Article

Not peer-reviewed version

# Artificial Intelligence and National Security: The Role of Two-Step Verification in Safeguarding Privacy and Digital Rights

Khaled M.M. Alrantisi *

Posted Date: 14 May 2025

doi: 10.20944/preprints202505.1037.v1

Keywords: artificial intelligence; cybersecurity; digital rights; two-step verification (2sv); digital identity; machine learning; threat detection; privacy; user autonomy; sim-swapping; user fatigue; biometric verification; human rights; ethical deployment; automated world; enterprise security; governmental security; innovative pathways; ai-integrated verification

 doi:10.20944/preprints202505.1037.v1



*Article*

# Artificial Intelligence and National Security: The Role of Two-Step Verification in Safeguarding Privacy and Digital Rights

**Khaled M. M. Alrantisi**

Department of Computer Science and Engineering, Ala-Too International University;
khaled.alrantisi@alatoo.edu.kg

**Abstract:** In the age of artificial intelligence, cybersecurity and digital rights have become increasingly intertwined. This paper explores the role of Two-Step Verification (2SV) as a pivotal mechanism in securing digital identities and infrastructures. Drawing primarily on the work of Alrantisi [10], and contextualized within broader AI-driven threat landscapes [9] and human rights concerns [8], the paper investigates how 2SV complements machine learning-based threat detection while enhancing privacy and user autonomy. The study further discusses its implementation across governmental and enterprise domains, outlines current limitations—such as vulnerability to SIM-swapping and user fatigue—and suggests innovative paths forward through AI-integrated and biometric verification methods. Ultimately, this paper emphasizes that 2SV, when ethically deployed, can act as both a technological safeguard and a human rights protector in an increasingly automated world.

**Keywords:** artificial intelligence; cybersecurity; digital rights; two-step verification (2sv); digital identity; machine learning; threat detection; privacy; user autonomy; sim-swapping; user fatigue; biometric verification; human rights; ethical deployment; automated world; enterprise security; governmental security; innovative pathways; ai-integrated verification

## 1. Introduction

In the digital age, cybersecurity measures such as two-step verification (2SV) have become central to safeguarding personal data, institutional systems, and national infrastructure. As articulated by Alrantisi [10], 2SV enhances security by requiring an additional authentication layer, thereby reducing the risk of credential theft and unauthorized access. However, its significance becomes even clearer when analyzed alongside other research on AI-driven cybersecurity [9] and human rights challenges in digital governance [8].

## 2. The Intersection of 2SV and AI-Based Cybersecurity

The review by Alshuaibi et al. [9] outlines how machine learning (ML) algorithms ranging from support vector machines to deep neural networks can detect sophisticated cyber threats such as malware, DDoS, phishing, and zero-day exploits. These threats often exploit weak authentication systems, especially those relying solely on passwords.

2SV, as advocated by Alrantisi, complements these ML-driven approaches by acting as a resilient endpoint control. While AI detects threats in real-time, 2SV ensures that even if a system's perimeters are breached, access remains tightly guarded by verifying user identity across independent factors.

"Machine Learning will positively change the cybersecurity field" by enabling predictive analysis and proactive response mechanisms [9].

This symbiosis between AI analytics and 2SV ensures a multi-layered security posture, where 2SV guards the access gates while AI monitors behavioral anomalies, network patterns, and emerging attack vectors.

 doi:10.20944/preprints202505.1037.v1



## 3. Human Rights Implications of Authentication Technologies

Ahmad et al. [8] present a comprehensive analysis of the multifaceted human rights challenges arising in the era of artificial intelligence, emphasizing the growing concerns around individual privacy, data autonomy, and the systemic misuse of personal information.

As AI systems become more embedded in critical decision-making processes ranging from healthcare diagnostics to criminal justice algorithms—they increasingly rely on large-scale, often sensitive, personal data. This creates a scenario where the efficiency of AI-driven operations must be carefully weighed against the potential for abuse, surveillance, and exclusion.

In this landscape, Two-Step Verification (2SV) acts not merely as a cybersecurity tool but as a mechanism for reinforcing digital civil liberties. By requiring users to authenticate through two independent factors such as a password and a time-sensitive code sent to a trusted device 2SV reduces the likelihood of unauthorized access, thereby limiting avenues for surveillance, identity theft, and data exploitation.

It empowers users with greater control over their digital identities by ensuring that their access credentials are not the sole determinant of system entry.

Furthermore, 2SV adds an essential layer of defense against coercive surveillance practices or large-scale data breaches, particularly in authoritarian or high-risk environments. For individuals in politically sensitive contexts, where state surveillance or targeted digital attacks are common, the presence of 2SV may serve as a protective barrier against unjust scrutiny or persecution.

Nevertheless, Ahmad et al. [8] rightly argue that technological solutions alone are insufficient. While 2SV mitigates several technical vulnerabilities, it must be deployed within a robust legal and ethical framework.

