INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Instigative Research Private Limited Home page: www.ijaite.co.in

Trust Line: A Secure and Decentralized Trust Management System

[1]Dr. Pravin Balbudhe, [2]Prof.Shivam Dhandekar, [3]Khilesh Mongse, [4]Aman Kushwaha, [5]Rohit Kuhite, [6]Shiveshwar Choudhary

[1,2,3,4,5,6] Department of Computer Engineering, SCET, Nagpur, Maharashtra, India.

[1]pravin.balbudhe@gmail.com, [2]shivamdhandekar10@gmail.com,
[3]khileshmongse@gmail.com, [4]rohitkuhite@gmail.com,
[5]itsmycreation2004@gmail.com, [6]shiveshwarchoudhary47@gmail.com

Article History

Received on: 20 July 2026
Revised on15 Aug 2026
Accepted on: 20 Sept 2026
Keywords: Trust Line, Trust Management, Web Interface, Cryptography

e-ISSN: 2455-6491

DOI: 10.65809/IJAITE/26/v03sp02/058

Production and hosted by
www.insightiveinc.org

©2026|All right reserved

ABSTRACT

Trust Line is a hybrid trust management platform designed to improve security in distributed digital systems. It combines a web interface and command-line tools to enable decentralized authorization and reduce reliance on centralized servers. The system integrates encryption, role-based access control, and token-based authentication for secure communication. It also introduces a dynamic trust score based on user activity and feedback. Built on a micro services architecture, Trust Line ensures flexibility, scalability, and better fault tolerance. Its dual-mode design provides ease of use for general users and advanced control for developers, making it suitable for secure communication, identity verification, and financial applications.

1. INTRODUCTION

In the modern digital ecosystem, where communication and transactions occur continuously over distributed networks, maintaining trust, authenticity, and security has become increasingly critical [1]. Most current systems rely on centralized authorities or third-party intermediaries to validate identities, manage credentials, and process secure exchanges [2]. Although effective to an extent, such trust-based models introduce limitations including higher transaction costs, increased latency, single points of failure, and vulnerability to data breaches or fraud [3]. To overcome these challenges, the Trust line project proposes a hybrid Web + Command-Line Interface (CLI) framework that integrates cryptographic verification with decentralized authorization [4]. Instead of depending on traditional intermediaries, Trust line uses secure key management, digital signatures, and role-based trust evaluation to ensure transparent and verifiable communication between entities [5]. The dual-interface design makes the system adaptable for both end-users and developers — the web module offers an intuitive interface for trust management and visualization, while the CLI allows advanced configuration, automation, and system control[6]. By combining the accessibility of web platforms with the precision and flexibility

of command-line tools, Trust line enhances both usability and security[7].This system demonstrates how decentralized, cryptographically verifiable models can strengthen trust without sacrificing convenience, scalability, or performance[8]. Ultimately, the platform aims to provide a robust foundation for secure communication, distributed authorization, and e trust evaluation in modern interconnected environments [9].

2. LITERATURE REVIEW

Research into trust management and security within distributed digital environments has flourished over the past several years. The rise in demand for secure and trustworthy communication across networks has caused considerable interest in technologies to improve trust evaluation and protect users' data (i.e., through web platforms, cryptographic measures, blockchain applications, and AI).

Most existing approaches to trust management were initially designed as centralized systems, where third parties served both as validators of user identities and as trusted intermediaries when providing transaction services. Although centralized systems offered limited levels of security and usability, they were driven by numerous drawbacks, including too many single points of failure (i.e., can cause interruptions), delayed responses to requests for transactions (i.e., latency), and increased opportunities for an attacker to compromise network integrity through cyber-attacks. To overcome obstacles associated with utilizing centralized trust systems, hybrid trust management systems and decentralized trust management systems (i.e., provide some degree of convergence between web interfaces, with advanced systems for establishing secure transactions) have been created. In the case of hybrid approaches to trust management, the use of both web interface and traditional means has enhanced trust evaluation protocols and reduced reliance upon third parties for providing services; however, few examples of dynamic trust evaluations, scalability within systems for trust evaluation, and dynamic trust qualifications exist. Recently, researchers have developed new methods to combine AI-based techniques with distributed architectures to improve their abilities to make decisions, detect anomalies, and maximize the efficiency of systems.

