Annals of Process Engineering and Management

www.apem.reapress.com

Ann. Proc. Eng. Manag. Vol. 3, No. 2 (2026) 128–135.

Paper Type: Original Article

Optimizing the Cyber Crisis Management Process with an Artificial Intelligence Approach in Iranian Banks

Samira AzadSanjari[1,*], Seyed Kamal Charsoughi[1]

[1] Department of Industries, Faculty of Industrial and Systems Engineering, Tarbiat Modares University, Tehran, Iran; azad@aut.ac.ir; skch@modares.ac.ir.

Citation:

Received: 17 January 2025 *Revised: 18 February 2025* *Accepted: 20 April 2026*	AzadSanjari, S., & Charsoughi, S. K. (2026). Optimizing the cyber crisis management process with an artificial intelligence approach in Iranian banks. *Annals of process engineering and management*, *3*(2), 128-135.

Abstract

Given the increasing frequency and complexity of cyber-attacks in recent years, leveraging Artificial Intelligence (AI) to enhance Cyber Crisis Management (CCM) has become a necessity. According to various cybersecurity reports, banking malware and financial fraud have experienced significant growth over the past decades. In light of the escalating sophistication of cyber threats and the rapid emergence of new attack vectors, traditional crisis management methods are no longer sufficient to meet the security demands of Iranian banking institutions. In this research, we propose an optimized AI-driven framework for CCM. In our proposed approach, AI is employed in the pre-crisis phase to predict complex cyber threats, allowing for the rapid deployment of defensive measures that minimize the likelihood of a crisis. During the crisis itself, AI enhances the Incident Response (IR) process through advanced automated algorithms capable of analyzing vast volumes of data in minimal time. The integration of AI into the CCM process facilitates faster response times, process automation, reduction of human error, real-time analysis of high-volume and complex datasets, and enables continuous learning and adaptive improvement.

Keywords: Artificial intelligence, Cyber crisis management, Electronic banking, Cybersecurity, Threat detection, Incident response, Vulnerability assessment.

1 | Introduction

An efficient banking system is essential for active participation in competitive markets and the successful execution of electronic commerce activities. This technology not only enhances operational efficiency and productivity but also transforms the way financial businesses operate, communicate, and interact with the external world [1]. With the expansion of electronic services in financial and credit institutions, emerging risks and threats have surfaced for banks [2]. The growing prevalence of electronic banking represents a double-

Corresponding Author: azad@aut.ac.ir

Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0).

edged sword—bringing both opportunities and significant threats. The failure to identify emerging risks and threats in electronic banking can negatively impact a bank's reputation and revenue, and in severe cases, may even jeopardize national security.

According to cybersecurity reports, one of the recent major incidents involved the data leak of customers from 20 Iranian banks. In response, the company, Tosan, negotiated and paid IRLeaks to prevent the dissemination of the compromised information. Below, several cybersecurity reports highlighting security threats faced by Iranian banks are presented. According to Kaspersky's annual report, the number of Android users targeted by banking malware has increased over the past year. The details of this report are illustrated in "*Fig. 1*".

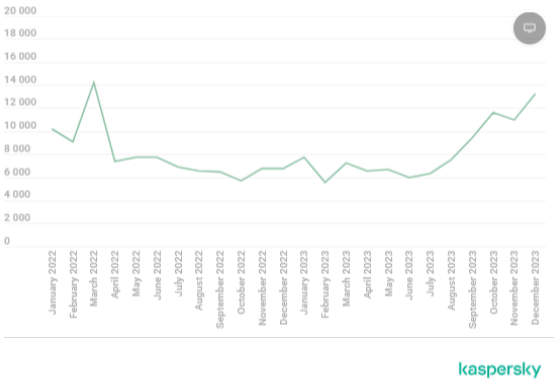


Fig. 1. The number of Android users targeted by banking malware increased significantly during the period from 2023 to 2024.

Over the past few decades, with the advancement of infrastructure and technologies, state-sponsored attacks have increasingly shifted to the cyber domain. Given Iran's geostrategic significance, the country has become a focal point for such cyber operations. According to a recent report by Kaspersky, illustrated in "*Fig. 2*", Iran ranks 8th globally in terms of ransomware infection rates based on data from the past month.

