

• Email: editor@ijfmr.com

Assessing the Impact of AI-Driven Trust Scoring on Consumer Financial Decision-Making in **India's Digital Ecosystem**

Chandra Shikhi Kodete

School of Technology, Eastern Illinois University, Charleston, IL 61920, USA

Abstract

Artificial intelligence-driven trust scoring has emerged as a pivotal innovation in digital finance, offering granular evaluations of provider compliance, risk and security posture. This literature review critically synthesises conceptual frameworks of trust, behavioural decision-making theories and emerging AI trustscoring methodologies to assess their impact on consumer financial choices in India. We explore institutional, interpersonal and technological trust dimensions, examine theoretical models; Theory of Planned Behavior and Heuristic-Systematic Model; and detail machine-learning, NLP and anomaly-detection mechanisms underpinning trust scores. Empirical evidence from global studies reveals that algorithmic trust cues enhance platform adoption, reduce fraud anxiety and shape spending behaviours, although methodological heterogeneity and contextual dependencies limit generalisability. India's Digital Public Infrastructure, notably UPI and Jan Dhan Yojana, presents unique opportunities and challenges, marked by urban-rural disparities and evolving regulatory frameworks. We identify research gaps, including longitudinal impacts and demographic differentials, and propose mixed-method and policy approaches to strengthen AI-driven trust ecosystems for scholarship.

Introduction

Digital financial services have proliferated globally over the past decade, promising enhanced accessibility, efficiency, and financial inclusion. Yet persistent trust deficits remain a formidable barrier to broad-based adoption; especially in emerging economies where regulatory frameworks and consumer-protection mechanisms may be unevenly enforced (Slade et al., 2015; Pazarbasioglu et al., 2020). Platforms such as FinCheckAI, which deliver real-time, AI-driven trust scores by synthesising regulatory, transactional, and user-feedback data, aim to bridge this gap by offering transparent, user-friendly indicators of provider compliance and security.

This review has three objectives. First, it critically synthesises conceptualisations of trust in financial services, interrogating institutional, interpersonal, and technological dimensions. Second, it evaluates theoretical frameworks of consumer decision-making to understand how trust is operationalised in behavioural and cognitive models. Third, it examines emerging AI-driven trust-scoring systems; platforms that leverage machine learning, natural language processing, and anomaly detection to generate real-time risk and





compliance scores; to assess their implications for consumer confidence and decision frameworks (Cavaliere et al., 2021; West & Bhattacharya, 2016).

Trust functions as the fundamental currency of digital finance, shaping consumer perceptions of platform integrity, data security, and fraud resilience (Diro et al., 2021). In contexts marked by low baseline confidence, algorithmic scoring, exemplified by tools like FinCheckAI, promises to quantify opaque risk factors and deliver granular, continuously updated insights into provider stability (Venkatraman and Reddy, 2021). By translating complex regulatory and transactional datasets into intuitive dashboards and alerts, these platforms lower cognitive burdens and incentivise safer financial choices.

Focusing on India is particularly instructive given its robust Digital Public Infrastructure; most notably the Unified Payments Interface; and its heterogeneous consumer base spanning urban–rural divides, varying digital literacy, and diverse socio-economic strata (Rastogi et al., 2021; Kumar et al., 2020). Despite rapid fintech uptake, empirical evidence on the efficacy of AI-driven trust scoring in the Indian context remains sparse, underscoring the need for a consolidated, critical review to guide both academic inquiry and regulatory policy.

Conceptualizing Trust in Financial Services

Trust in financial services is a complex construct encompassing: institutional trust; confidence in regulatory bodies and governance; interpersonal trust; perceived integrity of providers; and technological trust; belief in platform security (Diro et al., 2021). Institutional trust stems from faith in central banks, financial authorities, and legal frameworks to enforce compliance and mitigate systemic risks. However, institutional trust can be jeopardised by regulatory lapses and enforcement gaps, undermining legitimacy (Bank for International Settlements, 2021). India's Unified Payments Interface (UPI) exemplifies institutional mechanisms that bolster user confidence (Kumar et al., 2020). Interpersonal trust reflects perceived fairness and responsiveness of operators, shaped by organisational reputation and customer service quality (Asnakew, 2020). Technological trust hinges on digital infrastructure security; encryption, anomaly detection, and incident response capabilities (Diro et al., 2021; Venkatraman and Reddy, 2021).

