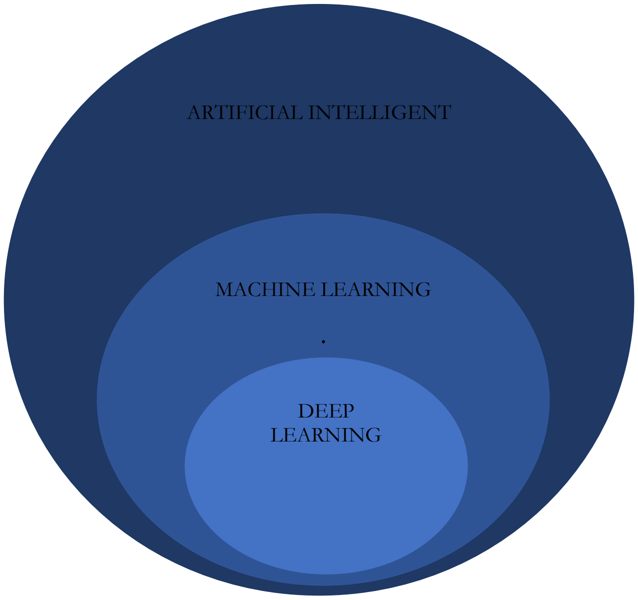

Figure 7: Architecture of Artificial Intelligent

Machine Learning

Machine learning (ML) is a branch of artificial intelligence that focuses on creating and analyzing statistical algorithms capable of learning from data, making predictions on new data, and performing tasks without being explicitly programmed (Taye, 2023). In recent times, artificial neural networks have demonstrated superior performance compared to several previous methods.

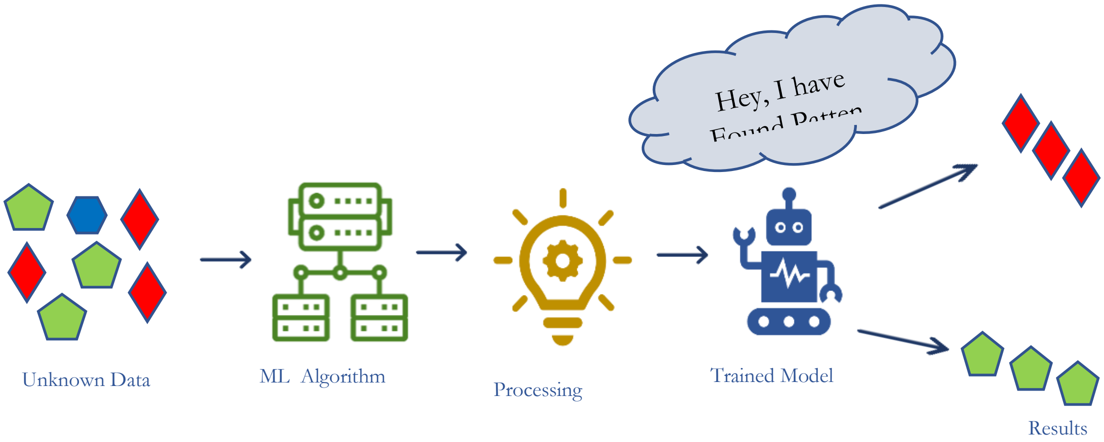

Figure 8: Working Method of Machine Learning

Then, the algorithm will classify all of that information into different classes. After processing those classifications machine learning will train themselves to identify which one is a cyberattack and which one is not. One of the best factures of machine learning and artificial intelligence is that the learning and identifying process will be conducted forever without human intervention which will help the machine algorithm to tackle future financial transactions cybersecurity effectively (Abdulhussein, 2024). With the help of artificial intelligent machine learning, AI can detect Denial-of-Service (DoS) Attacks, Identity-Based Attacks, Malware, Code Injection Attacks, DNS Tunnelling and so on which improve cybersecurity in financial transactions. Moreover, the production capability of machine learning enables artificial intelligence to spot potential cyberattacks at a premature stage when it is forming. Suppose, when attackers flood the targeted host or network with traffic until the target can't respond or crashes which is called a denial-of-service (DoS) attack, The ML can predicate that (DoS) attack is forming then machine learning can stop the flow of traffic before it jams or crashes the server (Kushardianto, 2023).

Reinforcement Learning

Another subset of Machine learning algorithm that acquires information by systematically experimenting and subsequently determines which course of action yields greater benefits. Reinforcement learning consists of three primary elements: the agent, the environment, and the actions (Sivamayil et al., 2023). The environment is everything the agent interacts with; the actions are what the agent performs; and the agent is the learner or decision-maker.

