The Effect of Artificial Intelligence on Data Security Systems

Suvarna Chaure and Sunil Punjabi(✉)

Department of Computer Engineering, SIES Graduate School of Technology, Nerul, Maharashtra, India
sunil.k.punjabi@gmail.com

Abstract. Artificial intelligence (AI) in its many forms is leading the charge in spurring breakthroughs in digital security in response to the emerging challenges in the post-COVID environment. On the one hand, businesses are finding it challenging to handle security risks related to a range of concerns, including web domain, decision-making, quality control, and system openness, to name a few. However, to comprehend the relationship between AI and those problems, research over the past ten years has concentrated on security capabilities based on instruments like platform complacency, intelligent trees, modeling techniques, and outage management systems. The literature has long acknowledged how important artificial intelligence will be in directing industries and reshaping the transportation, health, and education sectors. This paper presents an Artificial Intelligence-based Security method for Banking Sector (AISBS). AI is one of the best technologies for mapping and preventing unforeseen hazards from consuming an organization. The proposed method can be used to categorize, and resolve cyberattack issues. Algorithms like the Enhanced Encryption Standard (EES) encrypt and decrypt data to guarantee the security of financial sector data. The K-Nearest Neighbor (KNN) algorithm generates predictions by using its training data to make predictions.

Keywords: Artificial intelligence · Machine Learning · Data Security · Cyber Security

1 Introduction

Artificial intelligence (AI) is based on the idea that there are some striking similarities between the human and computer brains. This theory is reinforced by psychology, It holds that both individuals and animals' act like machines that process information through associative memory devices [1]. These days, scientists are investigating how artificial intelligence (AI) might be used to address various system security problems in a range of industries. As a result, AI is widely regarded as an interdisciplinary field of study that garners a lot of interest in the social and economic spheres due to its numerous technological advancements in the area of system security provided [2]. Investing in AI technology is a common trend to address everyday security issues in industries including transportation, medical, and statistical data [3].

P. Pareek et al. (Eds.): IC4S 2024, LNICST 599, pp. 408–419, 2025.
https://doi.org/10.1007/978-3-031-77081-4_32

Some argue that certain data from important industries have aided in the development of AI. These industries include e-commerce [4], businesses, and the government. These data sources have contributed significantly to the improvement of various machine-learning algorithms and solutions, particularly those that address systems security. Furthermore, China and Russia have recognized the significance of AI for overall competitiveness and system security. In a similar vein, China has acknowledged the significance of AI for housing security and hopes to lead the industry. Some of the world's most developed nations have already started making those efforts in order to maximize the significant advantages it offers. Despite AI's rapid advancement in recent years, there hasn't been much conversation about system security. As such, it is important to familiarize oneself with the most recent breakthroughs pertaining to the issue in order to chart the field's advancements and their consequent effects.

This work's contribution can be summed up as follows:

1. To understand impact of AI on Data Security
2. To develop a framework for improving cyber security in the financial sector.
3. To put into practice a machine learning-based strategy which generates predictions to classify data privacy.

The paper is organized as follows: A variety of theoretical ideas about AI in systems security in Sect. 2. It also outlines the impact of AI in security and a detailed review of cyber security measures in Financial Sector 2. A description of the suggested methodology can be found in Sect. 3. Section 4 deals with results followed by conclusions.

2 Literature Survey

After the idea of a digital computer was developed, the concept of artificial intelligence (AI) was presented to determine whether a machine could "think" or perform activities that people could [5]. The goal of artificial intelligence (AI), a broad field under information and computer technologies (ICT), is to create autonomous systems that function similarly to how people make decisions [6]. Artificial intelligence (AI) is mentioned as artificially intelligent machines with the volume to process information and make decisions [7]. A mechanism can study from skills by processing an infinite amount of data and spotting designs in it, as shown by technologies like image recognition [8] and Siri [9]. Moreover, artificial intelligence (AI) encompasses a varied range of related technologies, as well as machine learning [10] and neural networks [11], to name just a couple.