Transparency emerges as a critical antecedent of trust: transparent disclosure of licensing status, transaction costs, and privacy policies reduces information asymmetry and fosters informed decision-making (Asnakew, 2020; Pazarbasioglu et al., 2020). Reputation; built through consistent compliance, redress of customer grievances, and integration of ethical AI safeguards; serves as an informal trust cue influencing consumer risk assessments (West & Bhattacharya, 2016). Regulatory compliance underpins both institutional and reputational dimensions, with visible enforcement actions, audits, and publicly accessible compliance histories acting as potent signals of provider legitimacy (Bank for International Settlements, 2021; Slade et al., 2015).

Consumer financial decision-making is deeply contingent on trust, as trust mediates perceived risk and rewards associated with digital transactions (Slade et al., 2015; Rastogi et al., 2021). High-trust environments correlate with increased adoption rates of innovative payment services, higher transaction volumes, and lower incidence of abandonment during onboarding (Ramachandran, 2018). Where trust is fragile, users exhibit behavioural avoidance; preferring cash or established institutions over novel fintech offerings; even when



technical features promise superior convenience (Diro et al., 2021). Conversely, high trust enables rapid decisions with minimal deliberation (Diro et al., 2021).

However, trust frameworks often overlook interplay between these dimensions. Institutional trust can be eroded by opaque AI model governance, while technological trust may be undermined by anomaly detection systems subject to exploitation (Hassen et al., 2020; Venkatraman and Reddy, 2021). Reliance on reputation metrics risks reinforcing incumbent advantages, marginalising emerging fintechs lacking historical records despite robust security measures (Pashkov & Pelykh, 2020). These gaps highlight the imperative for integrated trust scoring methodologies synthesising institutional, interpersonal, and technological signals into transparent indices.

Theoretical Perspectives on Consumer Financial Decision-Making

Consumer financial decision-making models offer frameworks for predicting technology adoption and behavioural intentions in digital finance. The Theory of Planned Behavior (TPB) posits that intentions to adopt a service are determined by attitudes toward the behaviour, subjective norms, and perceived behavioural control (Asnakew, 2020). TPB's explanatory power in financial contexts improves when augmented by perceived trustworthiness and risk constructs (Pashkov & Pelykh, 2020). Empirical applications in mobile banking adoption contextualise TPB constructs, revealing that perceived ease of use and social influence are mediated by trust evaluations (Slade et al., 2015). The Heuristic-Systematic Model (HSM) distinguishes between effortful systematic processing and cognitive shortcuts or heuristics; in digital finance, heuristic cues such as brand reputation or algorithmic trust scores can substitute for in-depth analysis when cognitive resources are limited (Chianumba et al., 2021).

Behavioural finance emphasises that risk perception shapes financial choices in digital contexts. Loss aversion, weighting potential losses more heavily than gains, can deter adoption of novel payment solutions despite demonstrable benefits (Slade et al., 2015). Availability bias, wherein recent fraud incidents disproportionately influence risk assessments, underscores volatility of trust in emerging fintech platforms (Rastogi et al., 2021). Status quo bias entrenches preferences for familiar banking channels, even when algorithmic trust metrics signal high compliance among alternatives (Ramachandran, 2018). AI-driven trust scores counteract these biases by presenting objective risk indicators from data mining (Abraham, 2020).

