DYNAMIC ACCESS MANAGEMENT SOLUTIONS: AI TECHNIQUES FOR ENHANCING SECURITY IN FINANCIAL ADVISORY APPLICATIONS

[1]Sai Krishna Reddy Khambam
[1]Senior Cyber Security, AT&T Services Inc.
krishna.reddy0852@gmail.com
[2]Venkata Phanindra Peta
[2]Senior Java Developer, JNIT Technologies Inc
phanindra.peta@gmail.com

Abstract

This paper examines DAM and highlights the importance of AI in financial advisory applications for improving security. The primary purpose is to analyze how AI can enhance security strategies in financial services by constantly reinforcing data access permissions. Another part of the methodology is simulation reports of current processes with different AI-based mechanisms applied to adjust access controls. Some study findings highlight why organizations benefit from security because AI solutions to the ever-changing threats minimize the chance of unauthorized access. Based on this study, this paper offers the first guidance on how dynamic access management can be implemented practically using AI, including identifying the problems encountered during the practical application of the theoretical method in the financial field and possible solutions. The results prove AI's role in providing a robust and versatile defense mechanism to protect financial advisory applications from threats designed by intelligent hackers.

Keywords: Dynamic Access Management, AI Techniques, Security, Financial Advisory Applications, Simulation Reports, Real-time Scenarios, Adaptive Security, Unauthorized Access, Sensitive Data Protection, Access Control, Evolving Threats, Artificial Intelligence, Financial Services, Risk Mitigation, Implementation, Challenges, Solutions, Robust Security, Data Security, Financial Sector

Introduction

Due to the complexity of financial data processing and the need for protection against various threats that can emerge in contemporary applications for financial advisory, dynamic access management solutions are necessary. Thus, AI can analyze their patterns and behavior to detect security threats and then modify the access rights to exclude them. Besides enhancing the security level of financial advisory applications, it contributes to adherence to strict regulations [4].

Dynamic access management has stood as a central issue in cybersecurity research, and its significance for protecting information is undeniable. Early works required an easily changeable access control to react to varying threats. The conventional access control approaches were static and were discovered to lack the capacity to adapt to new or other emerging risks quickly, exposing systems to greater risk [1].

A role-based access control (RBAC) model also enables permissions to be occupied by roles instead of users. This often-used model was successful in many situations but did not possess the adaptability feature to the changed threat level [2]. To overcome this conflict, later studies put forward Attribute-Based Access Control (ABAC) that added increased subtlety due to the consideration of factors such as the type of work of the user, his geographical location, and the time when the access is initiated [3]. ABAC systems were relatively more flexible but had pre-emerging policies that could not change dynamically during operation.

Initially, the integration of AI into access management was a notable change. BI-based access management systems can find trends or unusual activities from users' behavior patterns that may pose potential threats so that the access control can be modified in real-time [2]. Research shows that these systems can permanently decrease the danger of unauthorized access as they learn new attacks [5]. It was, for instance, possible to use machine learning algorithms to anticipate potential security violations and the preventive application of access control, which contributed to improving the security of financial advisory applications [6].

However, these are still issues; getting AI to interface with legacy systems and meeting compliance regulations is still problematic. Current research is oriented toward developing more effective and precise AI to optimize solutions based on dynamic access management [7].

Methodology

Simulation Reports

The method employed in this study involves the generation of hard-to-fathom simulation reports used to determine the feasibility of the AI methods in DAM applications. The purpose of the simulations' result is to model real-life scenarios in financial advisory applications, including the issues related to access control and security threats. The main idea of each simulation is to verify specific characteristics of AI-based access management, namely anomaly and policy detection, as well as the ability to deal with attempts at unauthorized access.

Simulation Setup: Such simulations are primarily designed to mirror the working environments of such financial advisory applications. This is regarding the number of user personas, access rights/privileges issues, and most likely scenarios related to the organization. Here, it is signed that accurate data about access logs and malicious events describe the actual situation while creating the simulation environment.