This study also pinpoint some AI study areas:

a) A broad range of advancements are collectively referred to as machine learning, which allows computers to run algorithms on the basis of predefined commands and gathered data. This gives the machine the ability to learn without human guidance, adapting its algorithm to the circumstances and reprogramming itself. Examples of this include Google and Siri when they are performing voice-activated tasks. Moreover, aberrant activity is tracked by video surveillance [12].

b) The next phase of machine learning is called deep learning, where a computer can learn and characterise data at quite a few points of abstraction, just like the human brain, and perform jobs based on text, graphics, and voice [13]. Deep learning uses a complicated information design with multiple layers to accomplish this. This is exemplified, for example, by building a certification data framework for educational institution key indicators to solve issues like identity identification.
c) Neural networks are comprised of a design recognition system that machine/deep learning functions to select the best neural network models of the container tracks and thereby gain access. This allows neural networks to achieve knowledge from experimental information and come up with its peculiar results, like an auto-steering gear system with a fuzzy regulator [14].
d) Skilled organizations are made up of package configurations that help produce responses to specific questions submitted by a user or by another software package. Expert knowledge is dedicated to a specific section of the application that uses reasoning to obtain answers based on contextual data and subsequent decision-making [15].
e) Cybersecurity, including behavior analysis, access control, surveillance, and computer crime. An example of this may be seen in computer vision, where algorithms are used to analyze images and differentiate between processors and beings using CAPTCHA (Completely Automated Public Turing Test) methods.

2.1 Impact of AI on Security

Companies all around the world are urged to integrate artificial intelligence into their operations because of its many advantages, according to Das et al. [16]. One of these advantages is that AI becomes more intelligent with time. With time, artificial intelligence a technical intelligence—will be able to comprehend and enhance network security (see Fig. 1). Using machine learning and deep learning techniques, the system analyzes how business networks behave over time to identify patterns and classify the networks based on shared characteristics. Before responding, artificial intelligence keeps track of any deviations or security situations from the norm [17]. Artificial neural networks use their learnt patterns to assist design cybersecurity measures that thwart cyberattacks. Artificial intelligence keeps learning, making it more difficult for hackers to overcome. Inadequate intelligence causes people to miss all the hazards that an organization faces. However, a business can reduce unforeseen hazards posed by hackers and attackers who are always coming up with new attacks by implementing artificial intelligence. A corporation can transfer data more easily while simultaneously detecting and identifying risks hidden in the chaotic traffic thanks to artificial intelligence, such as residential proxy.

In cybersecurity, vulnerability management is essential for safeguarding an organization's network. Artificial intelligence should be used to identify, assess, and neutralize threats because organizations encounter new ones daily to keep them safe and secure. Research on artificial intelligence aids in the analysis and evaluation of security measures to control vulnerability [18]. For example, to handle critical security jobs and manage vulnerability on time, the system identifies weak places in business networks and computer systems. Using artificial intelligence in cybersecurity also has the benefit of enhancing overall security. Threats to cyber security are always evolving because of

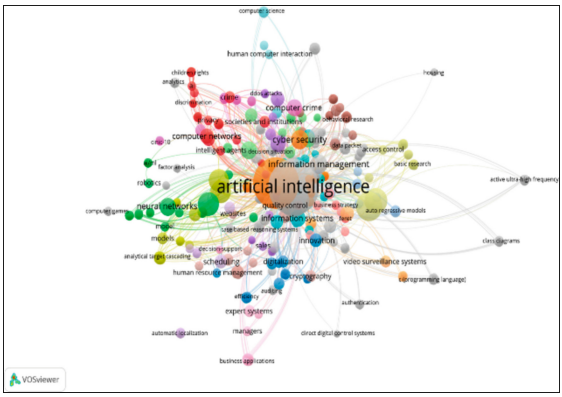

Fig. 1. Collection of keywords of Artificial Intelligence (AI)

technical advancements [19]. As hackers and attackers get more skilled, reaching a high degree of security becomes more difficult.