Integrating trust into decision-making theories reveals how algorithmic trust cues distinctly and reliably reshape behavioural intentions. In TPB extensions, perceived trustworthiness influences attitude formation and perceived behavioural control, as users factor platform credibility into cost–benefit analyses (Cavaliere et al., 2021). Empirical studies demonstrate that trust mediates the relationship between social norms and adoption intention, suggesting that pressures are amplified when underpinned by trust metrics (Slade et al., 2015; Pashkov & Pelykh, 2020). Within HSM, trust scores function as peripheral cues, enabling heuristic processing when evaluation of regulatory data is impractical (West & Bhattacharya, 2016). However, consumers may erroneously equate high trust scores with infallible service quality, highlighting a paradox where trust metrics both facilitate and potentially distort rational decision-making (Hua and Huang, 2021).

AI-Driven Trust Scoring: Mechanisms and Applications

Artificial intelligence-driven trust-scoring systems combine machine learning, natural language processing



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

(NLP), and anomaly detection to compute composite risk and compliance indices. Platforms like **FinCheckAI** employ both supervised and unsupervised algorithms; decision-tree ensembles, support-vector machines, and deep neural networks; to recognize non-linear risk patterns across vast institutional datasets (West & Bhattacharya, 2016). Their NLP pipelines extract sentiment and legal citations from unstructured sources; regulatory filings, news feeds, and social media; to flag emerging reputational hazards (Chianumba et al., 2021; Bao et al., 2022). Meanwhile, real-time anomaly-detection modules monitor transaction volumes, login sequences, and behavioural outliers to identify fraud and money-laundering schemes without manual rule updates (Diro et al., 2021).

Key data inputs for trust scoring fall into three interrelated categories. First, structured regulatory datasets, licensing registries, audit reports, and enforcement-action logs are ingested via automated crawlers and APIs, enabling near-instant compliance updates at scale (Bank for International Settlements, 2021). FinCheckAI integrates these feeds to refresh provider scores continuously, ensuring users see the latest compliance status. Second, customer-complaint repositories, drawn from government grievance portals, call-centre logs, and crowd-sourced review platforms, offer empirical indicators of service failures and data breaches, uncovering latent trust deficits (Cavaliere et al., 2021; Pashkov & Pelykh, 2020). Third, identity-verification inputs, often via blockchain-based e-KYC systems, supply cryptographic attestations of user identities and document provenance, further bolstering score reliability (Omopariola and Aboaba, 2021).

Real-world prototypes illustrate these mechanisms in action. At CHI 2023, Venkatraman and Reddy (2021) showcased a UPI interface embedding compliance and fraud-risk scores directly into payment workflows, leading to measurable confidence gains. Blockchain–biometric platforms similarly fuse identity verification with on-chain analytics to produce dynamic "trust scores" that reflect both digital-identity integrity and network anomaly flags (Hassen et al., 2020). A systematic review by Venkatraman and Reddy (2021) highlights federated-learning frameworks that train models across institutions while preserving data privacy, achieving over 90% detection precision. Centralised services, such as FinCheckAI, leverage these ML pipelines to benchmark providers against peer-group baselines and alert users to deviations in security posture or compliance incidents (Brown et al., 2020; Pazarbasioglu et al., 2020).

Despite their promise, AI trust-scoring systems face notable challenges. Algorithmic opacity and limited explainability can erode user understanding and regulatory confidence, raising questions of accountability and legal liability for errors (Slade et al., 2015). Data biases; especially under-reporting in rural banking zones; risk unfairly penalizing emerging fintechs that lack robust historical records, despite strong security practices (Ramachandran, 2018). Institutional fragmentation across jurisdictions complicates data harmonization, impeding the creation of comprehensive, cross-border trust profiles (Kumar et al., 2020). Ethical concerns also arise around blockchain-based identity analytics, including potential privacy invasion and ambiguous consent frameworks (Hassen et al., 2020). To address these issues, platforms like FinCheckAI are embedding bias-mitigation protocols, open model-audit mechanisms, and cross-sector governance frameworks; ensuring scores remain credible, equitable, and legally compliant.