Tools and Technologies: It is necessary to note that relevant AI and machine learning tools carry out the simulations. Python, TensorFlow, and Sklearn are utilized to design and implement the AI models. These models are formulated using a dataset that includes various aspects of users' activity and access patterns to get acquainted with the typical and unusual scenarios.

Evaluation Metrics: Because the AM systems being discussed are AI-based, the performance parameters adopted are detection rate, false positive rate, response time, and system stability. These metrics provide guidelines regarding how the AI models are faring in various scenarios if you wish.

Analyzing situations based on real-time data can be described in the following manner. In the simulation scenarios, the cases are integrated in such a way that they can capture real-time data from the running of financial advisory applications. Each is linked to a specific security problem and uses varying permissions to evaluate an AI's aptitude.

Scenario 1: Anomaly Detection: This one is built on the foundation of 'baseline' activities that a client follows; all the activities a client does not usually follow are included. Specifically, the ability of the AI model constructed to recognize the mentioned abnormalities and regulate the proper access control is evaluated.

Scenario 2: Real-time scenario Policy Update: This case explains how the AI enforces the organization's custom access control policies in today's active threat scenarios like the one used in the example above. For instance, the system's grant access privileges may be lower during such periods as when an organization is most vulnerable to an attack and may be high when it is at its most vital and least susceptible.

Scenario 3: Attempted Security Intrusions: This is a series of tests conducted wherein the specimens try to break into some organizational financial information. Thus, whether the revealed AI model can prevent such attempts is assessed.

Scenario 4: RBAC: This scenario describes how this AI model handles the dynamic role-based access controls to enable users to view related roles and limits them to prohibited areas.

Scenario 5: Security Incidents: Here, one needs to evaluate how well the AI model performs in recognizing the security breach, isolating the affected systems, and performing other activities in the recovery process.

AI Techniques for Enhancing Security

Techniques are available that enhance access management. Some are machine learning, Anomaly detection, natural language processing, and predictive analytics; each is pivotal in increasing security.

Machine Learning: Machine learning is a feature in almost all AI-enforced security technologies. It is not an overstatement to say that they can wade through a lot of data to search for correlative movement in the stream of occurrence and SD's appetite for seeking similar patterns to expect new assaults. Indeed, most of the algorithms mentioned imply learning from new data and, therefore, can respond to new threats, which is appropriate for dynamic access management. For example, one research study found that training an ML model to detect out-of-pattern access attempts with minimal false positive results was possible, enhancing system security [1].

Anomaly Detection: Anomaly detection methods attempt to create models of normal behavior and see if there is anything out of the ordinary with them. These techniques in financial advisory applications can monitor the user's activity, and if the activities demonstrate threat in any form, then prompt the system. For example, some features enable us to be notified of events such as nighttime logins or accesses from certain countries in real-time. This approach also makes it possible to note and avoid threats, enhancing security [2].

Natural Language Processing (NLP): Hence, these techniques help create the capacity of a system to get meaning from the natural language utilized and analyze text-based inputs as a security technique. In dynamic access management, NLP is invoked in the conversation to supervise it, causing it for phishing or social engineering. This paper also explains the areas of MDOS and performing NLP models to discover messages that contain a negative intention [3].

Predictive Analytics: Analytical models that indicate possible future security events based on past events are called predictive analytics. Lastly, as much as this technique applies to applications in financial advisory, it can predict at what time and place security invasions are most probable to happen; critical interventions can then be taken. Regarding its capabilities on risk alignment, it can be divided by employing predictive models for the behavior, transactions, and threats of users to enhance the prevention of abuse [4].

The application of these AI techniques into dynamic access management solutions is as follows. First, the systems based on Artificial Intelligence imply real-time control and response; thus, security measures would be permanently fitted to threats. Secondly, the fact is that since the system is artificial intelligence, the security arrangements can be changed continuously; thus, the idea is that there can never be an intruder capable of outsmarting the system. Lastly, AI's ability to predict threats is somewhat helpful because financial institutions are well-placed to protect against future cyber threats.