When artificial intelligence is used in cybersecurity, there are very few duplicates. According to Zope and Ingle [20], artificial intelligence replicates human characteristics to ensure that there are no flaws by removing redundant cybersecurity methods. This is because hackers are always improving their hacking tactics. The system detects and mitigates the main security risks. Furthermore, according to Chan et al. (2019), artificial intelligence examines the depth of an organization's network to find security holes that could compromise the network system. Artificial intelligence implementation speeds up detection and reaction times. Threat identification is the initial stage of network security for a business. Organizations should therefore act swiftly to detect dangers, such as untrusted threats, to prevent their networks from being permanently destroyed.

The solution is recommended because it simplifies security responsibilities by monitoring potential threats and scanning the entire system. Additionally, artificial intelligence ensures that only authorized individuals can access data by providing authentication security. An company ought to add an extra security layer in order to collect private and sensitive data. Because of the higher level of security, users of the company's network will feel secure while utilizing it. Secure authentication for user account logins will be ensured by the application of artificial intelligence in cybersecurity. Facial recognition software, fingerprint scanners, and CAPTCHA are examples of tools that help with identification. In addition, the information gathered by the devices helps validate the authenticity of the log-in study.

2.2 Cyber Security in Financial Sector Management

To avoid illegal access to a machine, net, or part of skill, cybersecurity is important. A business wants a keen cybersecurity experts in today's technically advanced situation in order to monitor possible cyber-crimes and develop counterstrategies (see Fig. 2). Displays the mechanisms that make up cybersecurity. Safe expense, individual secrecy online, antivirus package, firewalls, mobile safety, safety padlocks, information

guard, machine shield, and a specific universal protection are all measured to be main mechanisms of cybersecurity.

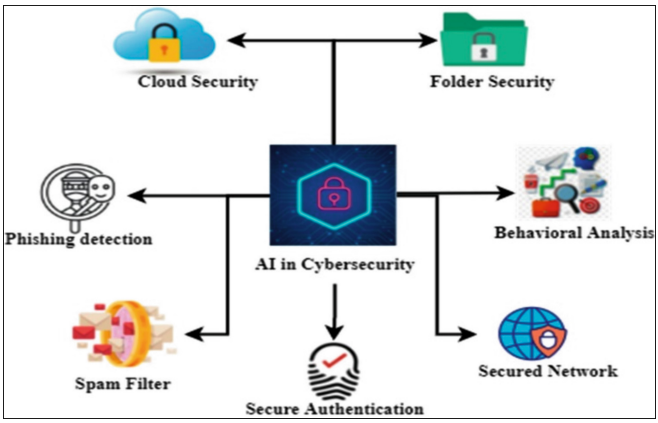

Fig. 2. AI in Cybersecurity

Finance safety is essential to data safety for any business that grips automatic fund transfer or dealings. As such, businesses should stay up to date on the latest advancements in e-commerce and safe business techniques and seek advice on how to incorporate them into their operations.

Fig. 3. Essential elements of cybersecurity in financial management

To protect both the security of their networks and the safety of their customers, banks need to implement cyber risk management strategies. Data breaches can undermine public confidence in financial institutions, which is why banks are quite concerned about

them. They risk losing a sizable portion of their customer base if their cybersecurity solution is inadequate.

Antivirus application guards machines from bugs by looking for, sensing, and getting rid of them. The majority of secure applications are designed to work automatically in the backdrop, preventing against cybercrimes as quickly as they occur. If users have a frequently updated and tested antivirus applications, they should feel safe from known threats. Antivirus application is important to a user's overall cybersecurity sanitation. The main objective of cybersecurity, sometimes referred to as digital safety, is to take the appropriate security measures to protect networks and data against damage, fraud, and unwanted access. Robust or costly computer equipment is secured with locks, sirens, and tracking numbers. An unauthorized user on a network could be a targeted attacker or an resourceful piece of malware. The application of artificial intelligence in cybersecurity is seen in (see Fig. 3). Every incoming communication is flagged for unsuitable material by Artificial Intelligence's spam filtering. Because malware is intelligent and adaptable, it may be identified.