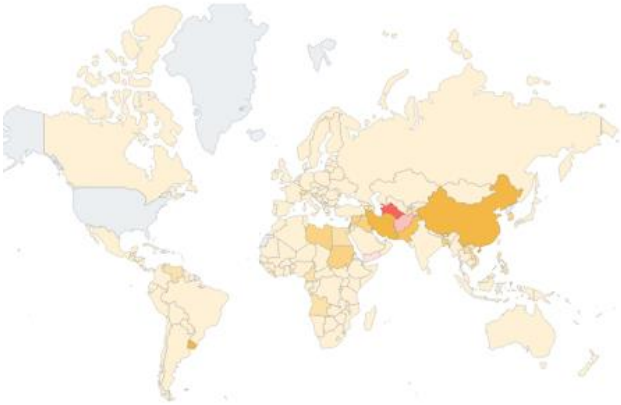


Fig. 2. Kaspersky report on the global ransomware infection landscape (past month).

Therefore, the planning and implementation of Cyber Crisis Management (CCM) strategies are essential to mitigate the risks associated with electronic banking in Iran. The emergence of Artificial Intelligence (AI) has brought transformative changes to cybersecurity, both in terms of threats and opportunities. Unlike traditional cybersecurity approaches, which primarily rely on predefined rule-based systems, AI introduces a new era of automated defense mechanisms. At the core of this transformation are Machine Learning (ML) and Deep Learning (DL) techniques [3]. AI-powered systems can analyze vast and complex datasets with remarkable accuracy and speed. By employing ML, these systems are capable of recognizing patterns and correlations within datasets, enabling them to detect emerging sophisticated cyber-attacks that are often undetectable by conventional methods [4].

A study conducted by the University of Westminster (London Metropolitan University) analyzed the role of AI and ML in digital forensic investigation and incident response (DFIR) processes [5]. Another study from the University of Newcastle, Australia, highlighted the ongoing challenges faced in crisis management during cyber-attacks [6]. Building upon these studies, the proposed framework focuses on enhancing CCM—particularly Incident Response (IR)—while addressing the limitations of traditional crisis management methods, such as low real-time responsiveness when handling large-scale data.

In this proposed model, considering the existing challenges in traditional CCM across Iranian banking institutions, we introduce an AI-driven improvement to the CCM process. The CCM framework is structured into two core phases: pre-crisis and during-crisis. This model outlines AI-based strategies for threat detection, vulnerability assessment, and IR to enhance the overall effectiveness and agility of the crisis management cycle.

To outline the proposed framework, Section 2 of the paper introduces the foundational concepts necessary for understanding the study, including electronic banking and its associated risks, CCM, AI, ML, and DL. Subsequently, Section 3 reviews the existing body of research and discusses the current challenges in crisis management within the context of electronic banking, to establish the relevance and significance of the contributions made in this study. In Section 4, we present our proposed AI-driven framework for enhancing the CCM process. Finally, Section 5 provides a summary and conclusion of the study's findings.

2 | Fundamental Concepts

2.1 | Electronic Banking and Associated Risks

Electronic banking refers to services that allow customers to access banking facilities remotely through secure channels, without the need for physical presence at a bank branch. This approach provides customers with the ability to perform financial transactions efficiently, saving both time and cost [7]. Electronic banking encompasses various channels, including internet banking, mobile banking, telephone banking, ATM-based banking, and card-based banking.

Electronic banking is associated with several types of risk, such as security risk, privacy risk, operational risk, reputational risk, legal risk, and strategic risk. Given the adverse impact these risks can have on bank capital and revenues, it is critical to anticipate, assess, and mitigate them effectively [8].

2.2 | Cyber Crisis Management

Crisis management has long been a significant concern for organizations operating in competitive markets. A crisis is an unpredictable event or incident—natural, technical, or social—that can cause severe disruption or damage. As the frequency and complexity of cyber-attacks increase, the need for effective CCM becomes crucial in minimizing the impact of such incidents.

By implementing proactive planning and maintaining preparedness based on the latest technologies and threat intelligence, potential cyber risks can be identified in advance, enabling preemptive action to reduce financial damages. Furthermore, proper planning and intelligent decision-making during the IR phase can significantly reduce the harmful effects of a cyber crisis [9].

2.3 | Artificial Intelligence

AI refers to systems that demonstrate intelligent behavior comparable to human cognition. AI has significantly transformed the detection of advanced threats through two central techniques: ML and DL. These techniques are further elaborated in the subsequent sections.

