УДК 340+342.7
DOI 10.33244/2617-4154.3(20).2025.37-50

F. P. Huseynzade,
Lecturer of the Financial Law,
Corporate law and Governance and Legal regulation of economy,
Faculty of Law, PhD(c) in Law,
Baku State University
email: farahim.huseynzade@outlook.com
ORCID 0000-0003-4179-1403

THE NECESSITY OF ENHANCED AUTHENTICATION FOR ELECTRONIC SERVICES: LEGAL CHALLENGES AND SOLUTIONS

This paper explores the necessity of enhanced authentication mechanisms for electronic services, emphasizing the legal challenges and possible solutions associated with their implementation. As digitalization accelerates across banking, healthcare, government, and other sectors, traditional methods such as passwords and PINs have proven inadequate in the face of rising cyber threats, identity theft, and data breaches. Advanced approaches – biometric authentication, multi-factor authentication, cryptography, and blockchain – offer stronger protection, but they simultaneously raise significant legal and ethical concerns. Key issues include compliance with data protection regulations such as the GDPR, the sensitivity and immutability of biometric data, cross-border data transfers, and accountability in decentralized systems. The paper examines these challenges in depth and proposes potential legal frameworks to balance technological innovation with the protection of individual rights. By harmonizing international standards, strengthening data privacy safeguards, and ensuring transparency and consent, enhanced authentication can become a secure, lawful, and trusted foundation for electronic services in the digital era.

Keywords: *Electronic Services, Authentication, Legal Challenges, Security, Biometrics, Encryption, Data Privacy, Blockchain, Legal Framework, Digital Identity.*

Introduction. The digital revolution has radically transformed how we communicate, transact, and access services, making electronic services a central component of daily life across various sectors, including banking, healthcare, education, and government services. The proliferation of electronic services has streamlined operations, it has simultaneously escalated the need for advanced authentication methods to ensure the protection of users' personal data and prevent cyber threats [1]. This paper examines the necessity for enhanced authentication, identifies related legal challenges, and proposes solutions to address these concerns [2]. For example, according to the IBM Security report, the average data breach in

2024 cost companies $4.5 million, highlighting the urgency for improved authentication mechanisms.

As reliance on electronic services continues to rise, the critical role of authentication becomes increasingly apparent. Authentication serves as the process by which systems verify the identity of users, ensuring they are legitimate before granting access to services. Traditional authentication methods such as usernames and passwords have proved insufficient against sophisticated cyber-attacks. Cybercriminals continually bypass these security measures, causing unauthorized access, identity theft, and financial losses. The necessity for more robust authentication systems is underscored by several factors, primarily the surge in cyber threats and data breaches.

As we progress further into the digital age, the increasing reliance on electronic services in various aspects of life, such as communication, finance, education, healthcare, and government services, underlines the critical role of authentication [3]. In essence, authentication is the process by which systems verify the identity of users to ensure that they are who they claim to be before granting access to services. The necessity for enhanced authentication in electronic services is underscored by a multitude of factors.

One of the primary reasons is the exponential increase in cyber threats and data breaches. Traditional authentication methods such as usernames and passwords have proved insufficient in the face of increasingly sophisticated cyber attacks [4] Cybercriminals continually develop new ways to bypass these security measures, leading to unauthorized access, identity theft, and financial losses.

Moreover, the proliferation of Internet of Things (IoT) devices has further amplified the necessity for enhanced authentication. With millions of devices connected to the internet and sharing data, the potential attack surface has expanded significantly. Ensuring secure and reliable access to these devices and the services they provide necessitates more robust and advanced authentication mechanisms.

Furthermore, the growth of online services has led to an increase in the amount of sensitive data stored and transmitted digitally. From personal health records in telemedicine to financial transactions in online banking, electronic services deal with a myriad of sensitive data that require stringent protection [5]. Therefore, improved authentication methods are necessary to provide this level of security and ensure user confidence.

Additionally, the ongoing global trend towards digitization and remote access to services, particularly accelerated by recent global events such as the COVID-19 pandemic, further underlines the necessity for advanced authentication measures. As more people work, study, and conduct transactions remotely, the need to verify identities and protect data in the digital realm becomes even more pressing.

Biometric authentication, multi-factor authentication, and risk-based authentication are among the advanced methods that have been proposed to mitigate these challenges. They offer a more reliable way to confirm the digital identity of users, which is critical in the era of electronic services. These methods, however, come with their own set of challenges, which will be further discussed in the following sections of this paper.