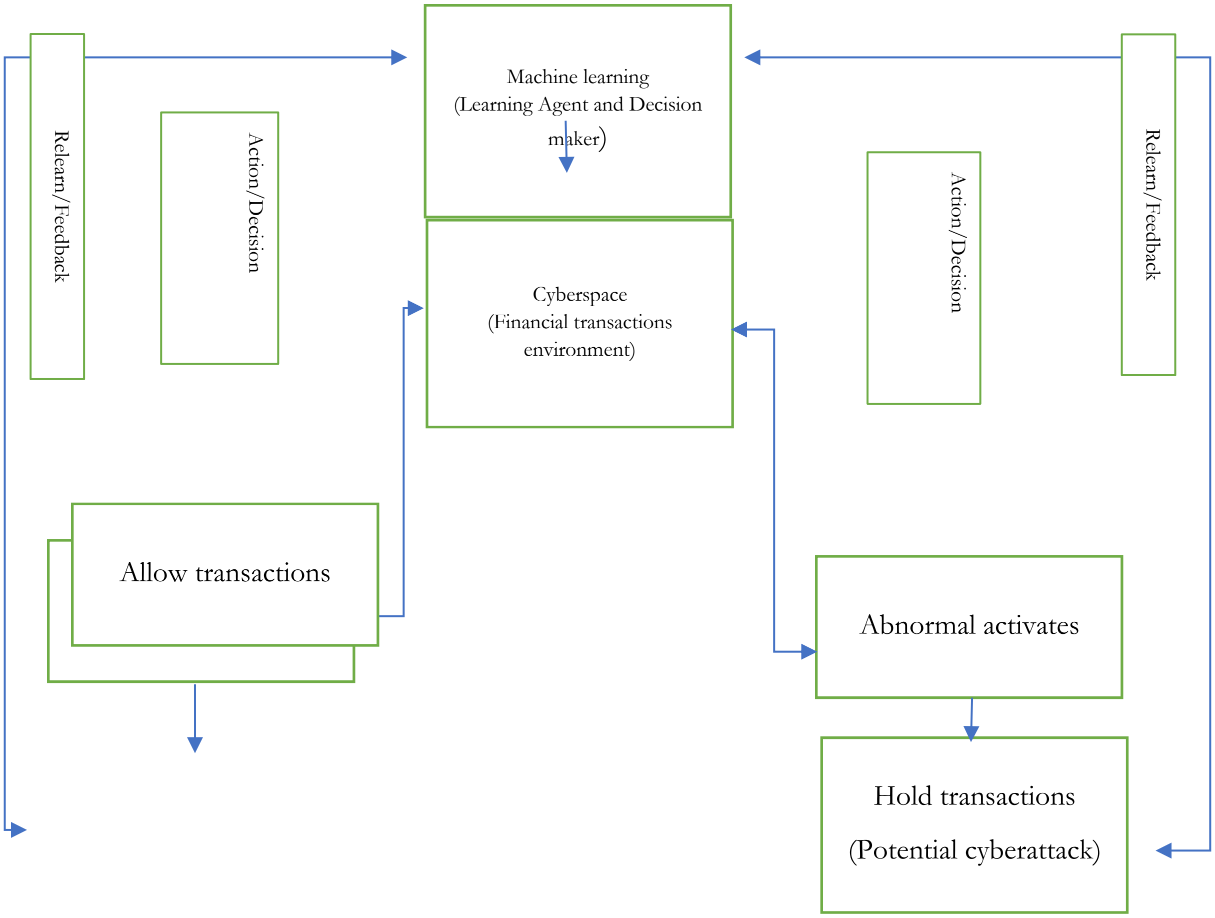

Figure 9: Reinforcement Learning process

Deep Learning

According to Sivamayil and others (2023) deep learning algorithms aim to derive comparable conclusions to those made by humans through continuous analysis of data using a predetermined logical framework. In order to accomplish this, deep learning employs a complex arrangement of algorithms known as neural networks, which consist of multiple layers. The neural network's design is derived from the architecture of the human brain. Similar to how our brains utilize pattern recognition and categorization to process information, we can train neural networks to carry out these tasks on data (Yang & Wang, 2020).

The individual layers of neural networks can be conceptualized as filters that operate from coarse to fine, hence enhancing the probability of accurately detecting and producing a right outcome. The human brain operates similarly. Upon receiving new knowledge, the brain endeavours to compare it with familiar objects. Deep neural networks also employ the same concept (Van Dyck et al., 2021).

