

The Role of Artificial Intelligence in Strengthening Digital Identity Verification Mechanisms in the Media and Communication Environment

Received date:08/01/2026 Accepted date:01/04/2026 Published date:30/04/2026

Ouahabi Naziha¹

¹ University of Blida2, Algeria, Email: n.ouahabi@univ-blida2.dz

Abstract:

This article explores the role of Generative AI in bolstering identity verification within digital media. It highlights how AI technologies—such as biometric and liveness detection—safeguard digital identities against deepfakes and impersonation risks, enhancing the cyber resilience of media institutions. While AI offers effective security, it triggers ethical concerns regarding data privacy and automated cyberattacks. The study recommends developing "Zero Trust" frameworks that balance technological efficiency with individual digital rights and algorithmic transparency.

Keywords: Artificial intelligence; Biometric authentication; Cybersecurity; Digital identity; Media systems; Privacy

Corresponding Author:OUAHABI Naziha, Email: n.ouahabi@univ-blida2.dz

1. INTRODUCTION

Digital transformation is one of the most prominent features of the modern era, as digital technology has become an essential tool for facilitating human interactions and organizing social, economic, and media relations. This shift has led to an extensive reliance on digital platforms, making digital identity a decisive factor in ensuring the security of transactions. With the rising frequency of cyberattacks and the emergence of Generative AI (GenAI), there is an urgent need to develop intelligent verification systems capable of securing digital identity efficiently. In this context, Artificial Intelligence (AI) has emerged as an advanced tool, shifting from traditional analytical functions to sophisticated creative capabilities used in biometrics and behavioral analysis.

However, the expansion of AI within digital media environments faces critical challenges, especially with the rise of AI-driven threats such as "Deepfakes" and synthetic identity theft. Relying on AI for identity verification raises legal and ethical concerns regarding privacy and the susceptibility of systems to adversarial attacks that also utilize autonomous AI. From this perspective, the central problem lies in researching the balance between employing AI to secure digital identity and respecting individuals' fundamental digital rights. To frame this issue, we proceed from two hypotheses: first, that AI increases the efficiency of identity verification; and second, that the absence of a regulated framework and "Zero Trust" protocols may diminish the effectiveness of these technologies.

This article seeks to study the employment of AI in supporting digital identity verification by analyzing contemporary



generative models and focusing on the technical and regulatory challenges they pose. It aims to explore ways to ensure a balance between information security and digital privacy, based on a descriptive-analytical method supported by recent quantitative data. Hence, the following primary research question is posed: **To what extent can AI technologies represent an effective solution for digital identity verification within the media space without compromising privacy principles and ethical considerations in the age of synthetic media?**

2. Artificial Intelligence: A Theoretical Approach

2.1 The Historical Evolution of Artificial Intelligence

According to Ahmed Kadhim (2012, pp. 5-6), the historical development of AI can be divided into three stages:

- **The First Stage:** Emerging immediately after World War II, this stage was initiated by Claude Shannon in 1950 with his research on chess and ended with the work of Feigenbaum and Feldman in 1963. This era was characterized by finding solutions to games and puzzles using computers, relying on developing search methods in state-space representation. This led to the creation of computational modeling based on three factors: representing the initial state of the subject (e.g., the chessboard at the start), selecting the goal state conditions (winning), and the set of rules governing moves.
- **The Second Stage (The "Romantic" Period):** Extending from the mid-1960s to the mid-1970s. During this time, Marvin Minsky developed "Frames" for information representation. Systems were also created to

understand English sentences, such as stories and conversations. Researchers like Winston and Brown summarized advanced work at MIT involving natural language processing (NLP), computer vision, robotics, and symbolic processing.