Legal challenges. In essence, the necessity for enhanced authentication in electronic services stems from the need to counter evolving cyber threats, protect sensitive data, accommodate the growth of IoT devices, and meet the increasing demand for remote access to services.

Enhanced authentication measures provide potential solutions for ensuring secure electronic service access but also pose significant legal challenges. Data privacy laws, for instance, place restrictions on the collection and use of personal data such as biometric information [6]. In some jurisdictions, explicit user consent is required before implementing certain authentication mechanisms [7]. This legislative landscape poses a challenge to service providers who aim to adopt these technologies for security reasons.

One of the significant challenges for implementing advanced authentication methods is the regulation around data privacy and user consent. Laws such as the European General Data Protection Regulation (GDPR) necessitate explicit consent from users before collecting and processing personal data, including biometric information [8]. Ensuring compliance with these laws while implementing advanced authentication methods can be a complex and daunting task for service providers.

Biometric authentication involves using unique physiological or behavioral traits (e.g., fingerprints, facial recognition, voice patterns) to verify a user’s identity. While these methods offer substantial security advantages, they raise critical legal concerns, primarily due to their highly personal nature [9]. By nature, biometrics are unique to individuals and difficult to replicate, thereby providing a high level of security for electronic services [10]. Despite its apparent benefits, the use of biometric authentication raises notable legal and ethical concerns. One of the principal legal issues surrounding biometric authentication is the potential violation of data privacy rights. Biometric data, due to its intensely personal nature, falls under the domain of personal sensitive data in most data protection laws [6]. The indiscriminate collection and use of biometric data can lead to serious infringements of privacy rights. The GDPR, for example, necessitates informed and explicit consent from individuals before their biometric data is collected or processed. Some legal frameworks, such as the European Union's General Data Protection Regulation (GDPR), require explicit and informed consent from individuals before their biometric data can be processed [8].

Another critical legal challenge is related to the potential misuse of biometric data. In the event of a data breach, unlike passwords or PINs, biometric data cannot be changed or reset. Once compromised, the implications are severe and long-lasting, potentially leading to identity theft and other forms of fraud [11]. Legal uncertainties surrounding the ownership and control of biometric data also pose a significant challenge. Given that biometric data is intrinsically linked to an individual, questions about who owns this data, who can access it, and under what conditions, become critical. Current legal frameworks often lack clarity in defining these rights, leading to ambiguity and potential misuse [12].

The cross-border transfer of biometric data presents yet another legal complexity. As electronic services are often global, biometric data may need to be transferred across jurisdictions with different data protection laws. Ensuring compliance with diverse and often conflicting regulations can be a complex task for service providers. The use of biometric authentication in law enforcement, while valuable for enhancing public safety, has raised issues of potential state surveillance and civil liberties infringement [13]. Balancing the needs of security and individual privacy in this context is a pressing legal issue. It should be highlighted that, while biometric authentication promises heightened security for electronic services, its deployment is not devoid of legal hurdles. Careful consideration of these challenges and development of a comprehensive and balanced legal framework is essential to ensure the ethical and legal use of this powerful technology. In summary, while biometric authentication stands as a promising mechanism in enhancing the security of electronic services, it is of utmost importance to address the array of legal challenges that it introduces. Legal issues such as privacy rights violation, data misuse, and unclear ownership of biometric data, coupled with the intricacies of cross-border data transfer, necessitate a comprehensive and robust legal framework. It's imperative to strike a balance between the advancement of this technology and the protection of individual rights, making sure that biometrics serve as a tool for ensuring security and not a medium for unwarranted surveillance or privacy infringement. The evolution of a harmonious relationship between technology and law in this context, thus, remains a key to the future of secure electronic services.

In addition to legal obstacles, there are substantial technical challenges in deploying advanced biometric authentication. These systems must maintain high accuracy and reliability, yet environmental factors – lighting, sensor conditions, or user behavior – can all trigger false positives or false negatives, undermining both user trust and system integrity. Moreover, securely storing biometric data demands robust cryptographic and infrastructure safeguards. Implementing and maintaining such systems can strain organizational resources, particularly for smaller entities lacking specialized expertise.

On the international standards front, organizations like ISO/IEC JTC 1/SC 37 are working to harmonize biometric technologies globally. This subcommittee develops a range of standards – covering data interchange formats, interfaces, performance testing, and societal aspects – to help ensure interoperability and reliability across systems. For example, standards like ISO/IEC 19794 define formats for face, iris, and fingerprint data, while ISO/IEC 19795 outlines methods for testing biometric performance.