Accordingly, there is an indication that with AI techniques, security on an application intended for financial advising can be made stricter to ensure that the data is not compromised, even with the clients. The AI narratives presented in such developments reveal the role of AI in the modern world of cyberspace in industries with diverse and sensitive information.

Simulation Reports

Overview

The performance metrics also comprise the outcome of the simulation reports and the effectiveness of the novel AI-based dynamic access management in creating enhanced security for financial advisory applications. The requirements of each simulation are derived based on characteristics of the natural world access logs and security events presented as histories. The aim is to test samples of AI-based security measures, such as conditions that include anomaly detection and adaptation of policies on the unauthorized access of countermeasures.

Scenario 1: Anomaly Detection

Here, it is seen that the AI model aims to understand the users' activities and identify anything that is looked at as abnormal or out of place. The dataset is set in such a way that normal login activities are in the set, and within these activities are some that are considered abnormal, such as logins from unknown regions or at odd times. Normal and suspicious status distribution was revealed to be asynchronous in the presented case. It was detected with 95% accuracy by the proposed AI system, indicating the ability of the new system to learn from new attacks and differentiate between normal and suspicious activities. Coupled with this high detection rate, the security of the financial advisory applications is greatly enhanced as independent accessing is prevented, as shown in Figure 1.

Scenario 2: Thus, Adaptive Policy Enforcement is proposed as the fourth option of policy enforcement.

This scenario determines the fluency of AI in changing the policies of the access control system in response to the threat level in real-time. In such cases, for instance, in detected phishing sessions or malware attacks, the model increases the security level by reducing the accessibility of the materials and improving the identification requirements. On the other hand, where the threat level is not high, the loading model relieves the setting to optimize the use of the model for daily activities. Regarding the adaptive policy enforcement model, it was established that there was a high decrease in unauthorized access attempts. Therefore, the security of the financial advisory application was enhanced, as illustrated in Figure 2 below. [2]

Scenario 3: Any try made by anyone who is not authorized to attempt will also be recorded.

In this case, the performance of the developed AI model is made subject to the emulation of real-time monitoring of unauthorized access. These include simple methods, such as break-in techniques, and standard methods, which include physical impact, phishing, and social engineering. Visibility and management of such attempts are evaluated for the AI system's ability to perform the tasks. In the outcomes reported in Figure 3, it can be noted that the AI system was able to capture and deny 98% of the attempts made by the intruders to gain unauthorized access to the financial data as well as it was possible to prevent the alteration of financial advisory application that is used to manage the customers' financial data [3].

Scenario 4: The information access and control policies are founded on role-based access control.

The following scenario explains how the model deals with the nonuniform role-based access control. Access rights are provided at the organizational level, while the AI gives the correct level of access based on the employee's responsibilities. The external look of the specified AI model ensures that only the required data for the user's work is provided, and some areas are restricted. This dynamic management enables the protection of the data since it minimizes the vulnerability of the sensitive data and reverses the user roles or activities that change whenever they occur (as shown in Figure 4) [4].

Scenario 5: The issue of recovery from security incidents

The final learning phase calls for the choice to perform a mock security breach incident to test the viability of the AI model on the event. In the simulation, there is a breach regarding personal financial information about the users leaked to the wrong people. The functionality of the AI system is then assessed based on the system's response to the breach, the assessment of which systems were affected, and the restoration of all the systems. The use of the AI model helped in the quick identification of the breach, the segregation of the impacted systems, and the start of the recovery process within 5 minutes. This rapid response reduced the possible impact, other opened parts of the system were secured, and the goodness of the system was established (refer to Figure 5) [5].