- **The Third Stage (The Modern Period):** Beginning in the mid-1970s, this era is marked by the emergence of various techniques for numerous applications, effectively transferring a significant portion of human intelligence to computer programs. This "Golden Age" saw the maturation of AI techniques to include symbolic modeling, list processing mechanisms, and various programming techniques that interacted with many scientific disciplines.
- **The Fourth Stage (The Generative Revolution):** Beginning around 2022, this era is defined by the rise of Large Language Models (LLMs) and Generative AI (GenAI). Unlike previous stages that focused on classification and pattern recognition, this stage enables machines to create original content, including high-fidelity images, voices, and videos (Deepfakes). This technological leap has shifted the AI paradigm from "analytical" to "creative," presenting unprecedented challenges to digital identity and cybersecurity by blurring the lines between human-generated and machine-generated data (Chui et al., 2023, p. 12).

2.2 The Concept of Artificial Intelligence

The term "Artificial Intelligence" consists of two words: "Intelligence" and "Artificial." According to the Webster

dictionary, **Intelligence** is the ability to understand new or changing circumstances; more comprehensively, it is the ability to perceive, understand, and learn. Thus, the keys to intelligence are perception, understanding, and learning (Doukidis & Paul, 1990, p. 174). **Artificial** refers to things created through human activity or manufacturing, distinguished from natural phenomena. Essentially, AI refers to human-made intelligence implemented in a machine or computer—intelligence originally derived from humans and then granted to a system (Yassin, 2017, p. 179).

AI is considered the science concerned with making intelligent machines that act as a human is expected to act (Rawabeh & Boudah, 2015, p. 203). The Petit Robert dictionary defines AI as: "A part of computer science aimed at simulating cognitive ability to replace humans in performing appropriate functions in a specific context that requires intelligence" (Belhamou & Arzi, 2017, p. 66). Furthermore, Patterson defined it as a branch of computer science concerned with studying and creating computer systems that exhibit forms of intelligence, possessing the ability to make useful inferences and understand natural languages (Sheikh, 2018, p. 82). Minsky defined it as "the science of making machines do things that would require intelligence if done by men" (Yassin, 2004, p. 165).

In general, AI can be defined as the collective efforts to develop computerized information systems in a way that allows them to act and think similarly to humans. These systems can learn natural languages, accomplish physical tasks through integrated coordination, or use perceptual images to guide physical behavior, while simultaneously storing accumulated

human knowledge and experience for decision-making (Khawaled & Thalajia, 2012, p. 10).

2.3 Characteristics and Objectives of Artificial Intelligence

The most important characteristics of AI include (Turban, 2000, p. 08):

- Thinking and perception.
- Using intelligence to solve problems.
- Learning or understanding from experience.
- Acquiring and applying knowledge.
- Demonstrating creativity and imagination.
- Dealing with complex situations.
- Responding quickly and successfully to new circumstances.
- Dealing with incomplete or ambiguous information.
- Supporting administrative decisions.

2.4 Types and Applications of Artificial Intelligence

2.4.1 Types of Artificial Intelligence: (Khalifa, 2017, p. 41)

- **Narrow or Weak AI:** The simplest form, programmed to perform specific functions within a defined environment. Its behavior is a reaction to a specific situation, and it cannot function outside its specific environmental conditions.
- **Strong or General AI:** Characterized by the ability to gather and analyze information, accumulating experience to make independent and autonomous decisions. Examples include self-driving cars and chatbots.
- **Super AI:** Experimental models seeking to simulate humans. These include models that try to understand human emotions and social interactions, and "Theory of

Mind" models that can express internal states and predict others' feelings.

Discriminative vs. Generative AI:

Beyond the classical classification of weak and strong AI, modern categorization distinguishes between "Discriminative AI," which classifies and identifies data (e.g., facial recognition or spam filters), and "**Generative AI**" (**GenAI**). Generative AI, powered by Transformer architectures and Large Language Models (LLMs), has the ability to synthesize entirely new data samples that mimic the statistical properties of the training data. In the context of digital identity, while Discriminative AI is used to *verify* identity, Generative AI can be misused to *fabricate* it through synthetic media, creating a dual-use technology challenge in cybersecurity. (Halaweh, 2023, p. 5).