These frameworks should ensure that authentication systems are transparent in their design, inclusive in their accessibility (especially for marginalized or digitally underserved populations), and respectful of user consent and autonomy. Without such safeguards, even well-intentioned security measures could inadvertently contribute to digital discrimination, exclusion, or the erosion of fundamental rights.

Thus, when Alrantisi's technical advocacy for 2SV [10] is synthesized with the ethical imperatives outlined by Ahmad et al. [8], it becomes clear that 2SV should be seen not only as a gatekeeper of systems but as a pillar of digital justice—securing not just data, but dignity and agency in the age of artificial intelligence.

## 4. Enterprise and Government Applications

Both Alrantisi [10] and Ahmad et al. [8] underscore the increasing reliance of enterprise and government sectors on robust authentication mechanisms to mitigate digital threats and preserve the integrity of sensitive data. In an era where cyberattacks target not only individuals but entire institutions and national infrastructure, Two-Step Verification (2SV) has emerged as a critical safeguard.

In enterprise environments particularly within sectors such as banking, healthcare, education, and finance 2SV serves as a first line of defense against identity fraud, unauthorized access, and credential stuffing. For instance, in online banking, 2SV can prevent attackers from accessing user accounts even if passwords are compromised, by requiring an additional, real-time verification step, such as a biometric scan or a one-time password (OTP) sent to a verified mobile device. This helps to drastically reduce financial fraud and unauthorized transactions.

In the healthcare industry, where electronic health records (EHRs) contain highly sensitive patient data, 2SV ensures that only authorized personnel can access confidential files. This is particularly important for maintaining compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act), which mandates strict controls on data privacy and access.

Educational institutions, too, have adopted 2SV to protect learning management systems (LMS), student databases, and faculty accounts. With the rise of remote learning and administrative

 doi:10.20944/preprints202505.1037.v1



digitization, preventing breaches in academic systems has become essential to ensuring institutional integrity and student privacy.

Governmental applications of 2SV are even more critical. From secure employee logins in defense and intelligence agencies to digital identity systems for public service access, the use of 2SV reduces the risk of espionage, data leaks, and insider threats. Moreover, it enhances citizen trust in digital government platforms by safeguarding personal information stored in e-governance systems.

Alshuaibi et al. [9] emphasize that the effectiveness of 2SV can be further amplified when combined with AI-powered monitoring tools. These systems can detect anomalies in user behavior, login times, IP addresses, and geolocation patterns, flagging suspicious activity in real time. When 2SV is used in tandem with AI-based threat detection, organizations can proactively respond to cyber threats before they escalate into breaches.

Additionally, the integration of 2SV and AI supports compliance with international regulatory frameworks such as the General Data Protection Regulation (GDPR) and HIPAA, which require both technical and procedural safeguards for data protection. 2SV provides the technical assurance of user identity, while AI tools enable constant vigilance and real-time adaptation to evolving security risks.

In summary, 2SV is more than a security feature; it is a strategic asset that bolsters institutional resilience, protects national interests, and fulfills legal obligations. By bridging traditional authentication with AI-enhanced oversight, 2SV empowers enterprises and governments to defend against both current and emerging digital threats.

## 5. Limitations and Calls for Innovation

While 2SV is highly effective, both Alrantisi and the broader AI literature [9] identify some core limitations:

- SIM-swapping attacks threaten SMS-based 2SV.
- User fatigue from repetitive logins can reduce adoption.
- Lack of integration with AI may reduce contextual threat awareness.

Emerging solutions like biometric 2SV, push-notification authentication, or AI-adaptive verification systems can resolve these issues [9][10]. These innovations are vital, especially as AI systems begin influencing more aspects of everyday life, from healthcare decisions to electoral processes [8].

## 6. Conclusion

Two-step verification is no longer a standalone defense it is a cornerstone of integrated cybersecurity systems that balance machine intelligence with human rights. The work of Alrantisi [10] illustrates how technically sound authentication mechanisms, when linked with broader AI defenses [9] and embedded in ethical frameworks [8], can help construct a resilient, trustworthy, and rights-preserving digital ecosystem.

## References

1. Alrantisi, K. M. M. (2025). The Importance of Two-Step Verification in Cybersecurity. Preprints.org. [10]
2. Alshuaibi, A., Almaayah, M., & Ali, A. (2025). Machine Learning for Cybersecurity Issues: A Systematic Review. Journal of Cyber Security and Risk Auditing, 2025(1), 36–46. https://doi.org/10.63180/jcsra.thestap.2025.1.4 [9]
3. Ahmad, N., Ali, A. W., & Yussof, M. H. B. (2025). The Challenges of Human Rights in the Era of Artificial Intelligence. UUM Journal of Legal Studies, 16(1), 150–169. https://doi.org/10.32890/uumjls2025.16.1.9 [8]