Within industry-specific domains, ISO 19092 provides a security framework tailored for financial services, offering guidance on biometric policy content, event auditing, and device security for remote and physical authentication scenarios. These standards not only promote technical robustness but also facilitate regulatory compliance through structured protocols and documentation.

Beyond technical and standards-oriented considerations, ethical and privacy safeguards are critical. Biometric data, by nature, is immutable and deeply personal – once breached, it cannot be reset like a password. This permanence amplifies privacy risks and implies long-term consequences for individuals. Research also highlights a regulatory gap: policymakers often lag behind technological adoption, struggling to develop adequate legal frameworks that balance innovation with privacy rights. Without such frameworks, biometric deployment may outpace the laws meant to protect individuals.

Ultimately, while biometric and other enhanced authentication measures offer promising avenues to bolster electronic security and accommodate IoT and remote access needs, their implementation must be supported by a multi-faceted approach. This includes resolving technical limitations, adhering to international standards, crafting robust legal and policy frameworks, and ensuring that user consent and privacy protections remain central. Only through such an integrated strategy can enhanced authentication truly serve as a secure, lawful – and trusted – pillar of electronic services.

The rapid advancement of digital services underscores the necessity for enhanced authentication mechanisms to protect users from increasing cyber threats and privacy violations. With the proliferation of Internet of Things (IoT) devices and the growing demand for remote access to services, traditional authentication methods such as passwords and PINs are proving inadequate. These conventional methods are vulnerable to various cyberattacks, including phishing, brute-force attacks, and credential stuffing, leading to potential unauthorized access and data breaches. Consequently, there is a pressing need to adopt more robust authentication mechanisms to safeguard sensitive information and ensure secure access to electronic services.

Advanced authentication methods, such as biometric authentication and multi-factor authentication (MFA), offer promising solutions to enhance security. Biometric authentication leverages unique physiological or behavioral characteristics, such as fingerprints, facial recognition, or voice patterns, to verify a user's identity. These traits are inherently difficult to replicate, providing a higher level of security compared to traditional methods. Multi-factor authentication, on the other hand, requires users to provide two or more verification factors, combining something they know (password), something they have (security token), and something they are (biometric data), thereby adding an additional layer of security.

However, the implementation of these advanced authentication methods introduces significant legal and ethical challenges. The collection and processing of biometric data raise concerns regarding privacy rights, data ownership, and the potential for misuse. In many jurisdictions, biometric data is classified as sensitive personal data, subject to stringent data protection laws such as the European Union's General Data Protection Regulation (GDPR). These regulations mandate explicit and informed consent from individuals before their biometric data can be collected or processed, posing challenges for organizations seeking to implement biometric authentication systems.

Moreover, the use of biometric data introduces risks related to data breaches and unauthorized access. Unlike passwords, biometric data cannot be changed or reset if compromised, leading to potential long-term privacy violations. For instance, unauthorized access to biometric databases can result in identity theft, fraud, and other malicious activities. Additionally, the integration of biometric systems into existing infrastructure may create vulnerabilities if not properly secured, further exacerbating the risk of data breaches.

The cross-border transfer of biometric data adds another layer of complexity to the legal landscape. As electronic services often operate globally, biometric data may need to be transferred across jurisdictions with varying data protection laws. Ensuring compliance with diverse and sometimes conflicting regulations can be a daunting task for service providers.

For example, the GDPR imposes strict conditions on the transfer of personal data outside the European Economic Area, requiring adequate safeguards to protect the data. Failure to comply with these regulations can result in significant legal and financial repercussions.

In the context of blockchain technology, while it offers enhanced security features such as decentralization and immutability, it also presents unique legal challenges. The decentralized nature of blockchain makes it difficult to assign legal responsibility, such as identifying a "data controller" under data protection laws like the GDPR. Furthermore, the immutability of blockchain records conflicts with legal requirements for data rectification and erasure, posing challenges for compliance with data protection regulations. For instance, the GDPR's "right to be forgotten" allows individuals to request the deletion of their personal data, which is incompatible with the permanent nature of blockchain records.

To address these legal challenges, several potential solutions can be explored. One approach involves harmonizing data privacy laws globally to facilitate the international use of advanced authentication technologies. Developing universally recognized guidelines for the collection, processing, and storage of biometric data would ensure consistency and clarity across jurisdictions. Additionally, legal frameworks could be developed to address the challenges associated with encryption and blockchain technology, ensuring that these technologies are used responsibly and in compliance with existing laws.