2.4.2 Applications of Artificial Intelligence: (Bin Al-Tayeb, 2017, p. 07)

- Self-driving cars and drones.
- Robotics: Mechanical devices programmed to work independently of human control for motor and verbal skills.
- Non-linear control, such as railway management.
- Smart devices capable of mental operations like examining industrial designs.
- Cognitive simulation to test theories on how the human mind works (facial/voice recognition, handwriting recognition).
- Medical diagnosis and surgical procedures.

- Economic data analysis (Stock market and trading systems).
- Natural language learning and real-time translation systems.
- **Expert Systems:** Capable of performing tasks like human experts to help make accurate decisions based on logical processes.

3. AI Applications in Cybersecurity:

3.1. Key Defensive Applications of AI

Artificial Intelligence provides proactive and reactive solutions to safeguard digital environments. The following are the primary defensive applications:

1. **Identity Verification:** AI helps developers increase the effectiveness and accuracy of biometric technologies.
2. **Reducing Phishing Attacks:** AI and Machine Learning (ML) identify and track phishing attacks more effectively than humans.
3. **Behavioral Analysis:** ML algorithms learn user behavior to create specific patterns used to analyze potential attacks.
4. **Vulnerability Management:** AI assesses systems quickly to identify weaknesses and design proactive management systems.
5. **Network Security:** AI accelerates the creation of security policies and manages a large number of devices, automatically updating and patching security.
6. **Securing Authentication:** AI improves authentication with layers like facial recognition, CAPTCHA, and fingerprint scanners, preventing unauthorized access.

7. **Combating Bots:** AI identifies and blocks malicious bots by recognizing their patterns and deploying "honeypots."
8. **Security Log Analysis:** ML algorithms detect anomalies in log data in real-time, identifying internal and external threats.
9. **Endpoint Security:** AI-driven endpoint protection establishes baselines for normal behavior to detect "zero-day" attacks in remote work environments.
10. **AI-Assisted Code Scanning:** AI improves Static (SAST) and Dynamic (DAST) security testing by reducing false positives before deployment (National Cybersecurity Authority, 2024, p. 12).

3.2. Emerging Threats: Generative AI and Deepfakes

While AI enhances defensive measures, the rise of "Generative Adversarial Networks" (GANs) has introduced sophisticated threats to digital identity. The most prominent among these is **Deepfakes**—AI-generated synthetic media that can mimic a person's facial expressions, voice, and gestures with alarming realism. This technology poses a direct threat to biometric authentication systems, as attackers can now bypass identity verification layers by using high-fidelity synthetic clones. This evolution shifts the cybersecurity challenge from protecting data to ensuring the "authenticity" of the communication source itself (Mirsky & Lee, 2021, p. 28).

Furthermore, "Synthetic Identity Theft" has emerged as a new frontier in cybercrime, where AI combines real and fabricated data to create entirely new, non-existent identities that can bypass traditional fraud detection algorithms. This necessitates the development of "Liveness Detection" technologies to

distinguish between biological humans and AI-generated avatars in real-time, especially in media institutions that handle sensitive audience data (National Cybersecurity Authority, 2024, p. 18).

- Defining Cybersecurity

Cybersecurity is a relatively new term linked to the technological revolution. Definitions vary:

1. **Lehto Martti & Neittaanmäki Pekka:** A set of measures taken to defend against computer hacker attacks and their consequences.
2. **Edward Amoroso:** The means of reducing the risk of attacks on computers or networks, including the tools used against hackers.
3. **ANSSI (France):** The communication space formed by the global interconnection of automated data processing equipment.
4. **US Department of Defense:** All organizational measures necessary to ensure the protection of information in all forms from crimes, attacks, sabotage, and espionage.
5. **Algerian Legislator (Law 18-04):** The total sum of tools, policies, security concepts, mechanisms, and practices used to protect electronic communications against any event that might compromise the availability, integrity, or confidentiality of stored or transmitted data.

- Elements of Cybersecurity: (Hayari, 2019)

- **Technology:** Provides superior protection for individuals and organizations through firewalls, anti-virus software, and protecting smart devices and networks.
- **People:** Users must apply basic protection principles like strong passwords, avoiding suspicious links, and performing data backups.