Through folder security, businesses can safeguard their software and platform operations through data stacking, deletion, and backup storage. Other alternatives include tokenization, encryption, biometric verification, and essential control. The aim of network security is to safeguard a banking industries infrastructure by preventing a variety of harmful bugs from joining or proliferating within a network. This can be achieved through a variety of strategies. Users require different kinds of network security (endpoint, online, wireless), as well as network security (firewalls, VPN encryption), in order to maintain network safety. Numerous methods, such as machine learning, artificial intelligence, big data, and statistics are used in behavior analysis.

Machine learning is used in a subsection of professional intellect to find novel designs, connections, and visions. A significant portion of the work that data analysts have historically done is automated thanks to artificial intelligence.

This paper discusses how these research streams can be utilized to identify, prevent, and determine the best course of action while minimizing risks and maximizing profits through the tremendous potential of AI in systems security that are employed by both nations and enterprises. Through a variety of security measures, such as redundant video surveillance systems, VOIP, and a reliance on different platforms for protection (also known as platform complacency), artificial intelligence (AI) may even prove to be more successful than humans at thwarting possible attacks.

3 Artificial Intelligence Based Security for Banking Sector (AISBS)

With the aid of artificial intelligence, the suggested paradigm, AI based Security for Banking Sector(AISBS), evaluates every intrusion and enables users to decide whether it is safe. If not, it halts admission and notifies the control room or the individuals gaining access. The overall systematics of the suggested system is depicted in (see Fig. 4).

All the financial data of the clients, the banking industry, and other information are kept in a cyber-secure database. When a single individual, client, or threat attempts to access such data, the firewall prevents untrusted entry. The data may be stored for real entries. Both a public key and a private key are used to encrypt these data. After

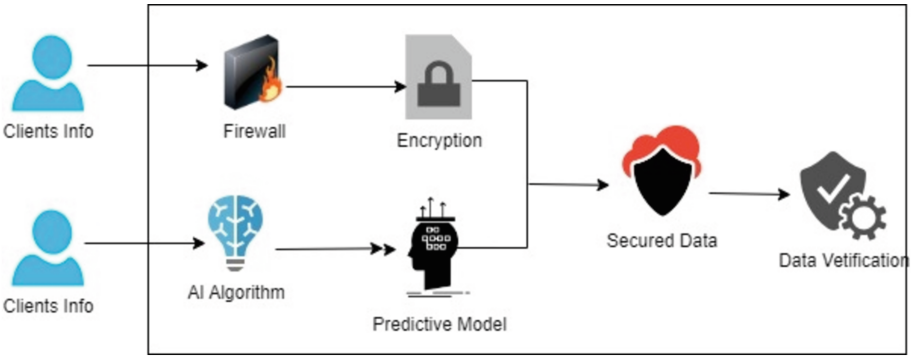

Fig. 4. Proposed Methodology for Artificial Intelligence based Security for Banking Sector

encryption, they will be stored in the database, guaranteeing that the information will be more secure in the event of a cyberattack. The KNN technique is used to create the best prediction model from both trusted and untrusted data. This algorithm creates a model using data provided by individuals with the necessary authorization.

Information availability is carefully examined following the development of a successful prediction model. In the event that a virus or unknown entry attempts to access data from the database, the prediction model will detect it, stop it from entering, and alert the appropriate person. The suggested model makes the financial data safer the financial services sector offers a wide range of products and payment alternatives to individuals and organizations. This economic sector is made up of depositors, investment groups, investors, credit institutions, real estate brokers, and health insurance. Without a firewall, commercial and financial banks are unable to conduct transactions or exchange sensitive data. The Crystal Act of 1933 acted as a firewall by forbidding banks and brokerage firms from cooperating. Furthermore, computers can employ extensive Fig. 4. Proposed Technique security procedures to scan every packet for malware. Proxies can function as filters in addition to load balancers, keeping bugs from tainting the web servers they are placed next to.

