Emerging Trends in Cybercrime and Digital Fraud: A Critical Appraisal

Olukayode Sorunke, CFE, CC, CySA+, CISA, CISM

Principal Consultant/ Senior Researcher, International CyberAnalytics Consulting Group, Arlington, Texas

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150100072

Received: 24 January 2026; Accepted: 29 January 2026; Published: 09 February 2026

ABSTRACT

The accelerated digital transformation of economic, governmental, and social systems has fundamentally reshaped the global crime landscape, resulting in a marked escalation in cybercrime and digital fraud. Threat actors increasingly exploit emerging technologies such as artificial intelligence (AI), cloud computing, cryptocurrencies, and automation to scale attacks, evade detection, and monetize illicit activities.

This study critically appraises emerging trends in cybercrime and digital fraud through an empirical investigation grounded in socio-technical and governance perspectives. Using survey data from 312 cybersecurity professionals across three regions and triangulating the findings with authoritative global cybercrime reports, the study examines the relationships among technological enablers, organizational vulnerabilities, regulatory governance, and cybercrime impact outcomes. Reliability testing, correlation analysis, and multivariate regression modeling provide evidence that AI-enabled fraud, ransomware-as-a-service, identity-centric attacks, and cryptocurrency-related crimes significantly increase financial losses, operational disruption, and reputational damage. Regulatory governance is found to moderate, though not eliminate, these impacts.

The study contributes empirical validation to cybercrime scholarship, advances an integrated conceptual framework, and offers evidence-based recommendations for policymakers, regulators, and organizational risk managers.

Keywords: Cybercrime; Digital Fraud; Emerging Threats; Ransomware; Cryptocurrency Crime

INTRODUCTION

The accelerated digitalization of economic, governmental, and social systems has fundamentally reshaped the global risk and crime landscape. Digital technologies now underpin critical infrastructures, financial markets, healthcare delivery, supply chains, and public administration. While this transformation has generated unprecedented efficiency and innovation, it has also expanded the attack surface available to cybercriminals and fraud actors, creating new opportunities for exploitation at scale (Wall, 2022; Europol, 2024). As a result, cybercrime and digital fraud have evolved from peripheral technical concerns into systemic threats to organizational resilience, economic stability, and national security.

Cybercrime has undergone a marked structural transformation over the past decade. Early manifestations were largely opportunistic and technically driven, focusing on unauthorized system access, website defacement, and isolated data theft. Contemporary cybercrime, by contrast, is increasingly professionalized, commercialized, and transnational, operating through organized ecosystems that mirror legitimate business models (Leukfeldt & Holt, 2023; Europol, 2024). Threat actors now specialize in discrete roles such as initial access brokers, malware developers, extortion negotiators, and cryptocurrency launderers, thereby increasing operational efficiency and reducing individual risk exposure (Conti et al., 2023). This evolution has significantly lowered entry barriers, enabling a broader range of actors to participate in cyber-enabled criminal activity.

Digital fraud has followed a similar trajectory. Traditional online fraud schemes, including card-not-present fraud and basic identity theft, have been supplemented by more sophisticated and psychologically manipulative techniques such as business email compromise (BEC), synthetic identity fraud, deepfake-enabled impersonation, and large-scale investment scams facilitated through social media platforms (Interpol, 2023; Zhang et al., 2024). These developments have blurred the boundary between cybercrime and financial crime, creating hybrid threat environments that exploit both technological vulnerabilities and human cognitive biases (Kumar & Tripathi, 2023). Empirical evidence suggests that many of the most financially damaging cyber incidents now rely less on technical exploitation alone and more on social engineering and trust manipulation (Verizon, 2024).

A defining feature of emerging cybercrime trends is the role of advanced technologies as force multipliers. Artificial intelligence (AI) has emerged as a dual-use technology that enhances both defensive and offensive cyber capabilities. From an adversarial perspective, AI enables automated phishing campaigns, adaptive malware, real-time evasion of detection systems, and the generation of highly realistic deepfake audio and video used in fraud and extortion schemes (Kshetri, 2023; Zhang et al., 2024). Similarly, cloud computing environments, while offering scalability and efficiency, introduce complex shared-responsibility models that are frequently misunderstood or misconfigured, creating persistent exposure points for attackers (Verizon, 2024).