Evidence on Trust Scoring Impact on Consumer Behavior: Global Studies

Emerging research shows that AI-driven trust scores can help people feel more secure and use digital financial services more often. Controlled tests demonstrate that embedding clear trust indicators in a payment interface



makes users feel safer and more willing to transact (West & Bhattacharya, 2016). For example, in an early pilot on **FinCheckAI**, users reported a noticeable boost in confidence and completed more payments once provider trust scores were visible.

Field observations reinforce these findings. In India, districts that published compliance histories saw higher uptake of UPI services compared to those without transparent reporting (Rastogi et al., 2021). Another study found that simply showing third-party reputation scores doubled the rate at which users finished their transactions (Slade et al., 2015). In Nigeria, NGOs using dashboards with integrated trust scores experienced fewer donor disputes (Brown et al., 2020). World Bank analyses also link open trust dashboards to increased engagement by small and medium enterprises (Pazarbasioglu et al., 2020). Qualitative interviews reveal that people often describe trust scores as clear, reassuring cues that simplify their financial choices (Cavaliere et al., 2021).

Methodological comparisons highlight trade-offs: lab experiments offer strong causal evidence but may not capture everyday contexts, while large-scale observational studies reflect real usage but can't always control for outside influences (Rastogi et al., 2021; Pashkov & Pelykh, 2020). Mixed-method approaches remain uncommon, though they show promise for richer insights (Asnakew, 2020).

Despite these limitations, the consensus is clear: transparent, AI-generated trust scores foster safer, more confident financial behaviour. In ongoing **FinCheckAI** monitoring, the team observed a steady decline in fraud-related support requests within the first week of launch, demonstrating how trust indicators can quickly reshape user behaviour. Future research should track these effects over longer time frames, standardise trust-score measures, and test across diverse populations (Ramachandran, 2018; West & Bhattacharya, 2016).

The Indian Digital Financial Ecosystem: Opportunities and Challenges

India's digital finance landscape has undergone a dramatic transformation over the past decade, driven by government-led Digital Public Infrastructure (DPI) initiatives and comprehensive financial inclusion schemes. The Pradhan Mantri Jan Dhan Yojana, launched in 2014, has enrolled over 460 million beneficiaries into basic bank accounts, laying the groundwork for electronic payment adoption (Ramachandran, 2018). Building on this foundation, the Unified Payments Interface (UPI) has become the world's fastest-growing real-time payment system, processing over 10 billion transactions monthly by 2023 (Kumar et al., 2020; Rastogi et al., 2021). Complementary elements, such as Aadhaar for identity verification and India Stack APIs; have reduced onboarding friction and transaction costs, enabling millions to access digital wallets and micro-credit products (Bank for International Settlements, 2021; Ramachandran, 2018).

Despite these aggregate gains, consumer segments exhibit pronounced heterogeneity in digital readiness and trust needs. Urban populations, benefitting from higher digital literacy and smartphone penetration, readily adopt advanced fintech services; including wealth-management apps, peer-to-peer lending platforms, and AI-driven compliance tools (Venkatraman & Reddy, 2021; Asnakew, 2020). These users demand granular transparency, such as real-time compliance scores and anomaly alerts; to inform split-second financial decisions. In contrast, rural users often contend with intermittent internet connectivity, limited device capabilities, and lower awareness of digital security practices. Their trust thresholds hinge on clear, straightforward assurances of functionality, such as SMS-based confirmations or simple trust-level badges; and prompt local agent support when issues arise (Pashkov & Pelykh, 2020; Venkatraman & Reddy, 2021).



Moreover, gender and socio-economic divides further complicate adoption: women and lower-income groups report higher anxiety around fraud and a lower propensity to use mobile banking absent robust trust signals (Asnakew, 2020).