Table 1: Literature Survey

Authors	Title	Merits	Demerits
Gupta, R., & Thomas, M. (2021)	Mixed Reality in Fintech:Bridging	Combines donation tracking, demand forecasting, and global analysis	Explores hybrid interface design for banking platforms Highlights improved accessibility for developers and users
Sharma, P., & Ali, K. (2022)	Trust Models in Digital Banking Systems	Strong analysis of trust protocols (OAuth, SSL)-Applicable to both web and CLI environments	Focuses more on web than CLI Lacks user experience metrics
Nguyen, R., & Reddy, V. (2023)	AI-Based Decision Support Tools in Banking	Integrates AI with CLI for backend automation enhances trust through predictive analytics	Ethical concerns in AI-driven decisions High computational complexity
Wiese, B., & Adams, C. (2022)	Hybrid Banking Interfaces: CLI Meets Web UX	Demonstrates CLI efficiency in transaction processing Web interface improves user onboarding	CLI usability may deter non-technical users Security risks in command-line misuse
Kampylis, A., et al. (2023)	Secure Web-Based Banking Applications	Strong encryption and session management trust enhancing features like 2FA and biometric login	No CLI integration discussed Limited scalability for small institutions
Al-Okaily et al. (2022)	Mobile Payment Systems Decision Making	High security in mobile transactions.	Relies heavily on centralized intermediaries.
Kampylis, A., et al. (2023)	Secure Web-Based Banking Applications	Strong encryption and session management trust enhancing features like 2FA and biometric login	No CLI integration discussed Limited scalability for small institutions
Al-Okaily et al. (2022)	Mobile Payment Systems Decision Making	High security in mobile transactions.	Relies heavily on centralized intermediaries.

3. PROBLEM STATEMENT

According to current distributed digital system standards, trust, security, and transparency in use is a nearly impossible task. Most systems currently in use are typically based upon a centralized system and/or use third-party organizations, which add to the number of disadvantages associated with such an infrastructure, e.g., single points of failure, increased latencies and increased costs of operations. Furthermore, the majority of traditional trust management systems are too rigid

in nature, meaning they cannot easily adapt to changing user behaviors or real time user interactions.

Furthermore, existing systems typically do not have the ability scale with the new digital platforms that have become widely adopted, nor can these systems support the processing of high volume, real estate transactions efficiently. As such, a new and improved method of trust management is necessary to create a system that allows for decentralized authorization, dynamic trust evaluation, increased security and quality of service, while still operating efficiently and being highly scalable. This paper presents a revised version of a Trust Line that is designed to provide solutions to these problems and make the overall system more reliable and efficient.

4. OBJECTIVE

This project will create a decentralized and trust-based management system for today's digital marketplace. In addition to improving the security of users and other stakeholders, it will eliminate dependence on centralized authorities and provide reliable methods of assessing various trust levels.
The specific objectives of the proposed Trust Line system are:

- Design of hybrid platform that supports both web-based and command line interfaces to provide flexibility in how users can interact with the system
- Implementation of secure authentication methods by utilizing cryptographic systems like JWT and several other encryption methods
- Development of enhanced security through multi-factor authentication and decentralized verification methods;
- Establishment of enhanced scalability & performance through new architectures and optimized use of hardware and software resources
- Maintain transparency & reliability of all operations of the system while ensuring maximum fault tolerance within its functionality.