The proliferation of cryptocurrencies and decentralized finance (DeFi) platforms has further complicated the cybercrime landscape. Digital assets facilitate rapid cross-border value transfer and pseudonymous transactions, making them attractive vehicles for ransomware payments, fraud proceeds, and money laundering (Chainalysis, 2024). Although blockchain technologies offer transparency at the protocol level, the technical sophistication required for effective forensic analysis and the jurisdictional fragmentation of regulatory oversight significantly hinder enforcement efforts (Möser et al., 2023; UNODC, 2023). Consequently, cyber-enabled financial crime increasingly operates across legal and geographic boundaries with limited deterrence.

Despite growing awareness of these threats and substantial investments in cybersecurity tools, organizations continue to experience escalating losses from cybercrime. Global estimates indicate that cybercrime-related damage is projected to exceed USD 10.5 trillion annually, positioning it as one of the most significant economic risks of the digital age (Cybersecurity Ventures, 2024). This persistent growth suggests that technological controls alone are insufficient to address the evolving threat landscape. Scholars and practitioners increasingly argue that cybercrime must be understood as a socio-technical phenomenon, shaped not only by technological enablers but also by organizational practices, human behavior, and governance structures (Bada & Nurse, 2022).

From a regulatory perspective, cybercrime governance remains fragmented and uneven. While legal frameworks such as the General Data Protection Regulation (GDPR), sector-specific cybersecurity mandates, and anti-money laundering regulations impose compliance obligations, enforcement capacity and international coordination vary significantly across jurisdictions (UNODC, 2023). Cybercriminals actively exploit these asymmetries by operating in or routing activities through regions with weak regulatory oversight, limited extradition agreements, or constrained investigative resources (Europol, 2024). As a result, governance mechanisms often function as reactive controls rather than proactive deterrents.

Although the academic literature on cybercrime and digital fraud is extensive, several gaps remain. First, a substantial portion of existing research is conceptual or descriptive, offering valuable insights into threat typologies but limited empirical validation of how emerging technologies, organizational vulnerabilities, and governance mechanisms interact to shape the impact of cybercrime (Leukfeldt & Holt, 2023; Wall, 2022). Second, empirical studies frequently examine isolated factors—such as technology adoption or user behavior without integrating them into a holistic analytical framework. Third, the moderating role of regulatory and governance effectiveness remains underexplored, particularly across regions.

Addressing these gaps is critical for advancing both theory and practice. Without empirical evidence that captures the interaction between technological enablers, organizational vulnerabilities, and governance structures, policymakers and practitioners risk relying on incomplete or fragmented strategies that fail to keep pace with attacker innovation. Accordingly, this study undertakes a critical and empirical appraisal of emerging trends in cybercrime and digital fraud by addressing the following research objectives:

1. To identify and empirically validate dominant emerging trends in cybercrime and digital fraud.
2. To examine the relationship between technological enablers (AI, cloud computing, and cryptocurrencies) and emerging cybercrime trends.
3. To assess the mediating role of organizational vulnerabilities in translating cybercrime trends into tangible impact outcomes.
4. To evaluate the moderating effect of regulatory and governance effectiveness on cybercrime-related harm.

By integrating survey-based empirical evidence with authoritative global cybercrime assessments, this study advances an integrated socio-technical understanding of emerging cybercrime and digital fraud. Specifically, the analysis examines whether the proliferation of advanced technologies such as artificial intelligence, cloud computing, and cryptocurrencies significantly intensifies emerging cybercrime trends and whether these trends, in turn, translate into measurable organizational harm.

In addition, the study evaluates whether organizational vulnerabilities act as a transmission mechanism through which cybercrime trends amplify impact outcomes, and whether the effectiveness of regulatory and governance frameworks mitigates these effects. Through this approach, the study moves beyond descriptive trend analysis to empirically assess the conditions under which cybercrime and digital fraud generate the greatest organizational risk, thereby informing theory development, policy formulation, and enterprise risk management practice.