Statement of the Financial Transactions in Cyberspace

According to Bhuiyan (2023) the existing cybersecurity is falling behind in protecting financial transactions in cyberspace due to continuously evolving and growing computer computing capability. Recent research on quantum computers suggests that available security tools and techniques will fail against quantum computers' computing capability which is a serious threat not only to financial transaction security in cyberspace but also to all kinds of cyber activities. Cyber attackers will have a new edge to exploit and expose the current financial transactions security mechanism (Aslan et al., 2023). Within these kinds of turmoil, artificial intelligence appears as an emerging shield against new and developing cybersecurity threats. With the massive learning capability, artificial intelligence can improve financial transaction cybersecurity.

Implications of the Study

The study of artificial intelligence driven approaches to enhance and upgrade cyber security in financial transaction has significant role (Mahalakshmi et al., 2022). This approach based solutions, offer financial institution the ability to identify defend against cyber vulnerabilities .AI driven approaches can improve cyber security with enhanced threat detection and respone.AI algorithm, particularly related with deep learning and machine learning, can analyze a lot of data transaction in real time to detect potential threat. By AI it is possible to predictive analytics, and it can forecast potential security breaches and weakness. Artificial intelligence driven approaches thoroughly learn and adapt to new types of cyber threats, and from this paper it is clear that most of the case AI system is one of the stronger applications for improving cyber security in financial transaction (Sarker, 2024). For artificial intelligence, customers in financial Institute can enjoy more smooth transactions. AI driven approaches to cyber security in transactions hold transformative potential. It promises not only to improve security and efficiency but also important economic and operational benefits (Adama et al., 2024). Policies aimed at improving digital infrastructure must be complemented by initiatives to enhance digital literacy, particularly among financial sectors. By addressing artificial intelligence to improve cybersecurity in financial transactions, the financial sector can harness the full potential of digital technologies to foster inclusive growth and improvement of cybersecurity. Overall, AI in cyber security for financial transactions can lead to improve threat detection, better risk management and improve the security of financial data (Odeyemi et al., 2024).

CONCLUSION

According to Chen and others (2021) AI has great impact in improving financial services and regulatory compliance. Improvement of privacy, scalability, reduction of risk, protecting data, and avoiding attack belong to some of the convenience of the upcoming CS-FSM paradigm, which is by AI to transform cybersecurity in the financial sector. This systematic review mentioned the metaphoric character of artificial intelligence including machine learning, deep learning and fraud detection in improving cyber security (Dasgupta et al., 2022). By improving incident response time, analyzing vast datasets for Insights, and automating threat detection, AI significantly elevated the consistency of financial service against cyber vulnerabilities. Moreover, the review prominence the importance of continuous adaptation and evaluation of artificial intelligence solutions to prevent progressive sophisticated cyber threats (Bahoo et al., 2023). It is vital for financial system to invest in AI-driven strategies that not only comply with regulatory requirements but also protect sensitive transaction data and foster customers trust (Milon, 2024). The overall findings and conclusion demonstrate the purity and usefulness of proposed method for improving financial transactions cyber security (Inuwa & Das, 2024). However, it is of greatest possible importance for the banking and commercial sector to examine the cost-benefit swap of investing in the Artificial Intelligence based solution not surely in monetary terms but also other element shall be taken into consideration like moral hazard, upstanding reputation, status etc. before reaching to a conclusion. A number of studies have said that the return of investment of upgrade technologies has been many folds over in terms of money and non-monetary returns, along with many positive implications (Jia et al., 2024).

Future Directions

Future research on this topic should focus on collaboration between financial institutions, AI developers, and expert of cyber security to create integrated solution that address the multifaceted behaviour of cyber threats (Arif et al., 2024). Future AI system should focus on adaptive learning techniques that can update the algorithm to new vulnerabilities and changing patterns in financial transaction on a large volume of primary and secondary data.

Acknowledgement

Authors have acknowledged to Mohammad Rakibul Islam Bhuiyan, Lecturer, Begum Rokeya University, Rangpur, for his valuable insights and guidelines for completing this research. There is no external funding for conducting this research. Author have contributed to each portion of the research equally.