Enhanced Encryption Standard Technique: EES is an iterative cipher rather than a Feistel cipher. The fundamental idea is a "substitution–permutation network.". In this way, numerous processes are connected to one another. While some only need changing one input for another, others involve bit shuffles, or permutations. The information is transformed into the EES model, as seen in (see Fig. 5). To protect their data from being lost or stolen, clients or authorized individuals encrypt their financial information using a security key before converting it to cipher text.

By using the same security key to encrypt and decrypt the data, the same individual can access the information once more, making it more secure against cyberattacks as shown in Fig. 6. Among other things, the financial statements are intended to provide information about an organization's profitability, financial situation, and strategy. This information helps readers of financial accounts make better resource allocation decisions. Simply said, system security keys are the password for the permitted device. A network

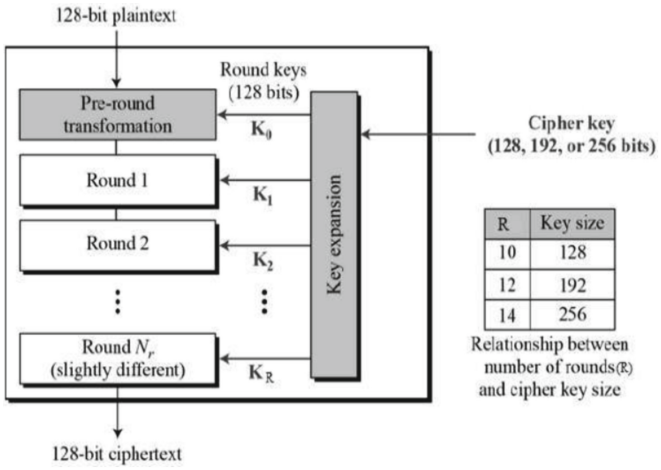

Fig. 5. Enhanced Encryption techniques

security key, a kind of system passcode sign that protects a system and its components against illegal invasions, is required to access the communication network.

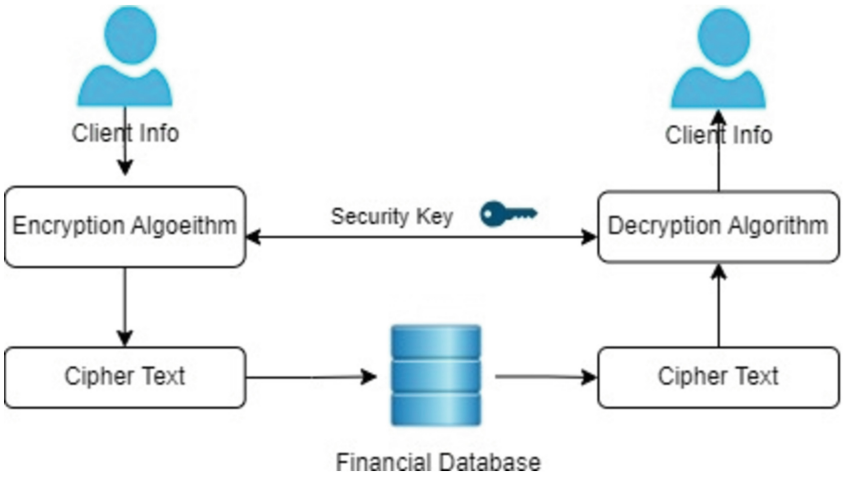

Fig. 6. Flow diagram of proposed approach

Prediction: As mentioned in (see Fig. 6) KNN generates predictions in real time by comparing each training example to an input model and calculating their similarities. Depending on their structure, the information being provided can be linked with different distance measurements. Prior to employing KNN, it is a good practice to rescale or normalize the data. All learning values are considered when using KNN for predicting what kind of testing information should be provided. Which group of "K" training information is most likely to contain the test data is determined by the KNN algorithm.