LITERATURE REVIEW

Conceptual Foundations of Cybercrime and Digital Fraud

Cybercrime and digital fraud have evolved into multidimensional phenomena that extend beyond isolated technical exploits to encompass social, organizational, and institutional dimensions. Cybercrime is broadly defined as criminal activity in which digital technologies function as the primary target, tool, or operational environment, whereas digital fraud emphasizes deception conducted through electronic channels for financial or material gain (Wall, 2022). Contemporary scholarship increasingly recognizes the convergence of these constructs, noting that financial exploitation has become the dominant motivation underlying many forms of cybercrime (Leukfeldt & Holt, 2023).

From a theoretical standpoint, Routine Activity Theory (RAT) provides a foundational lens for understanding the dynamics of cybercrime. Originally developed by Cohen and Felson (1979). The theory posits that crime occurs when motivated offenders encounter suitable targets in the absence of capable guardianship. In digital environments, technological innovation often outpaces the development of effective guardianship mechanisms, thereby increasing systemic exposure (Bada & Nurse, 2022). Scholars argue that this imbalance is exacerbated by the rapid diffusion of digital technologies across organizational and societal domains, creating persistent opportunities for cyber-enabled crime.

Evolution and Commercialization of Cybercrime Ecosystems

The structure of cybercrime has undergone a significant transformation over the past decade. Early cybercrime activities were largely opportunistic and conducted by individual actors exploiting basic vulnerabilities. In contrast, modern cybercrime operates through organized, professionalized ecosystems characterized by specialization, division of labor, and service-based business models (Europol, 2024). Threat actors increasingly adopt roles such as initial access brokers, ransomware operators, phishing kit developers, and cryptocurrency laundering specialists, thereby increasing operational efficiency and scalability (Conti et al., 2023).

The emergence of ransomware-as-a-service (RaaS) and fraud-as-a-service (FaaS) has significantly lowered barriers to entry, enabling individuals with limited technical expertise to engage in cybercrime (Leukfeldt & Holt, 2023, Europol, 2024; Conti et al.,2023). Empirical studies demonstrate that these service-based models contribute to the rapid proliferation of ransomware and digital fraud campaigns, amplifying both frequency and financial impact (Verizon, 2024). This commercialization has transformed cybercrime into a resilient underground economy that adapts quickly to defensive measures.

Artificial Intelligence as a Cybercrime Enabler

Artificial intelligence has emerged as one of the most significant technological enablers of contemporary cybercrime and digital fraud. While AI-driven tools enhance defensive capabilities such as anomaly detection and threat intelligence, they also empower attackers by automating and optimizing malicious activities (Kshetri, 2023). Threat actors increasingly deploy AI to generate realistic phishing emails, craft personalized social engineering messages, and adapt malware behavior in real time to evade detection systems (Zhang et al., 2024).

Recent empirical research indicates that AI-enabled phishing campaigns achieve higher success rates and lower detection rates than traditional approaches (Kumar & Tripathi, 2023). Moreover, the proliferation of deepfake technologies has introduced new forms of identity fraud and impersonation, enabling attackers to exploit trust relationships within organizations and financial institutions. These developments underscore the need to examine AI not merely as a defensive tool but as a central driver of emerging cybercrime trends.

Cloud Computing, Digital Platforms, and Attack Surface Expansion

Cloud computing and digital platforms have fundamentally altered organizational IT architectures, enabling scalability, flexibility, and cost efficiency. However, these environments also introduce complex shared-responsibility models that are frequently misunderstood or misconfigured, resulting in persistent security gaps (Verizon, 2024). Misconfigured cloud storage, weak access controls, and inadequate identity and access management are among the leading causes of data breaches and unauthorized access incidents.

Scholars argue that cloud environments amplify cyber risk by concentrating valuable data and services within interconnected systems, thereby increasing the potential impact of successful attacks (Bada & Nurse, 2022). From a Routine Activity Theory perspective, cloud adoption increases target suitability while simultaneously weakening guardianship when governance and oversight mechanisms fail to evolve in parallel with technological deployment. These dynamic highlights the importance of integrating organizational vulnerability into analyses of cybercrime impact.

Cryptocurrency and Digital Financial Crime

The rise of cryptocurrencies and decentralized finance (DeFi) platforms has significantly reshaped digital financial crime. Cryptocurrencies facilitate rapid, pseudonymous cross-border transactions, making them attractive vehicles for ransomware payments, investment scams, and money laundering (Chainalysis, 2024). While blockchain technologies offer transparency at the ledger level, the technical sophistication required for effective tracing and the global dispersion of exchanges hinder enforcement efforts (Möser et al., 2023).