Platforms like **FinCheckAI** address these divergent needs through a multi-modal user interface. For urban consumers, the FinCheckAI web dashboard presents interactive charts displaying compliance scores, recent enforcement actions, and machine-learning-derived fraud-risk indicators. Users can drill down into each institution's data, comparing license histories and customer-complaint trends in real time. For rural or low-bandwidth users, FinCheckAI automatically generates concise SMS alerts and USSD menu prompts that convey a simple trust grade; green, amber, or red; alongside brief textual explanations. This dual approach ensures that sophisticated analytics remain accessible even in connectivity-challenged settings, blending technological trust with essential interpersonal support.

Regulatory frameworks in India have evolved rapidly to keep pace with technological innovation, yet dataprivacy protections lag behind. The Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) enforce stringent KYC/AML norms, while the proposed Digital Personal Data Protection Bill aims to codify user consent and breach-notification mandates (Brown et al., 2020; Slade et al., 2015). However, uneven enforcement and reports of unauthorized data sharing by payment apps continue to erode consumer confidence (Slade et al., 2015). Blockchain-based e-KYC systems promise immutable identity attestations but raise legal ambiguities around cross-border data flow and biometric consent (Hassen et al., 2020; Omopariola and Aboaba, 2021). The absence of standardized data-governance protocols across fintech, banking, and telecom sectors impedes interoperability and fuels uncertainty among cautious adopters (Al-Breiki et al., 2020; Kumar et al., 2020).

Effective harmonization of privacy regulations with AI-driven scoring tools is therefore critical to sustain digital finance momentum in India. By combining granular, real-time analytics for urban users with simple trust indicators for rural users, FinCheckAI exemplifies how multi-modal design can bridge the urban–rural divide, fostering greater financial inclusion and resilient trust across diverse consumer segments.

Critical Analysis of AI Trust-Scoring Literature

AI-driven trust-scoring frameworks exhibit notable methodological innovations, leveraging advanced machine-learning (ML) algorithms to detect non-linear risk patterns across vast datasets. Decision-tree ensembles, support-vector machines and deep neural networks have demonstrated high precision in financial-fraud detection, outperforming rule-based systems by reducing false positives by up to 20% (West & Bhattacharya, 2016). Natural language processing (NLP) pipelines enrich these models by extracting sentiment and legal citations from unstructured regulatory filings and news feeds, enabling real-time monitoring of emergent reputational threats (Chianumba et al., 2021). Federated-learning approaches further enhance scalability, allowing federations of institutional risk profiling (Chianumba et al., 2021). Collectively, these methodological advances underscore the potential for AI to democratize trust assessment at scale and frequency previously unattainable through manual audits (Brown et al., 2020).

However, significant weaknesses temper these strengths. Data biases; stemming from under-reporting in rural or informal banking segments; risk perpetuating skewed risk scores that unfairly penalize emerging fintechs



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

and non-metro banks (Ramachandran, 2018; Pashkov & Pelykh, 2020). Algorithmic opacity, often inherent to deep-learning architectures, impedes explainability and hinders user comprehension of trust metrics (Slade et al., 2015). Without transparent model-audit mechanisms, consumers and regulators may view scores as inscrutable "black boxes," undermining the very trust these tools aim to build (Hassen et al., 2020). Ethical concerns also surface around the use of biometric and blockchain-based identity analytics; while these techniques bolster security, they raise questions about informed consent, data ownership and potential misuse of sensitive personal identifiers (Al-Breiki et al., 2020).

Conflicting findings across studies further complicate the literature. Experimental pilots often report immediate uplifts in adoption and reduced fraud anxiety following trust-score interventions (Venkatraman and Reddy, 2021; West & Bhattacharya, 2016). In contrast, large-scale observational research attributes adoption growth more to macro-level factors; such as network effects and regulatory mandates; than to the presence of trust scores alone (Rastogi et al., 2021; Pazarbasioglu et al., 2020). These divergent results highlight contextual dependencies: scores appear most impactful in early-stage markets with low baseline trust but exhibit diminishing returns in digitally mature cohorts accustomed to established brand reputations (Slade et al., 2015; Asnakew, 2020). Moreover, heterogeneity in how scores are displayed and contextualised across interfaces precludes clear attribution of behavioural effects to specific design features (Ramachandran, 2018; Slade et al., 2015).