It makes no biased use of the experimental data and learns nothing during the training phase. However, a training session is not necessary.

4 Results

The AISBS approach is the basis for the experimental data reported in this part, and its cataloguing presentation is related with other algorithms that yield comparable results. An Intel Core i7 processor running Windows 8 64-bit at 2.84 GHz with 64 GB of RAM was used for this experiment.

After loading the Python 3 emulator, the security application was used to look over the testing network's susceptibility data. Data about the network topology were collected using the ArcGIS toolkit. Python was utilized by the researchers to write the project's code. The study examined almost 250 thousand combinations of assault and defense tactics over the course of the trial. MATLAB 2018a was used to analyze and visualize data. The ability of individuals to manage the gathering and use of personal data is referred to as data privacy. Since safeguarding confidential customer information and proprietary resources is the initial step in maintaining numerical data and private information secrecy, information safety and confidentiality go hand in hand. The outcomes are contrasted with the most recent methods, including Linear Discriminant Analysis (LDA), Principal Component Analysis (PCA), and Support Vector Machine (SVM). Personal Identifying Information poses a serious risk to the privacy of data. In today's creative society, handling lots of gathered data might be difficult because of both the amount and the worth of the data. The objective is to set up the framework necessary to facilitate and promote future performance and to allow growth unhindered. It is imperative to have proper planning, finance, and infrastructure (people, processes, tools, and equipment). This speaks to an organization's or business strategy's capacity to expand in the face of increased productivity without being limited by its internal structure or financial resources. Scalable pricing is useful for raising revenue in a software company.

The main goal of data retention is to safeguard important IT assets through a system of rules and guidelines. Paperwork, charts, identity, and connectivity were all handled during this project. Data security is one method for determining and lowering the risk connected to data transportation and storage. Banks are required to prevent illegal access to the financial information of their clients. Customers may lose important time, savings, and personal information if cybersecurity is inadequate. Consumers can experience anxiety or dread, and businesses might miss the people's faith in protecting their currency and private data.

The efficacy AI for Security for Banking Sector (AISBS) in increasing cyber security in the banking sector has been assessed. The results show that, when it comes to data privacy (18.3%), scalability (17.2%), risk reduction (13.2%), data protection (16.2%), and attack avoidance (11.2%), AISBS outperforms more traditional approaches to cyber security as shown in (see Fig. 7) and (see Fig. 8). This shows that the suggested strategy is effective in fending off cyberattacks in the banking industry.

AISBS uses artificial intelligence (AI) technologies to give a comprehensive approach to cyber security, such as the Enhanced Encryption Standard (EES) and the K-Nearest Neighbor (KNN) algorithm. In the banking industry, the EES technique is used