For biometric authentication, stringent security measures must be enacted to prevent unauthorized access and misuse of biometric data. Legal frameworks should ensure that biometric data is collected, stored, and processed in a secure and privacy-respecting manner. This could involve implementing robust encryption methods, access controls, and regular audits to safeguard biometric information. Furthermore, organizations should provide individuals with clear information about how their biometric data will be used and obtain explicit consent before collection.

Concerning cryptography, a potential solution could be a legal framework that strikes a balance between the need for strong encryption for secure authentication and the need for law enforcement agencies to conduct investigations effectively. This balance could be achieved through a collaborative dialogue involving all stakeholders, including governments, businesses, and civil society. Establishing clear guidelines for the use of encryption technologies would help ensure that they are used responsibly and do not impede legitimate law enforcement activities.

With blockchain technology, the development of a comprehensive legal framework could be beneficial. Such a framework should clearly define the rights and responsibilities of all parties involved in blockchain transactions. Additionally, global cooperation could help address cross-border legal issues, ensuring that blockchain technologies are used in a manner that respects data protection laws and promotes international collaboration.

The rapid advancement of digital services underscores the necessity for enhanced authentication mechanisms to protect users from increasing cyber threats and privacy violations. As technology continues to evolve, it is imperative that legal and ethical considerations stand at the forefront of the design and deployment of advanced authentication mechanisms. With carefully constructed legal frameworks and informed decisions, we can navigate these challenges, ensuring that the adoption of enhanced authentication technologies in electronic services is secure, privacy-preserving, and legally sound.

Cryptography, Encryption and Blockchain Technology. Cryptography, specifically encryption, plays a crucial role in secure authentication processes. However, it also poses legal challenges, primarily due to issues related to the regulation of encryption technologies and potential conflicts with law enforcement activities (14). In some jurisdictions, strong encryption is viewed skeptically due to its potential use for illicit activities. Australia’s Assistance and Access Act 2018, mandating encryption backdoors, starkly illustrates this tension. Therefore, balancing the need for secure authentication with legal obligations and societal considerations is crucial.

Blockchain technology offers promising solutions for enhanced authentication in electronic services due to its decentralization, immutability, and transparency characteristics [15]. However, it also presents unique legal challenges, such as regulatory uncertainty, cross-border legal issues, and concerns about data privacy [16]. Estonia's e-Residency program successfully utilizes blockchain-based authentication but navigated complex EU regulatory landscapes addressing data privacy and cross-border transfer concerns. As blockchain-based authentication systems become more prevalent, understanding these legal implications is essential.

Cryptography remains a cornerstone of secure authentication – but its intersection with legal regimes often yields contentious debate. Governments in several jurisdictions have sought to compel access to encrypted data, citing public safety. Australia’s Assistance and Access Act of 2018 exemplifies the tension: it authorizes authorities to demand assistance from tech companies in accessing encrypted communications, potentially forcing engineers to introduce effective vulnerabilities – despite formal prohibitions on building systemic backdoors. Critics argue that such measures undermine cybersecurity infrastructure and erode public trust, particularly when mechanisms for judicial oversight are limited or vague. Therefore, encrypted authentication systems must be designed with acute awareness of legal mandates and the risks of forced assistance.

Moreover, the requirement to provide encryption keys or design systems that facilitate law enforcement access presents ethical and privacy perils. Compelled cooperation introduces risks of coercion and may violate privacy rights – even with good intentions. Experts warn that any weakening of encryption, even selectively, can be exploited by malicious actors, widening the attack surface of digital systems. Consequently, service providers and lawmakers must carefully balance legitimate investigative needs with preserving the integrity and reliability of encryption-based authentication.

At the same time, blockchain technology has emerged as a promising vehicle for decentralized and transparent authentication. Its immutable ledger and tamper-evident architecture can strengthen identity verification, audit trails, and credential management. However, this very immutability stands at odds with legal frameworks such as the GDPR, which mandates data rectification and erasure when legally required. The append-only nature of blockchains hinders compliance with “right to be forgotten” requests, creating challenges for service providers and legislators alike.