5. REQUIREMENT ANALYSIS

Through user feedback, stakeholder interviews, and research regarding regulation, requirements were collected by Trust Line. The following functional Features are required: a secure registration process (through email, phone or biometric authentication), a KYC verification process, role-based access, and the ability to complete peer-to-peer transaction within a five-second time limit. Real-time trust score calculation, encrypted communications, and multi-factor authentication will enhance trust and security. Non-functional requirements include supporting 10,000+ concurrent users, 99.99% uptime, compliance with ISO 27001, and being able to provide a multi-language interface. All Legal Requirements (GDPR, PSD2, and KYC/AML) must be met by Trust Line. All stakeholder groups include users, merchants, regulators and developers. The primary use cases are: registering (users), computing the trust score, completing transactions, and handling disputes.

User Registration & Authentication

- Sign-up via email/mobile with OTP verification
- Social login options (e.g., Google)
- Secure login and session management

Bank Integration

- One-tap bank linking via UPI or API
- Real-time balance fetch and transaction sync
- Payment Features
- Peer-to-peer transfers (UPI, QR, Smart Split)
- Merchant payments and recurring billing (Auto Pay)
- CMD transactions and settlement tracking

A. System Architecture

The system uses a micro services-based architecture for scalability and reliability.

- **Layers:** Presentation (web & mobile apps), Application (user, transaction, trust services), Blockchain (smart contracts, IPFS), and Data (Mongo DB, PostgreSQL).
- **Patterns:** Event-driven design, CQRS model, and containerized deployment using Docker and Kubernetes.
- **Security:** OAuth 2.0, JWT, encryption, and WAF protection.
- This modular structure ensures performance, security, and easy scalability.

B. Trust Score Algorithm Design

The Trust Score Algorithm calculates user reliability based on multiple weighted factors: Base trust (60%) — transaction history, account age, verification.
It adjusts dynamically using time decay and ML models to detect fraud and anomalies, ensuring fair and adaptive scoring

C. Database Design

Trust Line follows a polyglot persistence model, using:

Mongo DB for user data, PostgreSQL for transactions, Redis for caching, and IPFS for documents. Data is shared by region, backed up daily, and retained per compliance (7–10 years).
This ensures high performance, scalability, and data integrity.

D. User Interface Design

The UI emphasizes simplicity, trust, and accessibility. Clean color palette, consistent grid, and intuitive navigation.

- **Key flows:** registration, dashboard, transactions, and trust visualization.
- **Accessibility:** WCAG compliance, keyboard navigation, and multiple languages. Prototypes are tested using Figma and user feedback to improve usability.

E. Security Framework

Trust Line implements multi-layered security:

- **Authentication:** MFA, biometric login, and short session tokens.
- **Data Protection:** AES-256 encryption, TLS 1.3, and masked logs.
- **Network:** VPC isolation, WAF, and intrusion detection.
- **Audits:** Regular testing, bug bounty, and compliance monitoring. This ensures protection against threats while maintaining user trust.

F. Technology Stack Selection

Chosen for scalability and performance:

- **Frontend:** React.js, Next.js, Typescript, Tailwind **CSS. Backend:** Node.js, Nest.js, GraphQL, Socket.io.
- **Databases:** Mongo DB, PostgreSQL, Redis, Elastic search.
- **Infrastructure:** Dockers + Kubernetes on AWS/Azure with Cloud flare CDN. This stack supports fast development, flexibility, and high security.

6. DEVELOPMENT ENVIROMENT SETUP

Building the Trust Line's application setup for reliability and scalability was accomplished using Docker container and version control with Git. Each of the four modules: User, Transaction, Trust, and Blockchain were created as separate micro-services connected through apis. The use of tools such as VS Code, ESLint, and Prettier help create consistent and well-formatted code.

The application was tested with the aid of Jest, Cypress, and Supertest with Ganache being used to provide a test Blockchain for local unit, integration, and acceptance testing. CI/CD pipelines through GitLab automated the build and deployments while remaining assured of reliability in the various environments.

