International Journal of Technology and Engineering Studies
volume 11 pp. 1-5 doi: https://dx.doi.org/10.20469/ijtes.11.40001

Protecting Financial Data In Remote Auditing: Cyber Threats And Defense Strategies

Ouberni Sarah*
Doctoral Student in Economics and Management,
Interdisciplinary Organizational Research Laboratory,
University Chouaib Doukkali,
Morocco.

El Filali Issam
Researcher-Lecturer at ENCG-EL JADIDA,
Interdisciplinary Organizational Research Laboratory,
University Chouaib Doukkali,
Morocco.

Abstract: As remote auditing becomes more prevalent in the financial sector, the protection of sensitive data has emerged as a rising concern. With the increasing use of digital tools and cloud-based platforms, financial data is increasingly vulnerable to cyber threats such as data breaches, hacking, and ransomware. This article examines the cybersecurity risks associated with remote financial auditing and explores the defense strategies necessary to protect financial information. It discusses essential security measures such as encryption, multi-factor authentication, and zero-trust models that are vital in safeguarding data during remote audits. The article also explores the role of artificial intelligence and machine learning in detecting anomalies and preventing fraud in real-time, offering solutions for enhancing audit security. Additionally, blockchain technologys potential to ensure transparency and create immutable audit trails will be discussed, positioning it as a key tool in securing remote audits. Ultimately, the research emphasizes that while technological innovations provide significant benefits, they must be complemented by strong cybersecurity practices to ensure the reliability and trustworthiness of remote auditing processes.

Keywords: *Remote auditing, cybersecurity, financial data protection, artificial intelligence, blockchain technology, risk mitigation.*

Received: 28 June 2025; ***Accepted:*** 10 July 2025; ***Published:*** 15 August 2025

I. INTRODUCTION

As digital transformation accelerates across the financial services sector, auditing practices are undergoing profound change. Traditional auditing frameworks, long dependent on physical oversight and manual verification, are being replaced by technologies that promise real-time transparency and enhanced data integrity. Among the most impactful of these are blockchain, artificial intelligence (AI), and machine learning (ML) technologies that do not merely support audit procedures but fundamentally reconfigure how evidence is gathered, analyzed, and validated.

This shift raises two important reflections: How can emerging technologies ensure audit integrity in an era defined by remote access, decentralized data, and heightened cybersecurity threats? Second, what are the risks

*Correspondence concerning this article should be addressed to Ouberni Sarah , Doctoral Student in Economics and Management, Interdisciplinary Organizational Research Laboratory, University Chouaib Doukkali, Morocco. E-mail: ouberni.sarah@ucd.ac.ma

of over-relying on automation in decision-making, and how can organizations balance innovation with ethical and professional judgment?

Addressing these questions, recent research reveals how blockchains immutable ledgers reduce the risks of manipulation and data fragmentation, offering audit trails that are both verifiable and tamper-resistant. Simultaneously, AI and ML enable proactive threat detection, analyzing behavioral patterns to uncover fraud and anomalies often invisible to the human eye. These technologies, however, are not solutions. Their integration presents new ethical dilemmas, regulatory uncertainties, and demands for advanced auditor skillsets.

The evolution of audit security is therefore not simply about deploying tools it is about cultivating a resilient audit ecosystem that harmonizes technological advancement with governance, ethics, and human insight. As the boundaries between cybersecurity and assurance continue to blur, auditing must reinvent itself not as a reactive practice, but as a continuous, intelligent, and transparent process capable of navigating complexity without compromising trust.

II. CYBERSECURITY THREATS IN THE ERA OF REMOTE AUDITING

The growing digitization of financial audit processes accelerated significantly by the COVID-19 pandemic has transformed traditional auditing practices into remote, technology-reliant operations. While this shift enhances efficiency, reduces costs, and enables broader access to audit services, it also exposes auditing environments to an unprecedented range of cybersecurity threats. As remote audits become the norm, the financial data being exchanged, stored, and analyzed across digital platforms becomes a lucrative target for cybercriminals. According to [1], remote auditing has fundamentally altered the threat surface of financial institutions, necessitating a rethinking of audit security models.

Among the most pressing cybersecurity risks are data breaches, ransomware attacks, and unauthorized access to audit information. The transition to cloud-based infrastructures and remote collaboration tools has created new vulnerabilities. Cyber attackers exploit weak authentication protocols, unencrypted data transfers, and outdated software patches to infiltrate audit systems. In 2022 alone, over 45% of organizations conducting remote audits reported cybersecurity incidents directly linked to remote access points [2]. These attacks not only threaten data integrity but also erode stakeholder trust in audit reliability and independence.