REFERENCES

Abdul-Azeez, O., Ihechere, A. O., & Idemudia, C. (2024). Digital access and inclusion for SMEs in the financial services industry through Cybersecurity GRC: A pathway to safer digital ecosystems. Finance & Accounting Research Journal, 6(7), Article 7. https://doi.org/10.51594/farj.v6i7.1270

Abdulhussein, M. (2024). The Impact of Artificial Intelligence and Machine Learning on Organizations Cybersecurity. Doctoral Dissertations and Projects. https://digitalcommons.liberty.edu/doctoral/5242

Abdulhussein, M. (2024). The Impact of Artificial Intelligence and Machine Learning on Organizations Cybersecurity. Doctoral Dissertations and Projects. https://digitalcommons.liberty.edu/doctoral/5242

Adama, H. E., Popoola, O. A., Okeke, C. D., & Akinoso, A. E. (2024). ECONOMIC THEORY AND PRACTICAL IMPACTS OF DIGITAL TRANSFORMATION IN SUPPLY CHAIN OPTIMIZATION. International Journal of Advanced Economics, 6(4), Article 4. https://doi.org/10.51594/ijae.v6i4.1072

Milon, M. N. U. (2024). Gravitating towards Artificial Intelligence on Anti-Money Laundering A PRISMA Based Systematic Review. International Journal of Religion, 5(7), 303-315. https://doi.org/10.61707/py0fe669

Akter Poli, T., Hasan Sawon, Md. M., Nasir Mia, Md., Ali, W., Rahman, M., Hossain, R., & Mani, L. (2024). Tourism And Climate Change: Mitigation And Adaptation Strategies In A Hospitality Industry In Bangladesh. Tourism And Climate Change: Mitigation And Adaptation Strategies In A Hospitality Industry In Bangladesh. https://doi.org/10.53555/kuey.v30i5.3798

Akter, M. S., Amin, A.-, Bhuiyan, M. R. I., Poli, T. A., & Hossain, R. (2023). Web-based Banking Services on E-Customer Satisfaction in Private Banking Sectors: A Cross-Sectional Study in Developing Economy. Migration Letters, 20(S3), Article S3. https://doi.org/10.59670/ml.v20iS3.3976

Alaeiyan, M., Parsa, S., & P., V. (2023). Sober: Explores for invasive behaviour of malware. Journal of Information Security and Applications, 74, 103451. https://doi.org/10.1016/j.jisa.2023.103451

Alam, Md. K. (2020). A systematic qualitative case study: Questions, data collection, NVivo analysis and saturation. Qualitative Research in Organizations and Management: An International Journal, 16(1), 1–31. https://doi.org/10.1108/QROM-09-2019-1825

Alı, M. H., Hossaın, R., Mazumder, R., & Hasan, M. (2023). Does the extent of ownership by different shareholders enhance firm financial performance? Empirical evidence from an emerging economy. Journal of Business Economics and Finance, 12(4), 163-174. http://doi.org/10.17261/Pressacademia.2023.1843

Almuqrin, M., & Mishra, S. (2024). Using Artificial Intelligence to detect evasive techniques in Contemporary technologies. International Journal of Computing and Digital Systems, 16(1), 1–11. https://doi.org/10.12785/ijcds/XXXXXX

Amin, A., Bhuiyan, M. R. I., Hossain, R., Molla, C., Poli, T. A., & Milon, M. N. U. (2024). The adoption of Industry 4.0 technologies by using the technology organizational environment framework: The mediating role to manufacturing performance in a developing country. Business Strategy & Development, 7(2), e363. https://doi.org/10.1002/bsd2.363

Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International Journal of Multidisciplinary Sciences and Arts, 2(2), 242–251. https://doi.org/10.47709/ijmdsa.v2i2.3452

Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International Journal of Multidisciplinary Sciences and Arts, 2(2), 242–251. https://doi.org/10.47709/ijmdsa.v2i2.3452

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12(6), Article 6. https://doi.org/10.3390/electronics12061333

Awaludin, M., Yasin, V., & Risyda, F. (2024). The Influence of Artificial Intelligence Technology, Infrastructure and Human Resource Competence on Internet Access Networks. Inform : Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi, 9(2), 111–120. https://doi.org/10.25139/inform.v9i2.8109

Ayu Pramita, D. N., & Sardjono, W. (2024). The Role and Benefits of Innovative Technology in Using The Internet of Things (IOT) Towards Industrial Revolution 4.0. Dinasti International Journal of Education Management And Social Science, 5(5), 1177–1183. https://doi.org/10.38035/dijemss.v5i5.2788

Bahoo, S., Cucculelli, M., & Qamar, D. (2023). Artificial intelligence and corporate innovation: A review and research agenda. Technological Forecasting and Social Change, 188, 122264. https://doi.org/10.1016/j.techfore.2022.122264

Baniyounes, Z., & Bani Younes, Z. (2024). Cyber Attacks and its Implication to National Security: The Need for International Law Enforcement. 851–864.