- **Process:** Employing people and technology to carry out activities aligned with cybersecurity foundations to counter attacks efficiently.

4. Study Results

To address the gap between theoretical models and real-world implementation, recent quantitative data from global cybersecurity reports provide critical evidence regarding AI-driven identity threats. According to the **IBM Cost of a Data Breach Report (2024)**, there has been a **14% increase** in the use of stolen or compromised credentials as the primary initial attack vector, with AI-enhanced phishing attacks becoming significantly more effective at bypassing traditional security filters. Furthermore, data from the **World Economic Forum (2024)** indicates that "AI-generated misinformation and disinformation" are ranked as the top global risks over the next two years. In the context of digital identity, the frequency of deepfake-related fraud attempts has surged by over **300%** globally between 2023 and 2024, highlighting the urgent need for media institutions to upgrade their verification protocols (IBM Security, 2024, p. 45; WEF, 2024, p. 12).

The analytical reading of scientific and technical sources regarding AI in digital identity verification yielded several results:

1. **Increased Integration:** AI is increasingly used to support verification systems via biometrics (face, fingerprint, voice) and digital behavioral patterns (typing style, cursor movement). These tools provide high accuracy, especially in multi-layered verification systems. However,

effectiveness is affected by environmental context, such as lighting quality for facial recognition.

2. **Privacy Concerns:** Despite technical effectiveness, these technologies raise digital privacy issues as they rely on sensitive data. Furthermore, some algorithms remain vulnerable to "adversarial attacks" designed to deceive AI with fake images or data.
3. **Regulatory Gaps:** The absence of clear regulatory frameworks makes these systems susceptible to misuse or unethical deployment, particularly in media institutions handling vast audience data.
4. **Hypothesis Validation:** The first hypothesis—that AI improves verification efficiency—is largely supported, provided there is a proper operating environment and continuous algorithmic updates. The second hypothesis—that systems face legal and ethical constraints—was also proven correct; technical progress does not absolve the responsibility of establishing legal controls.

Comparing these results with previous studies (Doukidis & Paul, 1990; Rawabeh & Boudah, 2015), the trends converge in confirming that AI's effectiveness is contingent upon its context of use and integration within the institution's organizational and ethical structure.

5. Conclusion

The security of digital identity is no longer just a technical issue; it has become a fundamental requirement for the modern media and commercial environment. While Artificial Intelligence provides powerful tools for verification, the rise of Generative AI has created new challenges, such as deepfakes and

synthetic identity theft, that make traditional security methods insufficient.

To face these risks, institutions must adopt a more comprehensive approach that combines advanced technology with human oversight. Protecting digital identity in the future will depend on our ability to distinguish between biological humans and AI-generated content, ensuring a secure and trustworthy digital space for all users.

- Recommendations

- Adopt liveness detection tools to distinguish between real people and AI-generated clones.
- Update Algerian laws to include specific penalties for AI-assisted identity fraud and digital impersonation.
- Use blockchain technology to create secure and tamper-proof digital identity records.
- Train media professionals to recognize AI-generated content and digital manipulation.
- Deploy automated monitoring systems to detect unauthorized access and new cyber threats in real-time.
- Establish ethical guidelines for the use of artificial intelligence within media and commercial institutions.

6. Bibliography List:

1. Books

- Doukidis, I. G., & Paul, R. J. (1990). *A Survey of the Application of Artificial Intelligence Techniques within the OR Society*. Operational Research Society, United Kingdom.

- Kadhim, Ahmed (2012). *Artificial Intelligence*. Faculty of Information Technology Publications, Imam Ja'far Al-Sadiq University, Iraq.
- Turban, Efraim (2000). *Management Support Systems: Decision Support Systems and Expert Systems* (Translated by: Sorour Ali Sorour). Dar Al-Marikh, Riyadh, Saudi Arabia.
- Yassin, Saad G. (2004). *Decision Support Systems* (2nd Edition). Dar Al-Manahij for Publishing and Distribution, Amman, Jordan.
- Yassin, Saad G. (2017). *Decision Support Systems*. Dar Al-Manahij for Publishing and Distribution, Amman, Jordan.