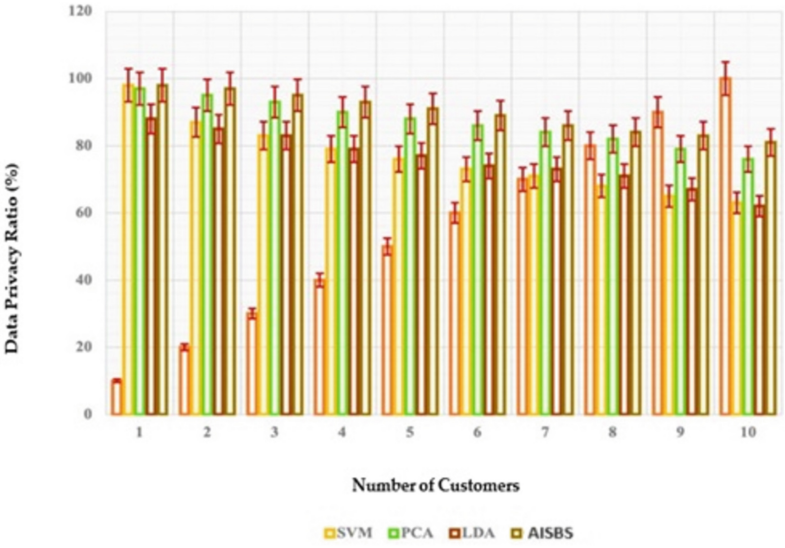

Fig. 7. Comparison of data privacy

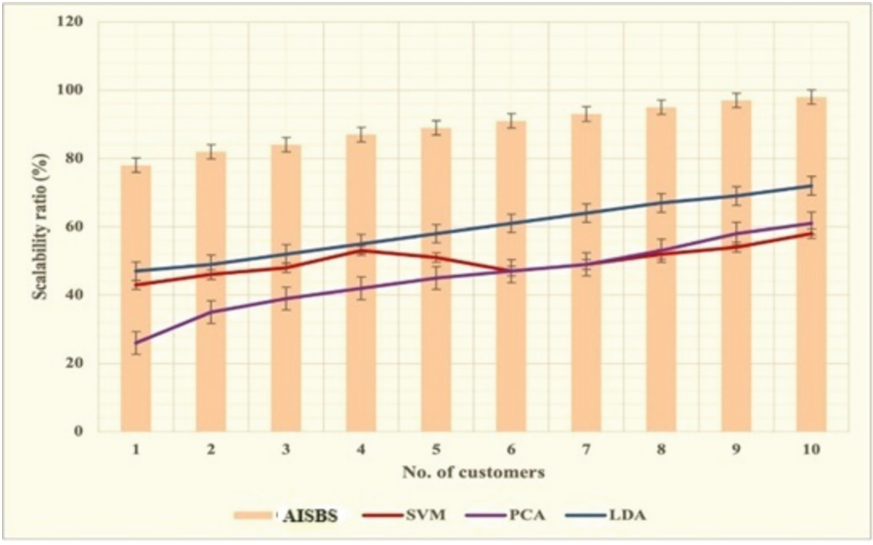

Fig. 8. Interpretation of scalability

to encrypt and decode data, while the KNN algorithm is utilized to detect and stop malicious data. The KNN algorithm, which studies from the training data and generates predictions, is used in the proposed method to classify cyberattack problems and offer remedies.

5 Conclusion

Enhancement of confidentiality, scalability, hazard mitigation, data security, and attack prevention are just a few advantages of the AI-driven suggested AISBS paradigm that is revolutionizing safety in the finance industry. The study illustrates the effectiveness of the KNN algorithm with the Enhanced Encryption Standard (EES) in anticipating and preventing breaches. There have been positive results in terms of risk reduction, privacy, and data security. The significance of integrating artificial intelligence (AI) techniques into cyber security solutions for the financial services industry is illustrated by this study.

The organization's analytical values are 96.1% for privacy of data, 97.2% for scalability, 98.7% for risk reduction, 95.4% for data security, and 94.3% for threat evasion. Blockchain technology has the potential to further enhance information security, and this is a topic for future research. Overall, this creative method strengthens online safety in the banking sector and is an enhancement over conventional cyber security protocols. With its innovative approach to security for the banking industry, AISBS enhances data protection, privacy, scalability, risk mitigation, and attack avoidance. Using AI algorithms like EES and KNN provides a comprehensive view of cyber security that is absent from more traditional methods. The suggested method for addressing cyber threats in the banking industry is a significant improvement over the procedures currently used in cyber security. The overall results and conclusions demonstrate the uniqueness and value of the suggested approach to improving cyber security in the banking sector.