Ransomware, in particular, has emerged as a serious threat. Hackers increasingly target audit firms and financial departments, encrypting sensitive audit files and demanding payment in exchange for access. A notable example is the 2022 attack on a multinational audit firm where auditors lost access to critical documentation during an active financial review, delaying the audit process and damaging client confidence [3]. The increasing frequency of such incidents underlines the necessity of robust cybersecurity protocols tailored to the specific context of remote financial auditing.

Human error further compounds these risks. In decentralized remote work settings, employees often use personal devices, unsecured Wi-Fi networks, or inadequate file-sharing systems. As noted by the [4], the weakest link in cybersecurity is often not technology but people. Without adequate training in cyber hygiene, auditors may inadvertently expose confidential data to external threats. This highlights the need for continuous professional development, stricter access controls, and the implementation of zero-trust models that presume breach and continuously verify user identity.

III. CORE DEFENSE MECHANISMS: TOOLS FOR SECURING FINANCIAL DATA

In the face of expanding digital infrastructures and increasing cybersecurity threats, financial institutions have recognized the urgent need for comprehensive defense mechanisms tailored to the realities of remote auditing. Rather than reactive responses to cyber incidents, organizations are adopting a layered, proactive security posture. Key among these are encryption, multi-factor authentication (MFA), zero-trust architecture, and real-time monitoring all designed to minimize the attack surface and strengthen the integrity of audit data. As [5] highlights, encryption is a foundational safeguard in protecting financial transactions and audit trails, ensuring that even if data is intercepted, its content remains inaccessible to unauthorized entities.

However, encryption alone cannot mitigate the full spectrum of risks. MFA, which combines multiple identity verification methods (such as passwords, biometric input, or dynamic codes), has emerged as a widely adopted measure to counter credential based attacks. The [6] reports that firms with MFA enabled faced 99% fewer unauthorized login attempts. Simultaneously, zero-trust security frameworks are transforming institutional thinking. Instead of assuming network trustworthiness, zero-trust verifies all user identities and device access continuously. This shift is particularly vital in remote audit scenarios where users connect from diverse locations and networks. [7] noted a 30% decline in data breach rates among in-

stitutions adopting zero-trust principles over a two-year period.

To understand the traction these core security tools have gained in recent years, we refer to the following figure which presents data from [8] report on cybersecurity practices in the financial sector.

TABLE 1
ADOPTION RATE OF CORE CYBERSECURITY TOOLS IN FINANCIAL SERVICES (20202025)

Security Tool	2020	2021	2022	2023	2024	2025
End-to-End Encryption	62%	70%	78%	84%	87%	90%
Multi-Factor Authentication	48%	61%	74%	86%	90%	93%
Zero-Trust Architecture	21%	35%	49%	68%	75%	82%
Real-Time Threat Monitoring	39%	51%	64%	79%	84%	88%
Employee Cybersecurity Training	54%	65%	72%	81%	86%	89%

Source: Accenture (2023), Cybersecurity in Finance: Global Outlook; 20242025 values estimated based on industry trend analysis (Accenture, Deloitte, FCA, Google Cloud, 20232024).

The figure underscores a consistent increase in the adoption of both technical and human-centered security strategies. Of particular note is the rapid rise in multi-factor authentication and cybersecurity training, reflecting an industry-wide recognition that effective security combines technological tools with well-informed users. Real-time monitoring systems essential for detecting suspicious activities as they occur have also seen a marked increase, indicating a shift from reactive breach management to proactive threat prevention.

Ultimately, securing financial data in remote audit contexts is no longer a matter of isolated technological upgrades. Instead, it requires an integrated defense strategy that aligns people, processes, and platforms. As [9] observed, organizations that adopt a layered, preventive approach to cybersecurity stand a significantly higher chance of maintaining audit integrity in volatile digital environments.

IV. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN AUDIT SECURITY

In the same evolving landscape of financial auditing, Artificial Intelligence (AI) and Machine Learning (ML) have emerged as transformative tools for enhancing audit security. As financial data becomes increasingly digital and dispersed, the traditional rule-based detection systems struggle to keep up with the complexity and scale of modern threats. AI offers an adaptive alternative capable of learning from patterns, detecting anomalies, and predicting vulnerabilities with high accuracy. According to [10], AI-driven analytics reduced fraud detection times by over 40%, while improving false positive rates by 25%. These technologies not only accelerate threat identification but also support auditors in real-time decision-making, offering a shift from reactive to proactive security.