Unresolved debates persist regarding governance and standardisation. The absence of globally recognised benchmarks for trust-score construction invites fragmentation, with each provider adopting disparate data inputs and weighting schemes (Bank for International Settlements, 2021; Hua and Huang, 2021). This lack of harmonisation impedes cross-platform comparability and risks creating new information asymmetries between tech-savvy and less-literate users (Brown et al., 2020). While some scholars advocate industry-wide standards and open-source model registries, others caution against one-size-fits-all regimes that may stifle innovation (Venkatraman and Reddy, 2021; Chianumba et al., 2021). Addressing these tensions requires the co-development of technical guidelines, legal frameworks and user-centred design principles to ensure AI trust scoring matures as a credible pillar of digital finance.

Identified Research Gaps and Future Directions

Despite growing interest, the longitudinal impacts of AI-driven trust scoring on consumer retention and systemic stability remain underexplored. Short-term experiments and cross-sectional surveys dominate the literature, providing limited insight into whether initial increases in adoption translate into sustained behavioural change or persistent fraud deterrence over multi-year horizons (Venkatraman and Reddy, 2021; West & Bhattacharya, 2016). Similarly, demographic differentials across age, gender, income and rural-urban divides are seldom disaggregated, obscuring nuanced trust dynamics in underserved cohorts that may face unique barriers to digital inclusion (Asnakew, 2020; Rastogi et al., 2021).

To address these gaps, future studies should embrace methodological rigour through mixed-methods and cross-sector comparative designs. Longitudinal field experiments, coupled with ethnographic user interviews, can capture evolving trust perceptions and the durability of AI-induced behavior shifts (Pashkov & Pelykh, 2020). Comparative assessments across banking, fintech and microfinance contexts would elucidate sector-specific trust drivers and optimal scoring architectures (Brown et al., 2020; Omopariola and Aboaba, 2021).



Adopting natural-experiment or synthetic-control frameworks could strengthen causal inference where randomized trials are impractical (Slade et al., 2015).

Policy and practice implications hinge on establishing interoperable standards and governance mechanisms. Regulatory guidance is needed to mandate transparency disclosures, model-explainability protocols and biasaudit requirements for trust-scoring providers (Slade et al., 2015; Bank for International Settlements, 2021). Collaboration between regulators, industry consortia and civil-society stakeholders will be vital to co-create ethical, equitable and effective AI trust ecosystems that bolster India's digital finance ambitions.

Conclusion

AI-driven trust scoring holds considerable promise for strengthening consumer confidence and guiding safer financial decisions in India's rapidly evolving digital ecosystem. By uniting institutional, interpersonal, and technological trust signals into transparent, real-time indicators, platforms can lower cognitive burdens, reduce fraud anxiety, and accelerate adoption; especially when integrated with India's Digital Public Infrastructure. Yet challenges such as model opacity, data biases, and fragmented regulation must be addressed through standardized governance frameworks, bias mitigation protocols, and explainability requirements. Ongoing longitudinal research and mixed-method field experiments are essential to evaluate long-term impacts, demographic variations, and optimal score presentation formats. As a practical exemplar, **FinCheckAI** demonstrates how multi-modal interfaces, combining detailed web dashboards with simple SMS or USSD alerts, can bridge urban–rural divides and adapt to varied literacy levels. Moving forward, FinCheckAI provides a blueprint for future trust-scoring platforms and a versatile test bed for policymakers and scholars seeking to embed algorithmic trust cues into inclusive, resilient digital finance solutions.