Bhuiya. (2022). Factors Affecting Users' Intention to Use Social Networking Sites: A Mediating Role of Social Networking Satisfaction. Canadian Journal of Business and Information Studies, 112–124. https://doi.org/10.34104/cjbis.022.01120124

Bhuiyan, M. R. I. (2017). UNDP-a2i: Citizens' Awareness Survey on E-Service and Service Simplification through the Digital Innovation Fair. Available at SSRN 4341799. https://dx.doi.org/10.2139/ssrn.4341799

Bhuiyan, M. R. I. (2019). An Analysis of Non-Performing Loan of Janata Bank from the Perspective of Bangladesh. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4341827

Bhuiyan, M. R. I. (2023). The Challenges and Opportunities of Post-COVID Situation for Small and Medium Enterprises (SMEs) in Bangladesh. PMIS Review, 2, 141–159.

Bhuiyan, M. R. I. (2024). Examining the Digital Transformation and Digital Entrepreneurship: A PRISMA Based Systematic Review.

Bhuiyan, M. R. I. (2024). Examining the Digital Transformation and Digital Entrepreneurship: A PRISMA Based Systematic Review. http://dx.doi.org/10.57239/PJLSS-2024-22.1.0077

Bhuiyan, M. R. I., & Akter, Most. S. (2024). Assessing the Potential Usages of Blockchain to Transform Smart Bangladesh: A PRISMA Based Systematic Review. Journal of Information Systems and Informatics, 6(1), 245–269. https://doi.org/10.51519/journalisi.v6i1.659

Bhuiyan, M. R. I., Akter, Most. S., & Islam, S. (2024). How does digital payment transform society as a cashless society? An empirical study in the developing economy. Journal of Science and Technology Policy Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/JSTPM-10-2023-0170

Bhuiyan, M. R. I., Uddin, Dr. K. M. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy: An Empirical Study in Bangladesh. https://doi.org/10.20944/preprints202307.1652.v1

Bhuiyan, M. R. I., Uddin, K. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy: An Empirical Study in Bangladesh. doi: 10.20944/preprints202307.1652.v1

Bhuiyan, M. R. I., Uddin, K. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy in the Context of ICT Usages: An Empirical Study in Bangladesh. FinTech, 2(3), 641-656. https://doi.org/10.3390/fintech2030035

Bhuiyan, M. R. I., Ullah, M. W., Ahmed, S., Bhuyan, M. K., & Sultana, T. (2024). Information Security for An Information Society for Accessing Secured Information: A PRISMA Based Systematic Review. International Journal of Religion, 5(11), 932-946. https://doi.org/10.61707/frfnr583

Bhuiyan, M. R., Islam, Md. T., Alam, S. M. A., & Sumon, N. (2023). Identifying Passengers Satisfaction in Transportation Quality: An Empirical Study in Bangladesh. PMIS Review, 2(1). https://doi.org/10.56567/pmis.v2i1.10

Bhuiyan. (2022). Factors Affecting Users' Intention to Use Social Networking Sites: A Mediating Role of Social Networking Satisfaction. Canadian Journal of Business and Information Studies, 112–124. https://doi.org/10.34104/cjbis.022.01120124

Chawki, M., & Abdel Wahab, M. S. (2006). Identity Theft in Cyberspace: Issues and Solutions. Lex Electronica, 11, 1.

Chitadze, N. (2023). Basic Principles of Information and Cyber Security: In M. Boskovic, G. Misev, & N. Putnik (Eds.), Advances in Human and Social Aspects of Technology (pp. 193–223). IGI Global. https://doi.org/10.4018/978-1-6684-5760-3.ch009

Costa, A. F., & Coelho, N. M. (2024). Evolving Cybersecurity Challenges in the Age of AI-Powered Chatbots: A Comprehensive Review. In L. M. Camarinha-Matos & F. Ferrada (Eds.), Technological Innovation for Human-Centric Systems (pp. 217–228). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-63851-0_15

Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57–106. https://doi.org/10.1177/1548512920951275

de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. Electronics, 12(8), Article 8. https://doi.org/10.3390/electronics12081920

Garg, P. K. (2021). Overview of Artificial Intelligence. In Artificial Intelligence. Chapman and Hall/CRC.

Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research, 215, 108975. https://doi.org/10.1016/j.epsr.2022.108975

Gil, Y., Garijo, D., Khider, D., Knoblock, C. A., Ratnakar, V., Osorio, M., Vargas, H., Pham, M., Pujara, J., Shbita, B., Vu, B., Chiang, Y.-Y., Feldman, D., Lin, Y., Song, H., Kumar, V., Khandelwal, A., Steinbach, M., Tayal, K., … Shu, L. (2021). Artificial Intelligence for Modeling Complex Systems: Taming the Complexity of Expert Models to Improve Decision Making. ACM Trans. Interact. Intell. Syst., 11(2), 11:1-11:49. https://doi.org/10.1145/3453172

Hansel, M., & Silomon, J. (n.d.). Ransomware as a threat to peace and security: Understanding and avoiding political worst-case scenarios. Journal of Cyber Policy, 0(0), 1–20. https://doi.org/10.1080/23738871.2024.2357092

Haseeb-ur-rehman, R. M. A., Aman, A. H. M., Hasan, M. K., Ariffin, K. A. Z., Namoun, A., Tufail, A., & Kim, K.-H. (2023). High-Speed Network DDoS Attack Detection: A Survey. Sensors, 23(15), 6850. https://doi.org/10.3390/s23156850

Hossain, R. (2024). Adopting Industry 4.0: A Strategic Solution for Transforming Smart Bangladesh: Prospective Connections, Opportunities, and Challenges. Pakistan Journal of Life and Social Sciences

Hossain, R., Al- Amin, A.-A., Mani, L., Islam, M. M., Poli, T. A., & Milon, M. N. U. (2024). Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country. WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS, 21, 1392–1408. https://doi.org/10.37394/23207.2024.21.114

HOSSAIN, R., AL-AMIN, L. I. S. A., ISLAM, M. M., POLI, T. A., & MILON, M. N. U. (2024). Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country. WSEAS TRANSACTIONS on BUSINESS and ECONOMICS, 21, 1392-1408. http://dx.doi.org/10.37394/23207.2024.21.114

HOSSAIN, R., AL-AMIN, L. I. S. A., ISLAM, M. M., POLI, T. A., & MILON, M. N. U. (2024). Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country.

HOSSAIN, R., AL-AMIN, L. I. S. A., ISLAM, M. M., POLI, T. A., & MILON, M. N. U. Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country.

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. Applied Sciences, 14(13), 5501. https://doi.org/10.3390/app14135501

Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. Internet of Things, 26, 101162. https://doi.org/10.1016/j.iot.2024.101162

Islam, M. A., & Bhuiyan, M. R. I. (2022). Digital Transformation and Society. Available at SSRN: https://ssrn.com/abstract=4604376 or http://dx.doi.org/10.2139/ssrn.4604376

Islam, Z., Bhuiyan, M. R. I., Poli, T. A., Hossain, R., & Mani, L. (2024). Gravitating towards Internet of Things: Prospective Applications, Challenges, and Solutions of Using IoT. International Journal of Religion, 5(2), 436-451. https://doi.org/10.61707/awg31130

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Khan, I. H. (2023). Unlocking the opportunities through ChatGPT Tool towards ameliorating the education system. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 3(2), 100115. https://doi.org/10.1016/j.tbench.2023.100115

Jia, J., Xu, Y., & Li, W. (2024). A study on the strategic momentum of SMEs' digital transformation: Evidence from China. Technological Forecasting and Social Change, 200, 123038. https://doi.org/10.1016/j.techfore.2023.123038

Kabir, M. R., Hossain, R., Rahman, M. M., Sawon, M. M. H., & Mani, L. (2024). Impact of E-Marketing on Book Purchase Tendencies: An Empirical Study on University Undergraduate Students. Journal of Ecohumanism. https://ecohumanism.co.uk/joe/ecohumanism/article/view/3388

Khan, S. A. (2023). E-Marketing, E-Commerce, E-Business, and Internet of Things: An Overview of Terms in the Context of Small and Medium Enterprises (SMEs). In A. Naim & V. A. Devi (Eds.), Advances in Marketing, Customer Relationship Management, and E-Services (pp. 332–348). IGI Global. https://doi.org/10.4018/978-1-6684-8166-0.ch017