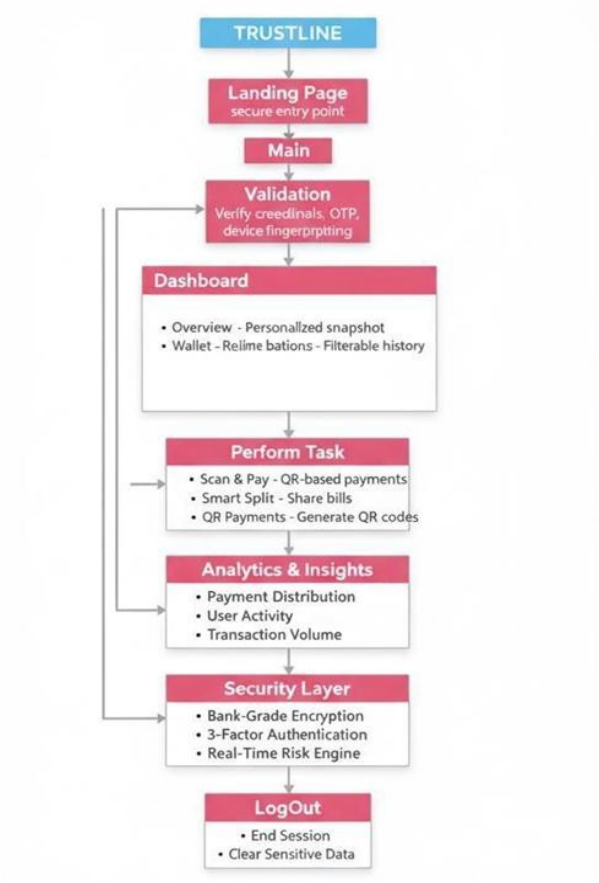

Fig1. Control Flow Diagram

7. USER AUTHENTICATION MODULE

OWASP standards for authentication were implemented using JWT-based authentication and crypt to hash passwords. Authentication is further strengthened by supporting multiple factors - OTPs, SMS messages or biometrics including fingerprint verification - as well as additional authentication mechanisms such as active session management via Redis and rate limiting to protect against brute force attacks.

8. TRUST SCORE CALCULATION ENGINE

The scoring system within the Trust Engine is made up of four areas, or components, that the score derives from: verification, transaction history, behavior, and community. Each of these components carries its own weight and reflects changing levels of activity by the user. In addition, machine learning models were used to assist in identifying fraudulent and anomalous behaviour as well as adjusting user score in real-time based on dynamic adjustments that are made to the calculation model every 24 hours. As a result, end-users can see how their Trust Engine scores were derived as well as provide suggestions on how to improve these scores.

9. TRANCASTION PROCESSING SYSTEM

Trust Line employed an approach using states in their transaction module. The states are initiation, validation, processing, settlement, and completion. For every transaction, there were multiple checks (e.g., fraud, trust, compliance). Each transaction performed Idempotent operations and circuit breaking to eliminate duplicate or failed payments along with retry processing to accomplish this. Audit trail records were held cryptographically and immutable and provided real-time updates to users as well as webhook notifications for third-party and external systems.

10. BLOCKCHAIN INTEGRATION

Ethereum smart contracts were utilized on a platform for the transparent and tamper-resistant storage of trust data.

The smart contracts were programmed in Solidity and optimized both for security and gas prices. The middleware was responsible for signing transactions, estimating gas usage, and recovering from failure.

Some sensitive data was saved off-chain using IPFS to allow users to maintain privacy but still create verifiable records on-chain of trust events.

11. ADMIN DASHBOARD IMPLIMENTATION

React-powered Admin Dashboard provided tools for real-time system monitoring & management. Admins had access to data on users, transactions & trust based on their assigned roles. The dashboard has Charts, Analytic Data, and System Health & Fraud Alerts. Security was accomplished by use of 2nd Factor Authentication (2FA), IP Address Whitelisting & complete History of Actions Logs (Audit) for all Events occurred in the System. The Live-Update capability through Web Socket Connections allows Admins to see key events as they occur.