Further complicating matters is the decentralization inherent in blockchain systems: when consensus mechanisms replace centralized control, assigning legal responsibility – such as identifying a “data controller” under GDPR – becomes ambiguous. Public blockchains in particular obscure accountability and complicate enforcement, making it difficult to comply with data protection laws that assume centralized governance structures. As a result, organizations deploying blockchain-based authentication must either adopt permissioned models with clear governance or pioneer new compliance frameworks.

Estonia’s e-Residency and blockchain-based digital identity initiatives illustrate both the potential and pitfalls of these technologies. While the program successfully integrates secure, cross-border digital authentication under EU regulations like eIDAS, it operates within a tightly governed and legally harmonized environment. Nonetheless, even well-regulated systems are not immune to technical or operational risks, highlighting the need for robust oversight, adaptability, and fall-back mechanisms. In sum, as cryptographic and blockchain-based authentication technologies evolve, their legal alignment, operational resilience, and trustworthiness must be continuously evaluated to ensure they bolster – not undermine – secure electronic services.

As encryption remains fundamental to secure authentication, recent developments further illustrate the friction between privacy and governmental oversight. In August 2025, the UK withdrew its demand that Apple insert a backdoor into iCloud encryption under the Investigatory Powers Act – a demand that had compelled Apple to suspend its Advanced Data Protection service in the UK and sparked high-level political tensions, including potential breach of the U.S. – U.K. CLOUD Act agreement. This episode underscores how such mandates not only threaten encryption integrity but also strain international cooperation and consumer trust.

Simultaneously, the EU reaffirmed its push for so-called "lawful access" to encrypted data through its “ProtectEU” initiative, which aims to make decryption capabilities available to law enforcement by 2030. Critics, including VPN providers like Proton VPN, Mullvad, and NordVPN, warn that this undermines cybersecurity and privacy by introducing exploitable vulnerabilities. These developments reflect an intensifying global debate: how to reconcile encryption’s essential role in protecting digital services with governments' investigative demands.

In parallel, key disclosure and mandatory decryption laws continue to pose ethical challenges. Some jurisdictions require individuals – or providers – to surrender cryptographic keys under judicial authority, raising concerns around coerced self‑incrimination and privacy sovereignty. Legal precedents like In re Boucher in the U.S., where a defendant was compelled to decrypt his hard drive without Fifth Amendment protection, illustrate the real--world implications of these laws. Such cases exemplify the pressure point between privacy rights and prosecutorial imperatives.

Turning to blockchain, its immutability and decentralization – while advantageous for authentication – conflict with GDPR’s right to erasure. Article 17 requires personal data be deleted upon user request, but true deletion from a blockchain is technically unattainable. Hybrid systems that keep sensitive data off-chain while storing only hashes on-chain are one workaround – but they compromise decentralization benefits and require careful governance.

The ambiguity around who serves as the “data controller” in blockchain environments further complicates compliance. With distributed ledgers, identifying responsible parties for GDPR liabilities – such as rectification or erasure – becomes opaque. Some regulators, like France’s CNIL, propose that the entity uploading personal data may be deemed the controller, while participants like miners are processors – but this remains a contentious and unsettled issue.

Technical innovations may offer partial relief. Techniques like chameleon hashes – used in permissioned blockchains such as Hyperledger Fabric – can allow data correction or removal to accommodate GDPR obligations, though at the expense of the blockchain’s immutable trust model. Other privacy-enhancing technologies, such as zero-knowledge proofs or selective disclosure, can minimize the amount of personal data ever exposed on-chain, thus aligning with privacy norms while maintaining authentication integrity.

Real-world examples illustrate these tensions. In healthcare, blockchain projects like MediBloc store patient records on-chain for transparency and data access – but the inability to erase or modify information poses compliance risks if patients request data deletion. Similarly, smart contracts – by design self-executing and immutable – raise further complications when they incorporate personal data such as identity markers or behavioral logs.

Despite these technical and legal hurdles, some regulatory bodies show pragmatic flexibility. The CNIL notes that encrypted or hashed data that is technically inaccessible may suffice in some cases of “erasure,” even if not physically deleted – reflecting a nuanced approach to compliance in blockchain contexts. Yet, more definitive legal guidance beyond theoretical frameworks is still needed.

Ultimately, the intersection of cryptography, encryption, and blockchain with law remains a battleground of conflicting values. Encryption is indispensable for authentication yet faces rising legal pressure for forced access. Blockchain promises transparent and resilient authentication but grapples with core data protection principles. Navigating these tensions will require interdisciplinary cooperation – between technologists, legislators, and privacy advocates – to craft frameworks that allow innovative authentication while safeguarding rights and legal obligations.