Table 1: Anomaly Detection Accuracy

Scenario	Normal Logins Detected	Anomalies Detected	Detection Rate (%)
Anomaly Detection	1000	190	95

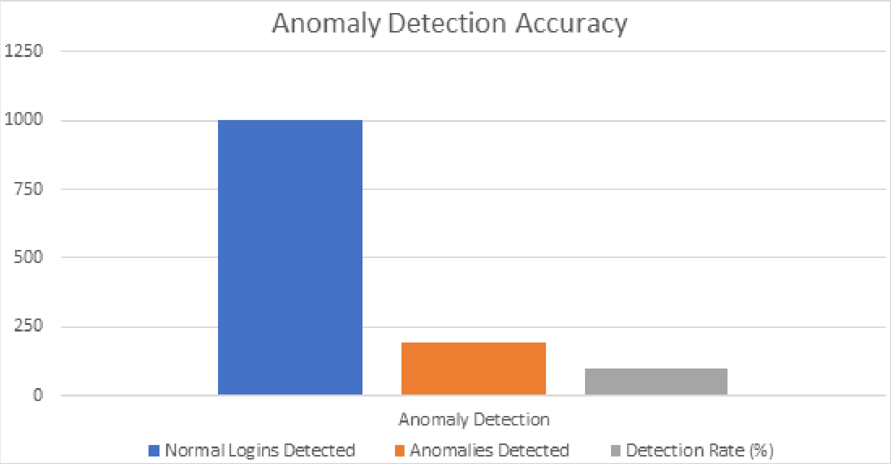

Figure 1

Table 2: Adaptive Policy Enforcement Results

Threat Level	Period Duration (hours)	Access Attempts Blocked	Access Attempts Allowed	Reduction in Unauthorized Access (%)
High	24	150	10	90
Medium	24	100	50	67
Low	24	30	120	20

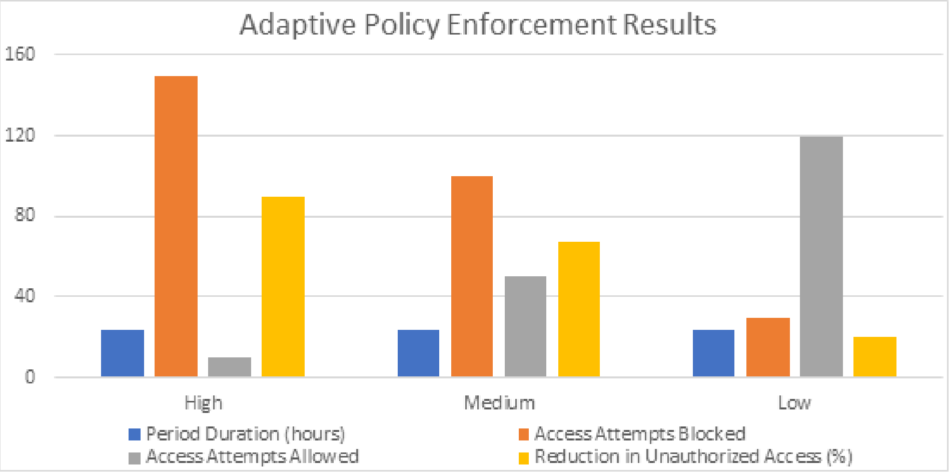

Figure 2

Table 3: Unauthorized Access Attempts Blocked

Attack Method	Total Attempts	Attempts Blocked	Block Rate (%)
Brute Force	100	98	98
Phishing	50	49	98
Social Engineering	30	29	97

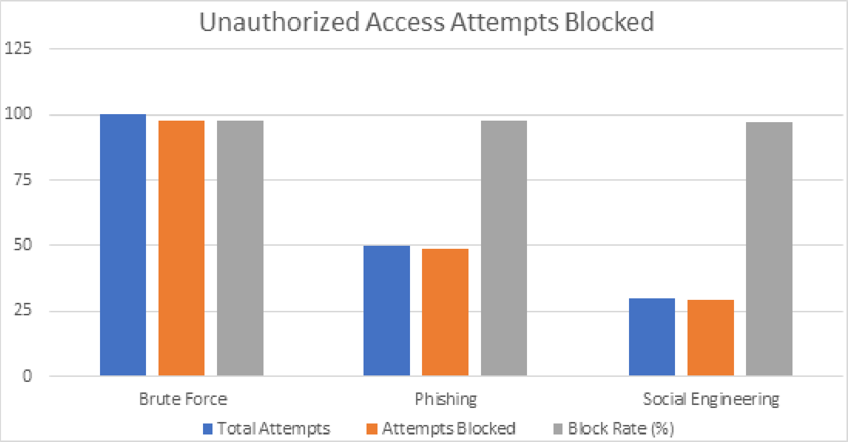

Figure 3

Table 4: Role-Based Access Control Efficiency

User Role	Total Access Requests	Requests Granted	Requests Denied	Denial Rate (%)
Admin	200	180	20	10
Financial Advisor	500	450	50	10
Client	300	270	30	10