2.3.1|Machine learning

ML focuses on the study of algorithms and statistical models that enable systems to learn from data and improve performance over time, without being explicitly programmed. ML-based systems acquire knowledge from patterns in data rather than relying on fixed rules or instructions.

Traditionally, ML approaches are categorized into three primary types based on the nature of input signals or feedback mechanisms:

I. Supervised Learning (SL): In this approach, the model is trained on labeled datasets, with the goal of accurately predicting outcomes for new, unseen data. For example, in a malware detection system, ransomware data may be labeled as "threat" while legitimate financial transaction data is labeled as "safe."

II. Unsupervised Learning (UL): This approach involves discovering hidden structures in data without any labeling. The goal is to detect underlying patterns, such as in clustering algorithms, which are widely used for anomaly detection.

III. Reinforcement Learning (RL): Here, the model learns through trial-and-error interactions with an environment. The system receives rewards or penalties for each action taken, and it aims to maximize cumulative rewards over time.

2.3.2|Deep Learning

DL is a subfield of ML and represents one of the most advanced implementations of AI. DL is directly associated with the development of intelligent systems, such as those used for threat detection. It utilizes multi-layered artificial neural networks to identify deep and complex patterns in data.

DL performs particularly well when processing large-scale, high-dimensional datasets. Deep Neural Networks (DNNs) are capable of automatically learning hierarchical data representations and are commonly employed to extract intricate features from raw data. Key types of DL architectures include:

I. Convolutional Neural Networks (CNNs): CNNs are designed specifically for structured data such as images. They can be used to analyze network traffic patterns or identify malicious signatures within executable malware files [10].

II. Recurrent Neural Networks (RNNs): RNNs are tailored for processing sequential or time-series data. A distinguishing feature of RNNs is their ability to pass outputs from one time step as inputs to the next. RNNs are well-suited for Natural Language Processing (NLP) and are commonly applied in log analysis and anomaly detection over time.

III. Generative Adversarial Networks (GANs): GANs consist of two competing networks—a generator (G) that creates synthetic data, and a discriminator (D) that distinguishes between real and generated data. Through this adversarial training, GANs evolve dynamically, allowing threat detection systems to adapt continuously to emerging attack vectors [11].

A summary of ML and DL applications in threat detection is presented in "*Table 1*".

Table 1. Summary of ML and DL techniques in threat detection.

Technique	Application in Threat Detection
SML	Detection of threats and malware
UML	Identification of unknown threats and anomalous behavior
RML	Adapting response strategies to new threats
CDL	Detection of malware patterns in network traffic
RDL	Identifying abnormal behavior over time
GDL	Augmenting threat intelligence datasets

3 | Challenges in Cyber Crisis Management in Iran's Electronic Banking Sector

Given the increasing complexity of cyber-attacks in recent years, traditional crisis management approaches are no longer adequate to meet the evolving needs of Iranian banks. For instance, in the pre-crisis phase, vulnerability assessments are typically conducted manually through code reviews or configuration audits. These methods suffer from human error, low processing speed, and limited coverage based on outdated knowledge, making them ineffective in today's rapidly changing threat landscape [12–15].

Moreover, traditional threat detection techniques—namely Signature-Based Detection (SBD) and Rule-Based Detection (RBD)—fail to detect Advanced Persistent Threats (APTs) or zero-day attacks due to their reliance on predefined patterns and static rules [16], [17].

In the IR phase, conventional methods also rely on manual tools, leading to slow detection and analysis of forensic evidence. These approaches are prone to human error and struggle with timely recovery following a crisis [18–20]. Given the high sensitivity of banking services, the adoption of AI across all stages of CCM has become imperative.

4 | Proposed AI-Driven Solution for Cyber Crisis Management

To address the shortcomings of traditional CCM, this paper proposes AI-powered solutions integrated into each phase of the crisis lifecycle. Specifically, the framework enhances two main stages: pre-crisis and during-crisis. These stages include AI-based methods for vulnerability assessment, threat detection, and IR.

4.1 | Pre-Crisis Phase

During the pre-crisis stage, practical and strategic planning enables banks to develop the necessary preparedness to confront cyber incidents and minimize potential threats. Proactively conducting vulnerability assessments and remediating identified weaknesses are essential measures for preventing cyber crises. Additionally, detecting threats and responding rapidly helps reduce risk and improve the CCM cycle.