Khanom, K., Islam, M. T., Hasan, A. A. T., Sumon, S. M., & Bhuiyan, M. R. I. (2022). Worker Satisfaction in Health, Hygiene and Safety Measures Undertaken by the Readymade Garments Industry of Bangladesh: A Case Study on Gazipur. Journal of Business Studies Pabna University of Science and Technology ISSN 2410-8170 2022, 3(1), 93–105. https://doi.org/DOI:10.58753/jbspust.3.1.2022.6

Kizza, J. M. (2024). System Intrusion Detection and Prevention. In J. M. Kizza (Ed.), Guide to Computer Network Security (pp. 295–323). Springer International Publishing. https://doi.org/10.1007/978-3-031-47549-8_13

Kushardianto, N. C. (2023). Misbehavior Detection System on Vehicular Network based On 2-Step Prediction, Deep Learning Algorithm and Basic Safety Messages [Phdthesis, Université Polytechnique Hauts-de-France ; Institut national des sciences appliquées Hauts-de-France]. https://uphf.hal.science/tel-04207506

Labu, M. R., & Ahammed, M. F. (2024). Next-Generation Cyber Threat Detection and Mitigation Strategies: A Focus on Artificial Intelligence and Machine Learning. Journal of Computer Science and Technology Studies, 6(1), Article 1. https://doi.org/10.32996/jcsts.2024.6.1.19

Lee, K., Lee, J., & Yim, K. (2023). Classification and Analysis of Malicious Code Detection Techniques Based on the APT Attack. Applied Sciences, 13(5), Article 5. https://doi.org/10.3390/app13052894

Li, C., Zhang, Y., Niu, X., Chen, F., & Zhou, H. (2023). Does Artificial Intelligence Promote or Inhibit On-the-Job Learning? Human Reactions to AI at Work. Systems, 11(3), 114. https://doi.org/10.3390/systems11030114

Mahalakshmi, V., Kulkarni, N., Pradeep Kumar, K. V., Suresh Kumar, K., Nidhi Sree, D., & Durga, S. (2022). The Role of implementing Artificial Intelligence and Machine Learning Technologies in the financial services Industry for creating Competitive Intelligence. Materials Today: Proceedings, 56, 2252–2255. https://doi.org/10.1016/j.matpr.2021.11.577

Mani, L. (2019). An Analysis of loan portfolio of Janata Bank Limited. Available at SSRN 4644687. or http://dx.doi.org/10.2139/ssrn.4644687

Mani, L. (2024). Gravitating towards the Digital Economy: Opportunities and Challenges for Transforming Smart Bangladesh. Pakistan Journal of Life and Social Sciences

Masum, M. Y., Mia, M. N., Islam, M. S., Ahmed, G. S., Milon, M. N. U., & Hossain, R. (2024). Poverty Alleviation Through Tourism Development In Bangladesh: Theoretical Perspectives And Empirical Evidence. Educational Administration: Theory and Practice, 30(5), 10050-10064. https://doi.org/10.53555/kuey.v30i5.4045

Meah, M. R., & Hossain, R. (2023). Ownership structure and auditor choice in emerging economy: An empirical study. Indonesian Journal of Business, Technology and Sustainability, 1(1), 12-22.

Mia, M. N., Mani, L., Rahman, M. M., Milon, M. N. U., & Hossain, R. (2024). Gravitating towards Community Based Tourism (CBT): Community Empowerment and Reducing Poverty in Tourism Sector Development in Bangladesh. International Journal of Religion, 5(6), 848-864. https://doi.org/10.61707/e1zchv24

Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences, 13(10), 5875. https://doi.org/10.3390/app13105875

Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2023). A systematic literature review of authorization and access control requirements and current state of the art for different database models. International Journal of Web Information Systems, 20(1), 1–23. https://doi.org/10.1108/IJWIS-04-2023-0072

Molla, C., Mani, L., Bhuiyan, M. R. I., & Hossain, R. (2023). Examining the Potential Usages, Features, and Challenges of Using ChatGPT Technology: A PRISMA-Based Systematic Review. Migration Letters, 20(S9), 927-945. https://doi.org/10.59670/ml.v20iS9.4918

Mulherin, J. H., Netter, J. M., & Overdahl, J. A. (1991). Prices Are Property: The Organization of Financial Exchanges from a Transaction Cost Perspective. The Journal of Law and Economics, 34(2, Part 2), 591–644. https://doi.org/10.1086/467237

Nweke, L. O., & Yayilgan, S. Y. (2024). Opportunities and Challenges of Using Artificial Intelligence in Securing Cyber-Physical Systems. In T. Sipola, J. Alatalo, M. Wolfmayr, & T. Kokkonen (Eds.), Artificial Intelligence for Security: Enhancing Protection in a Changing World (pp. 131–164). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-57452-8_7