References

1. Sheptunov, S.A., Sukhanova, N.V.: The problems of design and application of switching neural networks in creation of artificial intelligence. In: Proceedings of International Conference Quality Management, Transport and Information Security, Information Technologies, pp. 428–431. IEEE, Yaroslavl (2020)
2. Kim, M.S.: The design of industrial security tasks and capabilities required in industrial site. In: Proceedings of ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD-Winter, pp. 218–223. IEEE Computer Society, Seoul (2021)
3. Melville, N. McQuaid, M.: Generating shareable statistical databases for business value: multiple imputation with multimodal perturbation. Inf. Syst. Res. (2012)
4. Zhu, F., Li G.: Study on security of electronic commerce information system. In: Proceedings of 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011, Zhengzhou, China (2011)
5. Hu, X., Wan, K.: Bank financial innovation and computer information security management based on artificial intelligence. In: Proceedings of 2nd International Conference on Machine Learning, Big Data and Business Intelligence. IEEE, Taiyuan (2020)
6. Singh, J.: Real time BIG data analytic: security concern and challenges with machine learning algorithm. In: Proceedings of Conference on IT in Business, Industry and Government: An International Conference by CSI on Big Data. IEEE, Indore (2014)
7. Choi, H., Young, K.J.: Practical approach of security enhancement method based on the protection motivation theory. In: Proceedings of 21st ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter). IEEE, Ho Chi Minh City (2021)

8. Sun, Y., Men, T., Huang, G.: Analysis and design of China's E-Bank CAPTCHA. In: WIT Transactions on Information and Communication Technologies, vol. 61, pp. 1343–1350. WIT Press, Southampton (2014)
9. Popkova, E., Alekseev, A.N., Lobova, S.V., Sergi, B.S.: The theory of innovation and innovative development AI scenarios in Russia. Technol. Soc. **63**, 101390 (2020)
10. Zhong, X., Ji, G.: RETRACTED ARTICLE: research on the development measures of housing security system. In: Proceedings of 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC, Zhengzhou, China (2011)
11. Workman, M.: Validation of a biases model in strategic security decision making. Inf. Manag. Comput. Secur. **20**, 52–70 (2012)
12. Li, F.: The research on information safety problem of digital campus network. In: Proceedings of 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011, Zhengzhou, China (2011)
13. Sukhanova, N.V., Sheptunov, S.A., Glashev, R.M.: The Neuron Network Model of Human Personality for Use in Robotic Systems in Medicine and Biology. In: Proceedings of IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS. IEEE, Sochy, Russia (2019)
14. Ekenberg, L., Danielson, M., Boman, M.: Imposing security constraints on agent-based decision support. Decis. Support. Syst. **20**, 3–15 (1997)
15. Loideain, N.N., Adams, R.: From alexa to siri and the GDPR: The gendering of virtual personal assistants and the role of data protection impact assessments. Comput. Law Secur. **36**, 105366 (2020)
16. Khelvas, A., Demyanova, D., Gilya-Zetinov, A., Konyagin, E., Khafizov, R., Pashkov, R.: Adaptive distributed video surveillance system. In: Proceedings of International Conference on Technology and Entrepreneurship—Virtual (ICTE-V). IEEE, Bologna (2020)
17. Brahan, J.W., Lam, K.P., Chan, H., Leung, W.: AICAMS: Artificial intelligence crime analysis and management system. Knowl. Based Syst. **11**, 355–361 (1998)
18. Nikolskaia, K., Naumov V.: Ethical and legal principles of publishing open source dual-purpose machine learning algorithms. In: Proceedings of IEEE International Conference Quality Management, Transport and Information Security, Information Technologies, IT and QM and IS. IEEE, Yaroslavl (2020)
19. Hu, Z., Chiong, R., Pranata, I., Bao, Y., Lin, Y.: Malicious web domain identification using online credibility and performance data by considering the class imbalance issue. Ind. Manag. Data Syst. **119**, 676–696 (2019)
20. Angioni, M., Musso, F.: New perspectives from technology adoption in senior cohousing facilities. TQM J. **32**, 761–777 (2020)