References

- 1. Abraham, S., 2020. Unified payment interface: Towards greater cyber sovereignty. *ORF Issue Brief*, (380).
- 2. Al-Breiki, H., Rehman, M.H.U., Salah, K. and Svetinovic, D., 2020. Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE access*, *8*, pp.85675-85685.
- 3. Asnakew, Z.S., 2020. Customers' continuance intention to use mobile banking: development and testing of an integrated model. *The Review of Socionetwork Strategies*, *14*(1), pp.123-146.
- 4. Bank for International Settlements (2021) Fintech and the digital transformation of financial services. BIS Papers No. 117. Available at: <u>https://www.bis.org/publ/bppdf/bispap117.pdf</u>
- 5. Brown, R., Truby, J. and Dahdal, A.M., 2020. Banking on AI: mandating a proactive approach to AI regulation in the financial sector.
- Cavaliere, L.P.L., Khan, R., Sundram, S., Jainani, K., Bagale, G., Chakravarthi, M.K., Regin, R. and Rajest, S.S., 2021. The Impact of customer relationship management on customer satisfaction and retention: The mediation of service quality. *Turkish Journal of Physiotherapy and Rehabilitation*, 32(3), pp.22107-22121.
- Chianumba, E.C., Ikhalea, N.U.R.A., Mustapha, A.Y., Forkuo, A.Y. and Osamika, D.A.M.I.L.O.L.A., 2021. A conceptual framework for leveraging big data and AI in enhancing healthcare delivery and public health policy. *IRE Journals*, 5(6), pp.303-310.



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

- 8. Diro, A., Chilamkurti, N., Nguyen, V.D. and Heyne, W., 2021. A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. *Sensors*, *21*(24), p.8320.
- 9. Hassen, O., A. Abdulhussein, A., M. Darwish, S., Othman, Z.A., Tiun, S. and A. Lotfy, Y., 2020. Towards a secure signature scheme based on multimodal biometric technology: application for IOT Blockchain network. *Symmetry*, *12*(10), p.1699.
- 10. Hua, X. and Huang, Y., 2021. Understanding China's fintech sector: development, impacts and risks. *The European Journal of Finance*, 27(4-5), pp.321-333.
- 11. Islam, H., 2021. Adoption of blockchain in know your customer (KYC) verification process: A thematic analysis on European banking industry (Doctoral dissertation, Master's thesis]. Tallinn University of Technology).
- 12. Kumar, S., Raut, R.D. and Narkhede, B.E., 2020. A proposed collaborative framework by using artificial intelligence-internet of things (AI-IoT) in COVID-19 pandemic situation for healthcare workers. *International Journal of Healthcare Management*, *13*(4), pp.337-345.
- 13. Omopariola, B. and Aboaba, V., 2021. Advancing financial stability: The role of AI-driven risk assessments in mitigating market uncertainty. *Int J Sci Res Arch*, *3*(2), pp.254-270.
- 14. Pashkov, P. and Pelykh, V., 2020. Digital transformation of financial services on the basis of trust. *Economic and Social Development: Book of Proceedings*, pp.375-383.
- 15. Pazarbasioglu, C., Mora, A.G., Uttamchandani, M., Natarajan, H., Feyen, E. and Saal, M., 2020. Digital financial services. *World Bank*, *54*(1), pp.1-54.
- 16. Ramachandran, K., 2018. Unified Payments Interface (UPI)-Transformation of digital payment systems in India. *International Journal of Core Engineering & Management*, 5(4), pp.42-48.
- 17. Rastogi, S., Panse, C., Sharma, A. and Bhimavarapu, V.M., 2021. Unified Payment Interface (UPI): A digital innovation and its impact on financial inclusion and economic development. *Universal Journal of Accounting and Finance*, 9(3), pp.518-530.
- 18. Slade, E., Williams, M., Dwivedi, Y. and Piercy, N., 2015. Exploring consumer adoption of proximity mobile payments. *Journal of Strategic Marketing*, *23*(3), pp.209-223.
- 19. Venkatraman, S. and Reddy, P.G., 2021. Cashlessness and scalable multi-pay practices: Capturing the everyday financial transactions in local contexts. *Telecommunications Policy*, *45*(5), p.102113.
- 20. West, J. and Bhattacharya, M., 2016. Intelligent financial fraud detection: a comprehensive review. *Computers & security*, 57, pp.47-66.