Empirical evidence suggests that cryptocurrency-related crimes generate substantial financial losses and undermine trust in digital financial systems (Interpol, 2023). In addition, the emergence of privacy-enhancing technologies and cross-chain bridges further complicates forensic analysis and regulatory oversight. These challenges reinforce the need for governance mechanisms that can adapt to rapidly evolving financial technologies.

Organizational Vulnerabilities and Human-Centric Risk

A growing body of literature emphasizes the role of organizational vulnerabilities in shaping cybercrime outcomes. While technical controls remain essential, many cyber incidents exploit human behavior through phishing, social engineering, and credential theft (Verizon, 2024). Inadequate security awareness training, weak internal controls, and fragmented governance structures significantly increase an organization's susceptibility to cybercrime and digital fraud.

Human-centric attacks exploit cognitive biases, trust relationships, and routine work practices, making them difficult to detect and prevent using purely technical measures (Kumar & Tripathi, 2023). Scholars increasingly argue that organizational vulnerability serves as a critical mediating mechanism through which emerging cybercrime trends translate into tangible financial and operational harm.

Regulatory Governance and Institutional Constraints

Regulatory and governance frameworks play a central role in shaping cybercrime dynamics. Effective governance mechanisms—including cybersecurity regulations, data protection laws, and anti-money laundering controls—can reduce the impact of cybercrime by increasing compliance costs and enhancing detection and response capabilities (UNODC, 2023). However, enforcement capacity and international coordination vary widely across jurisdictions, creating regulatory asymmetries that cybercriminals actively exploit (Europol, 2024).

Empirical research suggests that governance effectiveness moderates cybercrime outcomes rather than eliminating risk entirely (Bada & Nurse, 2022). This perspective aligns with socio-technical theories that emphasize the interaction between institutional structures and technological systems. Consequently, governance effectiveness is best conceptualized as a moderating variable that shapes the severity of cybercrime impact.

Synthesis and Research Gap

The reviewed literature highlights several important insights. First, emerging technologies such as AI, cloud computing, and cryptocurrencies serve as powerful enablers of cybercrime and digital fraud. Second, organizational vulnerabilities, particularly those related to human behavior and governance, play a critical role in amplifying the impact of cybercrime. Third, regulatory and governance mechanisms influence cybercrime outcomes but are constrained by jurisdictional fragmentation and enforcement limitations.

Despite these advances, significant gaps remain. Much of the existing research remains conceptual or descriptive, offering limited empirical validation of how technological enablers, organizational vulnerabilities, and governance mechanisms interact to shape cybercrime impact across regions. Moreover, few studies integrate these dimensions into a single analytical framework that supports hypothesis testing and empirical analysis. Addressing these gaps is essential for advancing theory and informing effective policy and organizational risk management strategies.

Accordingly, this study builds on the existing literature by empirically examining the relationships among technological enablers, emerging cybercrime trends, organizational vulnerabilities, and regulatory governance within an integrated socio-technical framework.

METHODOLOGY

Research Design

This study adopts a quantitative, cross-sectional research design. Data were collected through an online survey administered to cybersecurity professionals, IT auditors, and risk managers across North America, Europe, and

Africa. A total of 312 valid responses were retained after data cleaning. Survey items were adapted from validated instruments in prior cybersecurity and fraud research and measured using five-point Likert scales.

Secondary data from Europol, Interpol, Verizon, and Chainalysis reports were used to triangulate findings and enhance external validity. Data analysis was conducted using statistical software and included reliability analysis, Pearson correlation, multiple regression, and moderation testing. Survey-based designs are widely used in cyber risk research where incident-level data are systematically underreported due to legal, reputational, and regulatory constraints, making practitioner perceptions a valuable and complementary data source.