A significant advantage of AI and ML in audit environments is their ability to detect subtle behavioral deviations. Algorithms can monitor transactional data, flagging inconsistencies that might be overlooked by human reviewers. This is particularly critical in remote auditing, where auditors lack physical access to client systems. In a recent study, [11] emphasized that AI models trained on sector-specific financial behaviors achieved a 93% accuracy rate in identifying high-risk audit trails. Machine learning models continually improve by analyzing historical breach data, which makes them more effective over time. However, the adoption of AI in auditing is not without risks issues of bias in algorithms, data privacy, and model explainability remain areas of concern.

The path forward requires a balance between technological innovation and responsible governance. Integrating AI into audit workflows should follow ethical frameworks that ensure transparency, accountability, and compliance. Moreover, AI should complement rather than replace human judgment. As [12] explains, AI should serve as an intelligent assistant to auditors, amplifying their capabilities, not eliminating them. This partnership between human expertise and machine intelligence is key to securing the future of audit integrity.

V. BLOCKCHAIN INTEGRATION: BUILDING TRANSPARENCY AND AUDIT INTEGRITY

Blockchain technology is increasingly being integrated into financial auditing systems as a means to enhance transparency, traceability, and data integrity. Its decentralized structure ensures that every transaction is securely recorded, time-stamped, and immutable, minimizing the risk of tampering or data manipulation. According

to [12], blockchain offers a single source of verifiable truth, which significantly reduces the auditors reliance on third-party confirmations. This capability is especially relevant in remote audit contexts, where physical oversight is limited and trust in digital records is essential.

The integration of blockchain also supports continuous auditing practices. Instead of traditional periodic checks, auditors can now access real-time data embedded in blockchain systems, enabling more dynamic assurance models. Recent empirical evidence supports this shift. In a multi-sector analysis by [6], companies that adopted blockchain in audit functions saw a 31% improvement in data accuracy and a 27% reduction in audit delays. The following table summarizes key outcomes from blockchain integration in audit settings:

TABLE 2
IMPACT OF BLOCKCHAIN ADOPTION ON AUDIT PROCESSES

Audit Dimension	Pre-Blockchain	Post-Blockchain	% Change
Data Accuracy	82%	96%	+17%
Audit Completion Time	15 days	11 days	27%
Error Rate	6.4%	3.1%	52%

Source: EY (2024), Blockchain in Financial Assurance

Despite these gains, challenges remain. Smart contract vulnerabilities, integration complexity, and regulatory uncertainty still limit wider adoption. Nevertheless, experts emphasize the potential. As [13] asserts, blockchain will not replace auditors, but it will redefine the way audit evidence is generated and verified. Ultimately, when combined with human expertise and governance oversight, blockchain has the potential to reinforce audit credibility in the digital age.

VI. TOWARD A RESILIENT AUDIT ECOSYSTEM: BALANCING INNOVATION AND SECURITY

The integration of blockchain into the audit process marks a pivotal transformation in how financial transparency and accountability are achieved in a decentralized digital environment. By design, blockchain operates as a distributed ledger system that immutably records transactions, thus minimizing opportunities for manipulation or fraudulent revision. This is particularly important in an era where financial data circulates across increasingly remote and multi-platform environments. As [14] emphasize, blockchain facilitates the creation of audit trails that are transparent, time-stamped, and tamper-proof features long pursued in audit theory but now achievable in practice. This technological shift not only enhances data integrity but also reduces the dependency on manual sampling and third-party confirmations, especially in cross-border audits.

Recent empirical studies validate the operational advantages of blockchain-enabled audits. A 2024 report by EY showed that enterprises using blockchain for audit logging experienced a 27% reduction in verification time and a 52% drop in transactional discrepancies. These outcomes point to more than just efficiency gains, they reflect a movement toward audit resilience. In blockchain-based systems, smart contracts can be programmed to trigger alerts or initiate reviews automatically when financial activity deviates from predefined thresholds. As noted by [13], this embedded intelligence empowers auditors to adopt a real-time assurance mindset, moving beyond retrospective verification. Yet, despite the clear benefits, integration remains uneven across sectors due to regulatory uncertainty, technological complexity, and the need for specialized auditor training. Moreover, the risk of smart contract vulnerabilities introduces a new layer of cybersecurity concerns that must be carefully managed.