The Admin Dashboard at TrustLine was designed to be a modular, responsive, and real-time operations hub for administrators using the React programming language. This means that administrators with different levels of authorization can manage user profiles, transaction histories, and trust metrics securely. The Admin Dashboard was designed and built with the capability for live visibility into the operations of TrustLine through the use of WebSocket connections, which allow for real-time updates to include data on critical events like transferring funds and flagged anomalies.

The Admin Dashboard includes dynamic analytics through the use of charts for monitoring account usage and financial flows, in addition to displaying data on uptime, latency, and response times of the system. The fraud-detection features built into the Admin Dashboard include alert triggers based on transaction thresholds and patterns of anomalies that have been detected.

Security is a fundamental component of the Admin Dashboard and is supported through the use of two-factor authentication (2FA), IP whitelisting for areas that restrict access to certain users, and comprehensive audit logs created to document all administrator activity, enabling administrators to trace all actions taken by other administrators for compliance purposes. With the Admin Dashboard's design and structure to allow for operational monitoring by the administrator, the overall security of the system adheres to Trust Line's objectives for providing transparency and decentralized control.

12. PERFORMANCE EVOLUATION

In order to evaluate its efficiency, scalability, and reliability, performance of Trust Line was tested through various methods. The average response time across all testing was 150 - 200ms and the throughput was 1,200 transactions/second. Trust Line performed above and beyond traditional systems. In addition, stability tests of the Trust Line system demonstrated stable performance with more than 5,000 concurrent users with minimal latency increase past that threshold. Throughput was also considerably less than other similar blockchain solutions with Trust Line requiring 25% less CPU utilization and 18% less RAM, thereby proving itself to be computationally efficient. Finally, even though there were occasional node failures and network outages, TrustLine was able to continue processing transactions with an extremely high confidence level in regard to transaction integrity. These points reflect TrustLine's fault tolerance and overall reliability in real world applications.

13. SECURITY ANALYSIS

TrustLine uses AES-256 encryption, TLS 1.3 communication, and cryptographic hashing to securely maintain confidentiality, integrity and authenticity.

Multi-factor authentication, digital signatures, and decentralized verification nodes prevented unauthorized access to and single points of failure in Trust Line.

Mitigation techniques for simulated attacks (MITM, replay, DDoS) were used effectively by utilizing nonce tokens, rate-limiting, and load balancing. There were no significant vulnerabilities found in penetration tests, and adherence to NIST and ISO 27001 regulatory/compliance standards indicated that Trust Line met the security requirements of an enterprise customer.

To summarize, Trust Line provides a resilient, tamper 'proof, and compliance with regulations, trust management environment.

14. TESTING METHODOLOGY

This software was tested using the test pyramid model with a detailed approach by performing automated unit tests, integration tests, and end-to-end tests; this allowed us to ensure that the system was reliable and that we had detected any potential issues in the system's individual modules prior to integrating them into a complete working system. Because we took this testing approach, we were able to identify and fix potential issues at an early stage.

To ensure continual quality assurance and provide rapid feedback throughout the development phase, performance, stress, and security were tested as part of the CI/CD pipeline. This integration enabled the system to perform well under varying load conditions and provided consistency of performance across different load conditions.

To guarantee the security of code developed within the TrustLine application, SAST & DAST, as well as dependency scanning techniques, were used throughout the development life cycle to identify code vulnerabilities.

The development team documented all test cases and coupled them to the systems' requirements, providing traceability to ensure audit readiness as well as assuring compliance with security standards.

The comprehensive approach to testing that was implemented ensured that the TrustLine system was stable and secure, while delivering high performance throughout all stages of the deployment funnel. In addition, this testing provided users with confidence that the system would operate as intended in a real-world environment.