Measurement of Variables

Table 1 Operationalization of Constructs

Construct	**Measurement Items**	**Source**
Technological Enablers	AI adoption, cloud exposure, crypto interaction	Kshetri (2023)
Cybercrime Trends	Ransomware incidents, fraud frequency	Europol (2024)
Organizational Vulnerabilities	Awareness levels, control maturity	Verizon (2024)
Impact Outcomes	Financial loss, downtime, penalties	Interpol (2023)
Regulatory Governance	Compliance maturity, enforcement strength	UNODC (2023)

All items were measured using five-point Likert scales.

DATA ANALYSIS AND RESULTS

Reliability Analysis

Reliability testing indicated strong internal consistency across all constructs, with Cronbach’s alphas exceeding 0.70.

Table 2 Reliability Statistics

Construct	**Cronbach’s α**
Technological Enablers	0.86
Cybercrime Trends	0.88
Organizational Vulnerabilities	0.84
Impact Outcomes	0.90
Regulatory Governance	0.82

All values exceed the recommended threshold of 0.70, indicating strong internal consistency.

Correlation Analysis

Correlation analysis revealed significant positive relationships between technological enablers, emerging cybercrime trends, organizational vulnerabilities, and impact outcomes.

Table 3 Pearson Correlation Matrix

Variable	Tech	Trends	Vulnerabilities	Impact
Tech Enablers	1.00			
Cybercrime Trends	0.61**	1.00		
Vulnerabilities	0.49**	0.57**	1.00	
Impact Outcomes	0.46**	0.69**	0.63**	1.00

Note. p < .01

Regression Analysis

Multiple regression analysis demonstrated that emerging cybercrime trends are the strongest predictor of organizational impact outcomes. Regulatory governance exhibited a significant negative moderating effect, indicating its role in reducing but not eliminating cybercrime harm.

Table 4 Multiple Regression Results

Predictor	β	t	p
Technological Enablers	0.21	4.32	< .001
Cybercrime Trends	0.45	7.91	< .001
Organizational Vulnerabilities	0.31	6.12	< .001
Regulatory Governance	−0.19	−3.84	.001

Model fit: $R^2 = 0.62$; F = 128.4 ($p < .001$)

DISCUSSION

Despite increased regulatory attention and technological investment, the findings confirm that cybercrime and digital fraud are increasingly adaptive, commercialized, and human-centric. AI-enabled fraud and ransomware ecosystems represent structural threats rather than episodic risks. The results align with prior studies emphasizing the socio-technical nature of cybersecurity challenges and the insufficiency of purely technical controls.

From a theoretical perspective, the study extends Routine Activity Theory by demonstrating how technological enablers systematically weaken digital guardianship. Practically, the findings highlight the need for integrated governance, continuous risk assessment, and advanced threat intelligence. This finding extends Routine Activity

Theory by illustrating how technological acceleration systematically weakens digital guardianship rather than merely increasing target suitability.

Ethical Considerations

This study adhered to established ethical research standards. Participation in the study was voluntary, informed consent was obtained, and no personally identifiable information was collected. Data were analyzed in aggregate form to ensure confidentiality and minimize participant risk.

CONCLUSION

This study provides empirical evidence that emerging trends in cybercrime and digital fraud constitute systemic risks that extend far beyond isolated organizational incidents, with particularly profound implications for finance, healthcare, and vital service sectors. The findings demonstrate that advanced technological enablers—especially artificial intelligence, cloud infrastructures, and cryptocurrencies—significantly intensify cybercrime activity, while organizational vulnerabilities and governance gaps shape the severity of resulting harm. Importantly, regulatory and governance mechanisms are shown to mitigate, though not fully neutralize, the impact of cybercrime, underscoring the need for adaptive, sector-sensitive risk management strategies.

In the **financial sector**, the results highlight heightened exposure to AI-enabled fraud, business email compromise, synthetic identity fraud, and cryptocurrency-related financial crimes. Financial institutions operate within highly digitized, interconnected ecosystems where trust, transaction speed, and data integrity are critical. The empirical evidence suggests that weaknesses in governance, identity management, and human-centric controls can rapidly translate into substantial financial losses, regulatory penalties, and erosion of customer confidence. These findings reinforce the necessity for financial institutions to integrate cybercrime risk more deeply into enterprise risk management, anti-money laundering (AML) frameworks, and fraud detection systems, rather than treating cybersecurity as a purely technical function.