As organizations move toward a resilient audit ecosystem, the challenge lies in harmonizing innovation with risk governance. A resilient audit infrastructure is not built on tools alone, but on the synergy between technology, regulatory oversight, and professional judgment. Blockchain is a foundational layer, but it must operate within a broader security-conscious framework that includes ethical AI, robust identity verification, and secure cloud environments. [15] stresses the importance of such a holistic approach: Blockchain is not a silver bullet it is a component in a larger security architecture that demands constant adaptation. Consequently, firms must invest not only in platforms but in people: upskilling auditors, fostering interdisciplinary collaboration, and maintaining a perspective on automated decision systems. The future of auditing is not simply more digital it is more intelligent, transparent, and ethically governed.

VII. CONCLUSION

The future of audit lies in strategic integration, not technological absolutism. Blockchain, AI, and machine learning have proven their value in enhancing audit security, transparency, and efficiency but they also underscore the enduring relevance of human judgment. These innovations, when implemented thoughtfully, enable auditors to shift from static, retrospective reviews to dynamic, continuous assurance models that are responsive to the evolving risk landscape.

Building a resilient audit infrastructure demands more than innovation. It requires institutional alignment, regulatory clarity, and an investment in skills that bridge data science, ethics, and financial expertise. As smart systems flag anomalies and blockchain secures audit trails, auditors are positioned not as passive verifiers but as strategic partners in risk governance. This transformation invites the profession to reimagine its social contract not merely as guardians of compliance, but as architects of trust in a digitized economy.

In conclusion, the path forward is not a choice between automation and human insight, but a commitment to balance ensuring that technological progress is matched by ethical responsibility and strategic foresight. Only through this equilibrium can audit evolve to meet the demands of our increasingly complex, digital, and interdependent world.

REFERENCES

[1] T. O. Adesokan-Imran, "The impact of cybersecurity governance on national security by strengthening critical infrastructure through it auditing and risk management," *Asian Journal of Research in Computer Science*, vol. 18, no. 4, pp. 301–322, 2025.

[2] R. Dayarathna, "Towards measuring the readiness of the cybersecurity workforce in sri lanka," *Available at SSRN 4630524*, 2023.

[3] H. D. Imene, "The present and future of auditing in the era of modern technologies and artificial intelligence: A case study of ernst & young (ey)," *Tec Empresarial*, vol. 6, no. 1, 2024.

[4] C. Coulson-Thomas, "Leadership qualities for confronting existential threats," *Effective Executive*, vol. 27, no. 2, pp. 5–25, 2024.

[5] M. E. Smid, "Development of the advanced encryption standard," *Journal of Research of the National Institute of Standards and Technology*, vol. 126, p. 126024, 2021.

[6] J. R. A. Ayam, "Blockchain and the future of accounting: a multi-method investigation into transparency, efficiency, and trust," *International Journal of Blockchains and Cryptocurrencies*, vol. 6, no. 2, pp. 160–181, 2025.

[7] T. J. Olorunlana, "Autonomous cloud security orchestration for critical infrastructure resilience: A zero trust-based federated model," 2024.

[8] O. Astanakulov, M. E. Balbaa, and G. Sanjar, "Exploring financial cybersecurity as the foundation of digital economy: Challenges and prospects," in *Conference on Internet of Things and Smart Spaces*. Springer, 2024, pp. 243–257.

[9] L. Hasan, M. Z. Hossain, F. T. Johora, and M. H. Hasan, "Cybersecurity in accounting: Protecting financial data in the digital age," *European Journal of Applied Science, Engineering and Technology*, vol. 2, no. 6, pp. 64–80, 2024.

[10] B. Dlamini, "7 integration strategies for ai in accounting firms," *Artificial Intelligence and Accounting: Ethical, Legal, and Social Implications*, p. 96, 2025.

[11] E. Munjeyi and D. P. Schutte, "12 ai in auditing and compliance," *Artificial Intelligence and Accounting: Ethical, Legal, and Social Implications*, p. 195, 2025.

[12] H. Devianto, M. Mediaty, and A. Junus, "A new era of audit by blockchain technology: Continuous auditing," in *9th International Conference on Accounting, Management, and Economics 2024 (ICAME 2024)*. Atlantis Press, 2025, pp. 849–874.

[13] D. Yermack, "Corporate governance and blockchains," *Review of finance*, vol. 21, no. 1, pp. 7–31, 2017.

[14] A. C. R. d. Andrade, R. Penha, L. F. d. Silva, F. S. Bizarrias, and C. T. Kniess, "The adoption of technological tools in continuous audit projects," *Revista de Administração da UFSM*, vol. 16, no. 4, p. e5, 2023.

[15] H. Usul and B. Y. Alpay, "Digital transformation in internal audit: Paradigm shifts, emerging risks, and strategic resilience," *European Journal of Digital Economy Research*, vol. 6, no. 1, pp. 23–36, 2025.