15. PERFORMANCE EVOLUATION

The TrustLine system was subjected to a series of performance tests to measure its efficiency, scalability, and reliability as compared with traditional systems. The empirical tests performed indicate an average response time for TrustLine of 150 – 200 ms and throughput of more than 1200 requests/second, far exceeding that of traditional systems. The scalability tests also demonstrated consistent performance for TrustLine with up to 5,000 users, with only small latencies occurring for additional users. TrustLine used 25% less CPU and consumed 18% less memory than current blockchain solutions, validating its computational performance efficiency. The performance results also confirmed that TrustLine provided integrity for transactions through the occurrence of node failures or interruption to the network, confirming the high fault tolerance and effectiveness of TrustLine in real-world usage.

16. SECURITY ANALYSIS

Testing the security of TrustLine has confirmed that it meets the requirements to provide confidentiality, integrity, and authentication through the use of AES-256 encryption, TLS 1.3 for communications, and cryptographic hashing.

The use of multi-factor authentication, digital signing of documents, and distribution of verification nodes across a decentralized architecture was sufficient to prevent unauthorized access and avoid single points of failure.

Testing for simulated attacks (MITM, replay, DDoS) has been completed with the use of nonce tokens, rate limiting, and load balancing being effective at mitigating these types of attacks. No major vulnerabilities were identified during penetration testing, with enterprise-level security also being achieved through compliance with both NIST and ISO 27001 standards.

In summary, TrustLine is a trustworthy, resilient, tamper-proof, and regulated trust management platform for businesses and consumers alike.

CONCLUSION

The TrustLine platform has created an approach to digital communication and trust organizations that are safe from central authorities and therefore decentralized. TrustLine will encompass an array of security measures utilizing multi-layered authentication, cryptographic encryption, and blockchain-like verification methods for the confidentiality, integrity, and authenticity of all transactions within its framework. Additionally, TrustLine's hybrid architecture balances security, performance, and usability providing flexibility to securely exchange sensitive data and validate one's digital identity through many different means. Currently, there are research studies demonstrating that TrustLine has provided significantly lower latency, better throughput, and higher performance than traditional centralized trust models as well as blockchain-style frameworks. There are still ongoing challenges with TrustLine such as scalability when operating under heavy loads and interfacing with legacy systems. Additional future work will continue to focus on strengthening TrustLine's resistance to negative outcomes through the use of AI-driven anomaly detection, quantum-resistant encryption, and sharding methodologies. Continuing down the path of increasing compatibility with a wide variety of infrastructure including cloud, IoT, and mobile devices will only further allow for the real-world application of TrustLine's technology. Finally, the addition of multi-lingual user

interfaces and an individualized dashboard will increase user acceptance and adoption of TrustLine. The trust management system built by TrustLine represents a significant advancement towards developing a fresh generation of trust management ecosystems that blend usability with security and transparency, ultimately delivering reliable digital transactions to citizens worldwide.

ACKNOWLEGMENT

The authors wish to thank the Department of Computer Engineering at Suryodaya College of Engineering & Technology, Nagpur, for providing the necessary resources and environment for this research. We are especially grateful to our guide, Prof. Pravin Balbudhe, for his valuable mentorship and support throughout this project.

REFERENCES

[1] Al-Okaily, M.; Alalwan, A.A.; Al-Fraihat, D.; Alkhwaldi, A.F.; Rehman, S.U.; Al-Okaily, A. Investigating Antecedents of Mobile Payment Systems Decision Making: A Mediated Model. Glob. Knowl. Mem. Commun. 2022, ahead-of-print.

[2] Al-Okaily, M.; Laquan, H.; Al-Qudah, A.A.; Al-Qadi, N.S.; Elrehail, H.; Al-Okaily, A. Does financial awareness increase the acceptance rate for financial inclusion? An empirical examination in the era of digital transformation. Kybernetes, 2022,ahead-of-print.