Potential Legal Frameworks. A robust legal framework that accommodates enhanced authentication mechanisms for electronic services is a pressing necessity. Such a framework should consider data privacy laws, encryption regulations, and the emerging legal issues associated with technologies like biometrics and blockchain [17]. An international convention similar to the Budapest Convention on Cybercrime could specifically address biometric data use and blockchain authentication standards. It should also address the cross-border nature of electronic services, which adds another layer of complexity to the legal landscape [18].

To address these legal challenges, several potential solutions can be explored. One solution involves harmonizing data privacy laws globally to facilitate the international use of advanced authentication technologies. The development of universally recognized guidelines for the collection, processing, and storage of biometric data would ensure consistency and clarity across jurisdictions. It could be beneficial to establish clear, globally recognized guidelines for collecting and processing personal data, including biometric data, for authentication purposes [19]. In addition, legal frameworks could be developed to address the challenges associated with encryption and blockchain technology.

For biometric authentication, stringent security measures must be enacted to prevent unauthorized access and misuse of biometric data. Legal frameworks should ensure that biometric data is collected, stored, and processed in a secure and privacy-respecting manner. This could be paired with robust legislation that regulates the collection, storage, and use of such data [20]. Concerning cryptography, one possible solution could be a legal framework that strikes a balance between the need for strong encryption for secure authentication and the need for law enforcement agencies to conduct investigations effectively. This balance could be achieved through a collaborative dialogue involving all stakeholders, including governments, businesses, and civil society [21]. With blockchain technology, the development of a comprehensive legal framework could be beneficial. Such a framework should clearly define the rights and responsibilities of all parties involved in blockchain transactions. Additionally, global cooperation could help to address cross-border legal issues [22].

The rapid advancement of digital services underscores the necessity for enhanced authentication mechanisms to protect users from increasing cyber threats and privacy violations. With increasing cyber threats and a growing need for remote and personalized services, it is imperative to enhance the methods of user authentication. While traditional measures, such as passwords and PINs, have served their purpose, they fall short in today's rapidly evolving digital landscape marked by sophisticated cyberattacks and the ubiquitous nature of IoT devices.

In this context, advanced authentication methods, such as biometric and multi-factor authentication, offer promising solutions. However, their implementation is not without legal implications and challenges. The personal and sensitive nature of biometric data raises substantial issues concerning privacy, data ownership, cross-border data transfer, and potential misuse. The legal aspects surrounding these technologies are complex, requiring comprehensive regulation and transparency to ensure that while we stride forward in technological advancement, we do not compromise individual rights and privacy. In the case of blockchain-based authentication, we witness a promising solution capable of tackling some of the prevailing security issues. However, this technology too, is met with legal challenges surrounding its acceptance and regulation. The decentralized nature of blockchain introduces a unique set of legal issues involving jurisdiction, legal recognition, and enforceability of rights. Addressing these legal challenges necessitates harmonizing technology with law, ensuring that advances in security measures do not compromise personal liberties. A balanced legal framework needs to be in place that would guide technological growth while preserving individuals' rights. It is of utmost importance to conduct further research to explore potential solutions, including privacy-preserving technologies, legally compliant design principles, and comprehensive legislative measures that adequately address these challenges. It is of utmost importance to conduct further research to explore potential solutions, including privacy-preserving technologies, legally compliant design principles, and comprehensive legislative measures that adequately address these challenges.

As we delve into the future, it becomes imperative that legal and ethical considerations stand at the forefront of the design and deployment of advanced authentication mechanisms. With carefully constructed legal frameworks and informed decisions, we can navigate these challenges, ensuring that the adoption of enhanced authentication technologies in electronic services is secure, privacy-preserving, and legally sound. In conclusion, the necessity for enhanced authentication in electronic services is unequivocal, and the path forward, although fraught with challenges, presents opportunities for innovation and progress in achieving a safer and more secure digital world.

A robust international legal framework for enhanced authentication is indeed becoming more critical than ever. Instruments like the Council of Europe's Convention 108 – originally adopted in 1981 and modernized in 2018 – serve as leading examples, advocating principles like fair processing, transparency, and accountability, and extending to biometric data protections. Additionally, frameworks such as the ASEAN Personal Data Protection Framework push for harmonized regional standards, addressing biometric safeguards and cross-border data challenges across Southeast Asia.