The use of AI in this phase—particularly for attack simulation and cyber drill execution—enhances readiness for real-world incidents. The proposed framework elaborates on two core AI-based actions in the pre-crisis phase: AI-driven Vulnerability Assessment and AI-powered Threat Detection.

4.1.1 | AI-Based vulnerability assessment

In the proposed approach, AI is employed to accelerate both the scanning and remediation of vulnerabilities. AI-powered vulnerability scanning tools leverage complex algorithms and extensive datasets to identify patterns, anomalies, and security flaws. ML algorithms analyze data to prioritize critical vulnerabilities and autonomously initiate remediation.

AI-based scanners automate the detection of security issues in software code structures and resolve them with high speed and accuracy. Overall, the use of AI in vulnerability assessment enhances efficiency, improves precision, and ensures adaptability in mitigating emerging threats through intelligent remediation.

Several AI-based tools have been developed to support vulnerability analysis. These include:

I. IBM security Qradar.

II. Qualys AI-driven threat detection.

III. Tenable.sc.

These tools have proven essential for enhancing the intelligence and responsiveness of crisis management processes.

4.1.2|AI-Based threat detection

As cyber-attacks have become more sophisticated, AI-based threat detection techniques are now necessary to identify advanced threats. In the proposed framework, AI enables the detection of APTs and zero-day attacks, thus reducing the impact of potential breaches before they escalate into full crises.

Notably, the use of advanced ML and DL algorithms enables large-scale data analysis, automated and high-speed pattern recognition, and continuous learning—all of which are critical for identifying new and evolving cyber threats. Examples of AI-based threat detection platforms include:

I. Darktrace.

II. Splunk User Behavior Analytics (UBA).

III. FireEye Threat Analytics Platform (TAP).

Integrating these tools into a bank's cybersecurity infrastructure is vital for early identification and mitigation of threats.

4.2|During Crisis

While preventive measures and proactive planning significantly reduce the likelihood of a crisis, encountering cyber incidents remains inevitable. Therefore, effective response planning is critical to minimizing the impact of such events. In the proposed framework, the integration of AI into the cyber crisis response process has led to substantial improvements, reducing both response time and the resulting damages.

4.2.1|AI for Incident Response

The use of AI during the IR phase enhances automation, speed, and precision in managing cyber crises. AI employs advanced algorithms to process large volumes of security alerts, prioritize incidents, and automatically implement necessary containment and mitigation actions. It also plays a crucial role in the forensic analysis of incident data, accelerating evidence collection and interpretation.

Overall, AI enhances all key components of the IR process—including incident identification, evidence preservation, analysis, threat eradication, system recovery, post-incident learning, and reporting. AI-driven techniques reduce response time, automate operations, minimize human error, and enable rapid processing of large-scale and complex data through DL and ML.

Several AI-based IR platforms that can support CCM include:

I. Darktrace.

II. Cynet.

III. Palo Alto Networks Cortex XSOAR.

5|Conclusion

With the exponential growth of online businesses and electronic payment systems, the frequency and severity of cyber threats and crimes have also increased. Since banking systems play a pivotal role in maintaining a nation's economic stability, the lack of a robust CCM strategy can lead to serious consequences.

As cyber-attacks become more advanced and dynamic, adopting an AI-driven crisis management approach is crucial for the detection and mitigation of emerging threats. This paper presents a framework that applies AI techniques for vulnerability assessment, threat detection, and IR, while also introducing cutting-edge tools to support each stage of the crisis management process.

The integration of AI in CCM improves operational efficiency by reducing human error, increasing response speed, and enhancing analytical precision. However, the deployment of AI in this context also brings challenges that warrant further investigation in future studies, such as:

I. Data Privacy Concerns (DPC): AI systems require extensive data collection to learn and predict, which poses privacy risks, particularly in sensitive banking environments.

II. Explainability and Transparency (E&T): Many AI models, especially DNNs, operate as "black boxes" with opaque decision-making processes, complicating the justification of threat assessments.

III. Bias and Fairness (B&F): AI systems trained on biased datasets may lead to unfair or unbalanced decisions, potentially undermining the integrity of security operations.

Addressing these concerns is essential for the safe and responsible adoption of AI in cybersecurity.