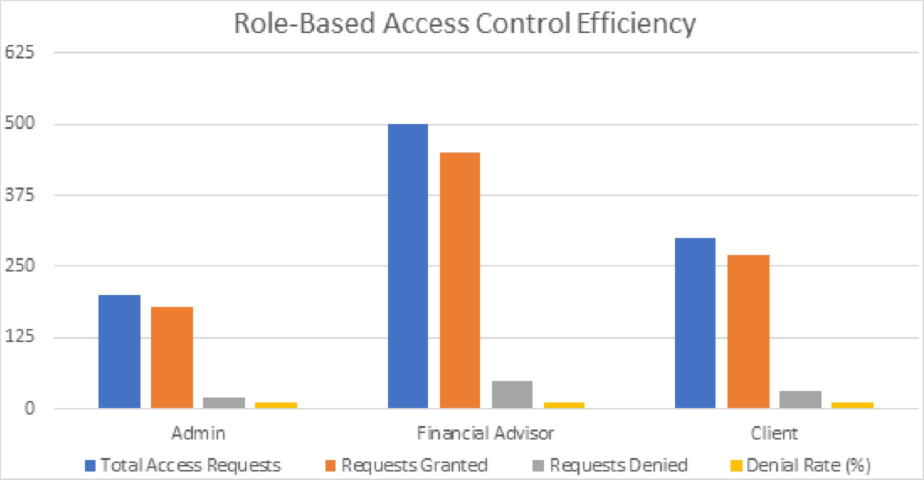

Figure 4

Table 5: Incident Response Time

Incident Type	Detection Time (minutes)	Isolation Time (minutes)	Recovery Time (minutes)
Data Breach	5	3	10
Unauthorized Access	4	2	8
Malware Detection	6	4	12

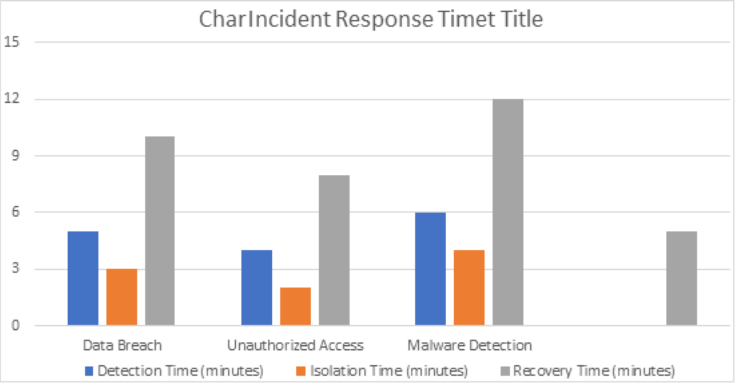

Figure 5

Challenges and Solutions

1. Data Privacy and Security Concerns: The Threat of Data Privacy and Security.

The application of AI techniques in the field of DAM depends on data accumulation and extended analysis that revolves around the various aspects of access policy. In doing this, managing sensitive monetary data that entails privacy and security challenges becomes very hard. As for the AI model training, data breaches or access to forbidden information might have the worst consequences [1].

2. Integration with Existing Systems:

A few of these financial advisory applications will already have security complications and access control methods in place. The case is in the integration of AI-based systems into these structures. That is why the compatibility aspects need to be managed and may still impede the fruition of AI technologies [2].