2. Printed Articles:

- Bakir, V., & McStay, A. (2018). Fake News and the Economy of Emotions. *Digital Journalism*, 6(2), pp. 154-172.
- Belhamou, Fatima Zohra & Arzi, F. (2017). The Contribution of Expert Systems in Improving Decision-Making in Algerian Enterprises: A Case Study of ABRAS SPA. *Revue Maghrébine Management Des Organisations*, 2(1), pp. 66.
- Ben Marzouk, Antara & Al-Karr, Mohammed. (2018). The Electronic Dimension of Algerian Security Policy in Combating Terrorism. *Journal of Human and Social Sciences*, (38), pp. 34.
- Bounif, Sami Mohammed. (2019). The Role of Proactive Strategies in Confronting Cyber Attacks – Cyber Deterrence as a Model. *Algerian Journal of Rights and Political Science*, 4(7), pp. 123.

- Guelaâ Dhrossou, Samir. (2022). National Cybersecurity – A Reading of the Key Security Strategies to Combat Cybercrime in Algeria. *Al-Riwaq Journal for Social and Political Studies*, 8(2), pp. 252–253.
- Halaweh, M. (2023). ChatGPT and Generative AI: What is new?. *Journal of Strategic Innovation and Sustainability*, 18(1), pp. 1-10.
- Khalifa, Ihab. (2017). Effects of the Increasing Role of Smart Technologies in Human Daily Life. *Trends of Events Periodical*, (20), pp. 41.
- Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. *ACM Computing Surveys*, 54(1), pp. 1–36.
- Rawabeh, Abba & Boudah, Abdeljalil. (2015). The Evolution of Loan Risk Assessment under Artificial Intelligence Models. *Journal of Human Sciences*, 26(04), pp. 203.
- Sheikh, Hajira. (2018). The Role of Artificial Intelligence in Managing E-Customer Relationships at the Credit Populaire d'Algérie (CPA). *Academic Journal for Social and Human Studies*, 10(02), pp. 82.

3. Seminar and Conference Articles:

- Bin Al-Tayeb, Ali & Mehoul, Zakaria (2017). *Artificial Intelligence Applications and their Role in Enhancing Community Digitization and Transition towards Smart Cities: UAE as a Model*. International Conference on Smart Cities under Current Changes, Arab Democratic Center, Berlin, Germany.

- Chui, M., et al. (2023). *The economic potential of generative AI: The next productivity frontier*. McKinsey Global Institute Report.
- Khawaled, Abubaker & Thalajia, Nawa (2012). *Artificial Intelligence-Based Information Systems: Between Theoretical Concepts and Practical Applications in Economic Enterprises*. The 10th National Seminar on AI-Based Information Systems, University of Skikda, Algeria.

4. Internet Websites and Reports :

- AI Superior (2024). *Use Cases of Artificial Intelligence in Cybersecurity*. AI Superior Website: <https://aisuperior.com/ar/ai-use-cases-in-cybersecurity/> (consulted on 18/11/2024).
- Al-Hayari, Iman (2019). *What is Cybersecurity, What are its Standards, and Why is it Important?*. Mahatat Website: <https://www.mah6at.net/> (consulted on 02/01/2026).
- IBM Security (2024). *Cost of a Data Breach Report 2024*. IBM Corporation: <https://www.ibm.com/reports/data-breach> (consulted on 10/01/2026).
- National Cybersecurity Guidance Center (2024). *Artificial Intelligence Applications in Cybersecurity*. National Cybersecurity Authority: <https://cert.gov.sa/ar/awareness/> (consulted on 12/11/2024).
- World Economic Forum (2024). *The Global Risks Report 2024*. 19th Edition: <https://www.weforum.org/reports/global-risks-report-2024/> (consulted on 15/01/2026).