References

[1] Urbinati, A., Chiaroni, D., Chiesa, V., & Frattini, F. (2020). The role of digital technologies in open innovation processes: an exploratory multiple case study analysis. *R\&D management*, *50*(1), 136–160. https://doi.org/10.1111/radm.12313

[2] Abdou, H. A., English, J., & Adewunmi, P. O. (2014). An investigation of risk management practices in electronic banking: The case of the UK banks. *Banks & bank systems*, *9*(3), 19–31. https://b2n.ir/tj1485

[3] Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions. *International journal on semantic web and information systems (IJSWIS)*, *18*(1), 1–43. https://doi.org/10.4018/IJSWIS.297143

[4] Borode, A., & Olubambi, P. (2024). Optimisation of artificial intelligence models and response surface methodology for predicting viscosity and relative viscosity of GNP-alumina hybrid nanofluid: incorporating the effects of mixing ratio and temperature. *The journal of supercomputing*, *80*(4), 4841–4869. https://doi.org/10.1007/s11227-023-05652-y

[5] Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic science international: Digital investigation*, *48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

[6] Alasmari, A. O. (2018). A review of the challenges of the crisis management during the cyber attacks. *Journal of contemporary scientific research (ISSN (online) 2209-0142)*, *2*(7), 1–9. https://b2n.ir/eq2687

[7] Alghazo, J. M., Kazmi, Z., & Latif, G. (2017). Cyber security analysis of internet banking in emerging countries: user and bank perspectives. *2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICETAS.2017.8277910

[8] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of xidian university*, *14*(7), 1523–1536. https://doi.org/10.37896/jxu14.7/174

[9] Chafjiri, M. B., & Mahmoudabadi, A. (2018). Developing a conceptual model for applying the principles of crisis management for risk reduction on electronic banking. *American journal of computer science and technology*, *1*(1), 31–38. https://doi.org/10.11648/j.ajcst.20180101.15 %0D

[10] Yamashita, R., Nishio, M., Do, R. K. G., & Togashi, K. (2018). Convolutional neural networks: an overview and application in radiology. *Insights into imaging*, *9*(4), 611–629. https://doi.org/10.1007/s13244-018-0639-9

[11] Salehi, P., Chalechale, A., & Taghizadeh, M. (2020). *Generative adversarial networks (GANs): An overview of theoretical model, evaluation metrics, and recent developments*. ArXiv Preprint ArXiv:2005.13178. https://doi.org/10.48550/arXiv.2005.13178

[12] 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), 1–42. https://doi.org/10.3390/electronics12061333

[13] Khan, S., & Parkinson, S. (2018). Review into state of the art of vulnerability assessment using artificial intelligence. In *Guide to vulnerability analysis for computer networks and systems: an artificial intelligence approach* (pp. 3–32). Springer. https://doi.org/10.1007/978-3-319-92624-7_1

[14] Xiaopeng, T., & Di, T. (2019). A distributed vulnerability scanning on machine learning. *2019 6th international conference on information science and control engineering (ICISCE)* (pp. 32–35). IEEE computer society. https://doi.ieeecomputersociety.org/10.1109/ICISCE48695.2019.00016

[15] Kumar, S., Gupta, U., Singh, A., & Singh, A. (2023). Artificial intelligence: Revolutionizing cyber security in the digital era. *Journal of computers, mechanical and management*, *2*, 31–42. http://dx.doi.org/10.57159/gadl.jcmm.2.3.23064

[16] Markevych, M., & Dawson, M. (2023). *A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (AI)* [presentation]. International conference knowledge-based organization (Vol. 29, pp. 30–37). http://dx.doi.org/10.2478/kbo-2023-0072

[17] Kim, S., Hwang, C., & Lee, T. (2020). Anomaly based unknown intrusion detection in endpoint environments. *Electronics*, *9*(6), 1–19. https://doi.org/10.3390/electronics9061022

[18] Javed, S. H., Ahmad, M. Bin, Asif, M., Almotiri, S. H., Masood, K., & Ghamdi, M. A. Al. (2022). An intelligent system to detect advanced persistent threats in industrial internet of things (I-IoT). *Electronics*, *11*(5), 1–25. https://doi.org/10.3390/electronics11050742

[19] Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE communications surveys & tutorials*, *23*(4), 2525–2556. https://doi.org/10.1109/COMST.2021.3117338

[20] Hassan, S. K., & Ibrahim, A. (2023). The role of artificial intelligence in cyber security and incident response. *International journal for electronic crime investigation*, *7*(2), 49–72. https://doi.org/10.54692/ijeci.2023.0702154