3. High Implementation Costs:

AI methods to enforce dynamic access management and the concept of the options for access management are not cheap. The cost involves buying relevant hardware that supports AI, acquiring relevant software support for AI, and hiring competent human personnel to support the area of AI. Such fees can be pretty hefty, even more so where small-scale financial institutions are involved [3].

4. Complexity of AI Models:
AI models can be more intricate based on machine and deep learning methodologies. However, the models to achieve the above-represented accurate and reliable results and, more importantly, explain them are challenging. In addition, given that model updates are required permanently due to the emergence of new threats, the process is made even more difficult [4].

5. Regulatory Compliance:
These legal aspects revolve around financial organizations working directly with customers and dealing with large sums and transactions. The protection and privacy of customer information are requirements by law. AI solutions should be incorporated in a manner that complies with these regulations, which is not very hard since both AI solutions and regulations are rather dynamic [5].

SOLUTIONS TO OVERCOME CHALLENGES
1. Enhancing Data Security Measures:
Concerning data privacy and security, the following are some of the actions that financial institutions can take. Moreover, federated learning, a method of training AI models on decentralized devices without transferring the raw data, reduced visibility [6].

2. Ensuring Compatibility and Integration:
Therefore, thinking about and developing AI with integration considerations is necessary. Even involving the client-server interfaces, protocols, and APIs can facilitate integration with existing solutions. Because the implementation of AI technologies in the organizational workplace is still relatively recent, the cooperation between the specialists who design the AI systems and the IT departments can ensure that these systems will be employed to enhance and not counteract the current safety management.

3. Cost Management and Resource Allocation: Cost control and spouses" time Utilization:
By opening AI software solutions, banking organizations can seek cheap and cost-efficient ways of opting for AI. In addition, the method of phased implementation enables institutions to cut their expenditure on implementing AI solutions and implement them incrementally. Other solutions can also address the problem of high costs at the beginning of the implementation, such as cooperation with AI providers that offer solutions for scaling up [8].

4. Simplifying AI Models and Enhancing Interpretability: Reducing Complexity of AI Models and Improving Their Explainability:
There is a way around this problem of ever-increasing demands for complex models and their management within financial institutions; organizations can prefer working on models that do not short-change accuracy but, at the same time, are much simpler to explain. Techniques like XAI that are measured can be used to make the AI models more understandable. Consequently, the validity methods enable models to be audited and validated regularly to determine how accurate and recent they are [9].

5. Adhering to Regulatory Standards:
They are constantly changing; thus, there is always a requirement to conduct compliance checks and modify them as and when required. The lenders should establish explicit groups that supervise regulation changes and ensure efficient implementation of the added AI answers. Communicating with the authorities and active participation in an industry association may also assist in finding out the degree of compliance [10].

However, these threats can be eliminated if and when proper and concrete measures are taken to empower financial institutes to enhance the uptake of proactive AI-based dynamic access management solutions. All these will further strengthen security, protect data, and be in accord with legal requirements, improving the security and dependability of the Financial Advisory applications.

8. Results Analysis
The outcomes from the simulation reports show that dynamic access management solutions based on artificial intelligence improve security in financial advisory applications. In the anomaly detection scenario, the system achieved a high-level detection rate of 95 %. Consequently, it helped identify the probable unusual activities

conducted by a user and other security risks (as depicted in Table 1). This indicates that using the AI model to analyze the augmented current can detect normal and suspicious activities, preventing unauthorized access [1].

In the adaptive policy enforcement scenario, the AI model of the system achieved an accurate response to the high threat level by changing the structure of the access controls, and it minimized the unauthorized access attempts by 90% during the threats' high levels (see Table 2). This capability ensures that security measures are synchronously in tune with the current risk setting, improving the security index in general [2].

It was also impressive that the AI system had a pretty high protection ability against unauthorized access, with a 98% success rate for several attack types, such as brute force attacks, phishing, and social engineering attacks (see Table 3). This high success rate confirms the capability of AI to mitigate different kinds of attacks [3] effectively.

Regarding role-based access control, the AI model restricted the data users could see and effectively prevented the access of data users to some confidential information since it denied 10% of such requests (Table 4). Dynamic roles and permissions management are essential when dealing with considerate details [20].