Odeyemi, O., Okoye, C. C., Ofodile, O. C., Adeoye, O. B., Addy, W. A., & Ajayi-Nifise, A. O. (2024). INTEGRATING AI WITH BLOCKCHAIN FOR ENHANCED FINANCIAL SERVICES SECURITY. Finance & Accounting Research Journal, 6(3), Article 3. https://doi.org/10.51594/farj.v6i3.855

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access, 12, 12229–12256. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3355547

Poli, T. A., Sawon, M. M. H., Mia, M. N., Ali, W., Rahman, M., Hossain, R., & Mani, L. (2024). Tourism And Climate Change: Mitigation And Adaptation Strategies In A Hospitality Industry In Bangladesh. Educational Administration: Theory and Practice, 30(5), 7316-7330. https://doi.org/10.53555/kuey.v30i5.3798

Rahman, Md. M., Bhuiyan, M. R. I., & Alam, S. M. A. (2024). The Empirical Study on the Impact of the COVID-19 on Small and Medium Enterprises (SMEs) in Bangladesh. Journal of Information Systems and Informatics, 6(1), 527–547. https://doi.org/10.51519/journalisi.v6i1.686

Rahman, Md. M., Islam, Md. M., Khatun, M., Uddin, S., Faraji, M. R., & Hasan, Md. H. (2024). Gravitating towards Information Society for Information Security in Information Systems: A Systematic PRISMA Based Review. Pakistan Journal of Life and Social Sciences (PJLSS), 22(1). https://doi.org/10.57239/PJLSS-2024-22.1.0089

Renaud, K., Warkentin, M., Pogrebna, G., & Van Der Schyff, K. (2024). VISTA: An inclusive insider threat taxonomy, with mitigation strategies. Information & Management, 61(1), 103877. https://doi.org/10.1016/j.im.2023.103877

Saqib, M., & Moon, A. H. (2023). A Systematic Security Assessment and Review of Internet of Things in the Context of Authentication. Computers & Security, 125, 103053. https://doi.org/10.1016/j.cose.2022.103053

Sarker, I. H. (2024). AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. Springer Nature.

Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures. Internet of Things, 25, 101110. https://doi.org/10.1016/j.iot.2024.101110

Shaw, E. (2023). The Psychology of Insider Risk: Detection, Investigation and Case Management. CRC Press. https://doi.org/10.1201/9781003388104

Sivamayil, K., Rajasekar, E., Aljafari, B., Nikolovski, S., Vairavasundaram, S., & Vairavasundaram, I. (2023). A Systematic Study on Reinforcement Learning Based Applications. Energies, 16(3), Article 3. https://doi.org/10.3390/en16031512

Sontan, A. D., Samuel, S. V., Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(2), Article 2. https://doi.org/10.30574/wjarr.2024.21.2.0607

Sontan, A. D., Samuel, S. V., Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(2), Article 2. https://doi.org/10.30574/wjarr.2024.21.2.0607

Taye, M. M. (2023). Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions. Computers, 12(5), 91. https://doi.org/10.3390/computers12050091

Tetteh, G. K., & Otioma, C. (2024). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. Small Business Economics. https://doi.org/10.1007/s11187-024-00946-8

Thakur, M. (2024). Cyber Security Threats and Countermeasures in Digital Age. Journal of Applied Science and Education (JASE), 4(1), Article 1. https://doi.org/10.54060/a2zjournals.jase.42

UDDIN, K. S., BHUIYAN, M. R. I., & HAMID, M. (2024). Perception towards the Acceptance of Digital Health Services among the People of Bangladesh.

Van Dyck, L. E., Kwitt, R., Denzler, S. J., & Gruber, W. R. (2021). Comparing Object Recognition in Humans and Deep Convolutional Neural Networks—An Eye Tracking Study. Frontiers in Neuroscience, 15, 750639. https://doi.org/10.3389/fnins.2021.750639

Wang, F., Gai, Y., & Zhang, H. (2024). Blockchain user digital identity big data and information security process protection based on network trust. Journal of King Saud University - Computer and Information Sciences, 36(4), 102031. https://doi.org/10.1016/j.jksuci.2024.102031

Yang, G. R., & Wang, X.-J. (2020). Artificial Neural Networks for Neuroscientists: A Primer. Neuron, 107(6), 1048–1070. https://doi.org/10.1016/j.neuron.2020.09.005.