When it comes to authentication technologies, established regimes such as the EU's eIDAS regulation prove instructive. eIDAS provides a legal foundation for cross-border recognition of electronic identities and signatures, fostering interoperability and trust across the member states. Likewise, the UNCITRAL Model Law on Electronic Transferable Records (MLETR) offers a technology-neutral template, facilitating acceptance of distributed ledger systems for legally binding records – paving a path for blockchain-based authentication methods.

In the realm of technical standards for biometrics, ISO/IEC JTC 1/SC 37 has created comprehensive international norms for biometric data formats, interfaces, testing and performance, supporting both interoperability and cross-jurisdictional deployment. Complementarily, ISO 19092 outlines a security framework tailored for biometric authentication in financial services, encompassing biometric policy, secure event logs, and cryptographic safeguards. These standards could form the backbone of mandatory and globally consistent requirements within any future legal framework.

Turning to blockchain-specific governance, some jurisdictions already offer useful models. Switzerland's DLT Act integrates blockchain regulation into existing financial laws, clarifying responsibilities and asset segregation rules in case of bankruptcy. Liechtenstein's TVTG (Token and Trusted Technology Service Provider Act) establishes a comprehensive token governance system, while Malta augments EU-wide standards (MiCA) with licensing regimes through its Virtual Financial Assets Act, demonstrating how layered legal structures can operate effectively in concert.

Ultimately, any future convention or treaty aimed at harmonizing enhanced authentication must pull from these existing frameworks. It should enshrine principles drawn from treaties like Convention 108, regulations like eIDAS and MLETR, technical norms from ISO, and modular blockchain governance models. Such a comprehensive legal architecture would enable secure biometric, cryptographic, and blockchain-based authentication systems – rigorously protecting privacy and enabling interoperability, cross-border operation, legal clarity, and technological innovation all at once.

Conclusion. The rapid advancement of digital services underscores the necessity for enhanced authentication mechanisms to protect users from increasing cyber threats and privacy violations. Advanced methods, such as biometric and blockchain authentication, offer promising solutions but entail significant legal implications. Future research should investigate specific case studies of successful integration of biometric and blockchain authentication in compliance-heavy environments such as healthcare and international banking. Carefully constructed legal frameworks and informed decisions will ensure secure, privacy-preserving, and legally sound adoption of enhanced authentication technologies.

The European Union's General Data Protection Regulation (GDPR) imposes strict requirements on the processing of biometric data, classifying it as sensitive personal data. Organizations must obtain explicit, informed consent from individuals before collecting or processing their biometric data. However, the use of biometric data for authentication purposes may be permitted under certain conditions, such as when processing is necessary for reasons of substantial public interest, provided it is based on Union or Member State law and includes suitable and specific measures to safeguard data subjects' fundamental rights and interests.

Similarly, blockchain technology, while offering decentralized and secure authentication solutions, presents challenges in complying with data protection laws. The immutability of blockchain records can conflict with regulations like the GDPR's "right to be forgotten," which allows individuals to request the deletion of their personal data. The decentralized nature of blockchain complicates the identification of data controllers, a requirement under GDPR, raising concerns about accountability and compliance.

While the adoption of advanced authentication methods like biometrics and blockchain offers significant benefits in securing electronic services, it is imperative to navigate the accompanying legal complexities. Establishing comprehensive legal frameworks that address data privacy, consent, and cross-border data flows is crucial. Ongoing research and case studies will be instrumental in shaping policies that balance technological advancements with the protection of individual rights, ensuring a secure and legally compliant digital landscape.

USED SOURCES

1. Li M., Yu S., Zheng Y., Ren K., and Lou W. Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption. *IEEE Transactions on Parallel and Distributed Systems.* 2013. Vol. 24, no. 1, pp. 131–143.

2. Kumar D., Ramani M., and Kuppusamy S. In pursuit of a robust universal user authentication design for E-commerce applications. *Expert Systems with Applications.* 2015. Vol. 42, no. 21, pp. 7518–7532.

3. Li M., Yu S., Y. Zheng, Ren K., and Lou W. Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption. *IEEE Transactions on Parallel and Distributed Systems.* 2013. Vol. 24, no. 1, pp. 131–143.

4. Juels A., and Rivest R. L. Honeywords: Making Password-Cracking Detectable, in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. 2013, pp. 145–160.

5. Zhang Y., Liu W., Lou W., and Hou Y. T. Securing Mobile Healthcare Data: An Associative Marking-based Data Linkage Approach, in Proceedings of the 6th International Symposium on Information, Computer, and Communications Security. 2011, pp. 143–150.