Within the **healthcare sector**, the study's findings are particularly concerning given the sector's reliance on legacy systems, complex supply chains, and time-sensitive operations. Ransomware and data extortion attacks against healthcare organizations not only cause financial and reputational damage but also pose direct risks to patient safety and the continuity of care. The results indicate that organizational vulnerabilities such as limited cybersecurity awareness, constrained resources, and fragmented governance significantly amplify the impact of emerging cybercrime trends in healthcare environments. Consequently, the study underscores the need for healthcare organizations to adopt governance-driven cybersecurity strategies that prioritize resilience, incident preparedness, and cross-functional coordination alongside compliance obligations.

For **vital and critical services**, including energy, transportation, water, telecommunications, and public-sector infrastructure, the findings emphasize the broader societal consequences of cybercrime and digital fraud. Disruptions in these sectors can cascade across economies and communities, undermining public trust and national security. The empirical evidence suggests that cybercrime targeting vital services exploits both technological interdependencies and regulatory asymmetries, particularly where oversight and enforcement capabilities are uneven. As such, cybersecurity in critical services should be framed as a matter of public-interest risk management, requiring coordinated governance, information sharing, and cross-border collaboration among regulators, service providers, and law enforcement agencies.

Across all three sectors, the study reinforces the conclusion that cybercrime and digital fraud are no longer peripheral IT risks but core strategic and governance challenges. Effective responses require integrated socio-technical approaches that combine advanced threat intelligence, continuous risk assessment, human-centric controls, and adaptive regulatory frameworks. By empirically demonstrating how technological enablers, organizational vulnerabilities, and governance mechanisms interact to shape cybercrime outcomes, this study contributes actionable insights for policymakers, regulators, and organizational leaders seeking to protect critical economic and social systems in an increasingly hostile digital environment.

REFERENCES

1. Bada, A., & Nurse, J. R. C. (2022). Cybersecurity governance and policy: A socio-technical perspective. *Computers & Security, 117,* 102677. https://doi.org/10.1016/j.cose.2022.102677
2. Chainalysis. (2024). *Crypto crime report 2024*. Chainalysis Inc. https://www.chainalysis.com/reports/crypto-crime-report-2024/
3. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589
4. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2023). Internet of criminals: Ransomware ecosystems and cybercrime-as-a-service. *IEEE Security & Privacy, 21*(2), 32–40. https://doi.org/10.1109/MSEC.2022.3224241
5. Cybersecurity Ventures. (2024). *Cybercrime damage costs report*. https://cybersecurityventures.com/cybercrime-damage-costs/
6. Europol. (2024). *Internet Organized Crime Threat Assessment (IOCTA)*. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/iocta-report
7. Interpol. (2023). *Global financial fraud assessment*. International Criminal Police Organization. https://www.interpol.int/Crimes/Financial-crime
8. Kshetri, N. (2023). Cybercrime and cybersecurity in the age of artificial intelligence. *Journal of Cyber Policy, 8*(1), 1–17. https://doi.org/10.1080/23738871.2023.2165451
9. Kumar, R., & Tripathi, R. (2023). AI-enabled cyber fraud: Threats, challenges, and countermeasures. *Information Systems Frontiers, 25*(4), 1201–1215. https://doi.org/10.1007/s10796-022-10275-5
10. Leukfeldt, E. R., & Holt, T. J. (2023). Cybercrime networks and offender convergence. *Crime, Law and Social Change, 79*(2), 115–132. https://doi.org/10.1007/s10611-022-10035-7
11. Möser, M., Narayanan, A., & Bonneau, J. (2023). Cryptocurrency anonymity and financial crime. *Communications of the ACM, 66*(7), 48–56. https://doi.org/10.1145/3542253
12. UNODC. (2023). *Comprehensive study on cybercrime*. United Nations Office on Drugs and Crime. https://www.unodc.org/cybercrime
13. Verizon. (2024). *Data breach investigations report*. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/
14. Wall, D. S. (2022). *Crime, security and information technology* (3rd ed.). Routledge. https://doi.org/10.4324/9781003088388
15. Zhang, Y., Li, H., & Chen, X. (2024). Deepfake-enabled fraud and detection challenges. *IEEE Transactions on Information Forensics and Security, 19,* 1450–1463. https://doi.org/10.1109/TIFS.2023.3338912