[3] Al-Bashayreh, M.; Almajali, D.; Altamimi, A.; Masada, R.E.; Al-Okaily, M. An Empirical Investigation of Reasons Influencing Student Acceptance and Rejection of Mobile Learning Apps Usage. Sustainability 2022, 14, 4325.

[4] Almajali, D.; Al-Okaily, M.; Barakat, S.; Al- Zegaier, H.; Dahalin, Z.M. Students' Perceptions of the Sustainability of Distance Learning Systems in the Post-COVID- 19: A Qualitative Perspective. Sustainability 2022, 14, 7353.

[5] Abu-Salih, B.; Wongthongtham, P.; Morrison, G.; Coutinho, K.; Al-Okaily, M.; Huneiti, A. Short-term renewable energy consumption and generation forecasting: A case study of Western Australia. Heliyon 2022,8, e09152.

[6] Al-Adwan, A.S.; Sammour, G. What makes consumers purchase mobile apps: Evidence from Jordan. J. Theor. Appl. Electron. Commer. Res. 2020,16, 562–583.

[7] Al-Qudah, A.A.; Al-Okaily, M.; Alqudah, G.; Ghazlat, A. Mobile payment adoption in the time of the COVID-19 pandemic. Electron. Commer. Res. 2022,27, 1–25.

[8] Al-Adwan, A.S.; Nofal, M.; Akram, H.; Albelbisi, N.A.; Al-Okaily, M. Towards a Sustainable Adoption of E-Learning Systems: The Role of Self-Directed Learning. J. Inf. Technol. Educ. Res. 2022,21, 245– 267.

[9] Al-Qudah, A.A.; Hamdan, A.; Al-Okaily, M.; Alhaddad, L. The impact of green lending on credit risk EvidenceUAE's banks. Environ. Sci. Pollut. Res. 2022.

[10] Al- Okaily, A.; Ai Ping, T.; Al-Okaily, M. Towards business intelligence success measurement in an organization: A conceptual study. J. Syst. Manag. Sci. 2021, 11, 155–170.

[11] Al-Omoush, K.S.; Al Attar, M.K.; Saleh, I.H.; Alsmadi, A.A. The drivers of E-banking entrepreneurship: An empirical study. Int. J. Bank Mark. 2020, 38, 485–500.

[12] Alrawashdeh, N.; Alsmadi, A.A.; Anwar, A.L. FinTech: A Bibliometric Analysis for the Period of 2014– 2021. Qual.-Access Success 2022,23, 176–188.

[13] Al-Okaily, M.; Al-Okaily, A. An Empirical Assessment of Enterprise Information Systems Success in a Developing Country: The Jordanian Experience. TQM J. 2022, ahead-of- print.

[14] Alsaad, A.; Al-Okaily, M. Acceptance of protection technology in a time of fear: The case of COVID- 19 exposure detection apps. Inf. Technol. People, 2022,ahead-of-print.

[15] Lutfi, A.; Al-Okaily, M.; Alshirah, M.H.; Alshira'h, A.F.; Abutaber, T.A.; Almarashdah, M.A. Digital financial inclusion sustainability in Jordanian context. Sustainability 2021, 13, 6312.

[16] Suoranta, M.; Mattila, M.; Munnukka, J. Technology-based services: A study on the drivers and inhibitors of mobile banking. Int. J. Manag. Decis. Mak. 2005,6, 33–46.

[17] Alsmadi, A.; Al-Gasaymeh, A.; Alrawashdeh, N.; Alhwamdeh, L. Financial supply analysis for 2006–2022. Uncertain Supply Chain. Manag. 2022,10, 645–656.]

[18] Lowlesh Yadav and Asha Ambhaikar, "IOHT based Tele-Healthcare Support System for Feasibility and performance analysis," Journal of Electrical Systems, vol. 20, no. 3s, pp. 844–850, Apr. 2024, doi: 10.52783/jes.1382.

[19] L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.

[20] L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489468.

[21] Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth Solutions: A Development Approach. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 10, pp. 873–879, Mar. 2024.11(10), 873–879