6. Smith S. W. Privacy-preserving Biometric Authentication: Challenges and Opportunities, in Proceedings of the 5th International Conference on Security, Privacy, and Applied Cryptography Engineering. 2015, pp. 147–161.

7. Wright D., and De Hert P. Introduction to Privacy Impact Assessment, in Privacy Impact Assessment. 2012, pp. 3–32.

8. Bygrave L. A. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*. 2017. Vol. 4, no. 2, pp. 105–120.

9. Tistarelli M., Li S. Z., and Chellappa R. Biometrics for Identification and Security, in Handbook of Biometrics. 2009, pp. 1–22.

10. Karpisek K., Cerny F., and Ocenasek A. User Authentication based on the Typing Patterns Analysis. *Information Security*. 2012. Vol. 15, no. 1, pp. 67–80.

11. Bonneau J., Herley C., van Oorschot P. C., and Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes, in Proceedings of the 2012 IEEE Symposium on.

12. De Hert P., and Papakonstantinou V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*. 2016. Vol. 32, no. 2, pp. 179–194.

13. Martin J. K. Surveillance and the Law, in Surveillance and Privacy. 2017, pp. 50–71.

14. Schneier B. Cryptography and Government, in Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2015, pp. 543–576.

15. Crosby M., Pattanayak P., Verma S., and Kalyanaraman V. Blockchain Technology: Beyond Bitcoin. *Applied Innovation*. 2016. Vol. 2, no. 6–10, pp. 71–74.

16. Zheng Z., Xie S., Dai H., Chen X., and Wang H. Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*. 2018. Vol. 14, no. 4, pp. 352–375.

17. Bannister F., and Connolly R. The Trouble with Transparency: A Critical Review of Openness in e-Government. *Policy & Internet*. 2011. Vol. 3, no. 1, pp. 1–30.

18. Leenes R., and De Hert P. Regulating Services in the Physical and Online World, in European Data Protection: Coming of Age. 2013, pp. 327–349.

19. Kuner C. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Privacy & Security Law Report*. 2012. Vol. 11, no. 2, pp. 1–9.

20. Sasse M., and Flechais I. Usable Security: Why Do We Need It? How Do We Get It? in Security and Usability: Designing Secure Systems That People Can Use. 2005, pp. 13–30.

21. Landau S. Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *IEEE Security & Privacy*. 2013. Vol. 11, no. 4, pp. 54–63.

22. Miano T. M. Decentralization the Web: Handshake, Namebase and the Uncensorable Internet. *Richmond Journal of Law and Technology*. 2020. Vol. 26, no. 3, pp. 1–39.

Ф. П. Гусейнзаде. ПОТРЕБА В ПОСИЛЕНІЙ АВТЕНТИФІКАЦІЇ ДЛЯ ЕЛЕКТРОННИХ ПОСЛУГ: ПРАВОВІ ВИКЛИКИ ТА СПОСОБИ ВИРІШЕННЯ

У статті досліджується потреба в посилених механізмах автентифікації для електронних послуг з акцентом на правові виклики та можливі способи їхнього вирішення. Із прискоренням цифровізації в банківській сфері, охороні здоров'я, державному управлінні та інших секторах традиційні методи, як-от паролі та PIN-коди, виявилися недостатніми перед зростаючими кіберзагрозами, крадіжкою особистих даних і витоками інформації. Розширені підходи – біометрична автентифікація, багатофакторна автентифікація, криптографія та блокчейн – пропонують більш надійний захист, однак водночас породжують суттєві правові й етичні виклики. Ключові проблеми охоплюють дотримання вимог законодавства щодо захисту даних, зокрема GDPR, чутливість і незмінність біометричних даних, транскордонну передачу даних і питання відповідальності в децентралізованих системах. У статті детально аналізуються ці виклики та пропонуються потенційні правові рамки для поєднання технологічних інновацій із захистом прав людини. Гармонізація міжнародних стандартів, посилення гарантій захисту даних, забезпечення прозорості й згоди можуть зробити посилену автентифікацію безпечною, законною та надійною основою для електронних послуг у цифрову добу.

Ключові слова: *електронні послуги, автентифікація, правові виклики, безпека, біометрія, шифрування, захист даних, блокчейн, правова база, цифрова ідентичність.*

Стаття надійшла до редколегії 20 жовтня 2025 року