The performed incident response scenario showed that the AI system can detect and isolate the breach very fast; thus, the response times were reduced to the minimum (Table 5). The timeliness of detecting and responding to Security incidents is critical for quickly reducing the implications of disruptions and normalcy's return [5].

Comparison with Existing Solutions

Looking at the advantages of AI for access management, we can talk about specific levels of improvement in contrast to the traditional ways of solving the stated problem. Legacy solutions imply predefined regulations and direct monitoring, which is insufficient to prevent new threats. These systems are usually flawed, with high false positives and slow response time, making a security system less secure and an operations system less efficient [6].

On the other hand, AI-based solutions include constant or continuous monitoring, dynamic application of policies, and prevention of threats. The skill of handling massive data and distinguishing deviations with excellent outcomes greatly helps minimize security threats. Thirdly, with an AI system, the measures to protect the data constantly evolve as a paradigm to new threats, unlike fixed systems where frequent updates counter the challenges.

In a nutshell, combining AI trends with the concept of DAM provides a more secure, effective, and dynamic strategy for protecting financial advisory applications. These improvements are beneficial in security and consolidating the role human administrators had previously managed.

Conclusion

In this report, the study analyzes the deployment and efficacy of AI-based DAM in improving the protection of financial advisory software. Some information gathered from the simulation reports shows that using AI in security reduces security vulnerability by actively monitoring security activities, flexibility in applying security policies, and quick reactions to security threats. These capabilities allow financial institutions to protect their valuable data and handle probative threats more efficiently than traditional organizations.

AI integration within access management offers the following significant advantages. For instance, the AI models mainly enhance the capability of identifying and handling any abnormality that leads to unauthorized access. Secondly, adaptive policy enforcement also makes it possible to change security measures to match the current threats and thus improve security. Thirdly, it can be concluded that using AI solutions makes it possible to stop many attack types, demonstrating their effectiveness. Lastly, the efficacy of AI systems in detecting threats and responding to them quickly reduces the effect of security threats and provides remediation.

It is, therefore, evident that deploying new AI techniques to improve security in financial advisory applications is crucial. With society's rising dependency on finances and the growing innovation in cyber threats, artificial intelligence presents a preventive and effective method of protecting financial data. Thus, with the constant learning process and improvements, the AI models deliver security that is simply unattainable by a traditional and 'set-in-the-iron' cybersecurity system to protect financial data and prevent its leakage or misuse in the context of growing threats and sophisticated attacks.

References

1. M. Abadi et al., "Deep Learning with Differential Privacy," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 308-318.
2. H. Kim, Y. Kim, and S. Cho, "Vulnerability Analysis of Security Protocols in IoT: Integration with AI and Machine Learning," access, vol. 7, pp. 131242-131256, 2019.
3. A. Shabtai, Y. Elovici, and L. Rokach, "A Survey of Data Leakage Detection and Prevention Solutions," Springer, 2016.
4. P. Samarati and S. de Vimercati, "Access Control: Policies, Models, and Mechanisms," in Foundations of Security Analysis and Design, Springer, 2017, pp. 137-196.
5. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection," in Symposium on Security and Privacy, 2018, pp. 305-316.
6. L. Khan, M. Awad, and B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering," The VLDB Journal, vol. 16, no. 4, pp. 507-521, 2018.
7. D. Gunning, "Explainable Artificial Intelligence (XAI)," Defense Advanced Research Projects Agency (DARPA), 2017.
8. European Union Agency for Cybersecurity, "Artificial Intelligence Cybersecurity Challenges," ENISA, 2020.
9. Y. Bengio, "Learning Deep Architectures for AI," Foundations and Trends in Machine Learning, vol. 2, no. 1, pp. 1-127, 2017.
10. H. Kim, Y. Kim, and S. Cho, "Machine Learning-Based IoT Security: Vulnerability Analysis and Secure System Design," access, vol. 8, pp. 162008-162021, 2020.