Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.15, No.2, 2025, pp.45-50

DOI: https://doi.org/10.51983/ijiss-2025.IJISS.15.2.07

Evaluation Metrics for User Trust in Information Systems

Ramee RiadHwsein[1], S. Jeyachandran[2], Dr.R. Satish[3], Muhidinov Ayubbek Nuritdinovich[4], Dr.P. Sundara Bala Murugan[5] and Dr. Atul Dattatraya Ghate[6]

[1]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq
[2]Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India
[3]Associate Professor, Department of Management Studies, St. Joseph's College of Engineering, OMR, Chennai, Tamil Nadu, India
[4]Faculty of Business Adminstration, Turan International University, Namangan, Uzbekistan
[5]Associate Professor, Department of Management Studies, St. Josephs Institute of Technology, OMR, Chennai, Tamil Nadu, India
[6]Professor, Department of Management, Kalinga University, Raipur, India
E-mail: [1]tech.iu.comp.ramy_riad@iunajaf.edu.iq, [2]gpmek@ametuniv.ac.in, [3]dr.satishsjit@gmail.com, [4]ayubbek1988@gmail.com, [5]sundarabalamurugan@gmail.com, [6]ku.atuldattatrayaghate@kalingauniversity.ac.in
ORCID: [1]https://orcid.org/0009-0009-2098-651X, [2]https://orcid.org/0009-0007-8881-0911, [3]https://orcid.org/0000-0002-3104-6429, [4]https://orcid.org/0009-0008-1295-5978, [5]https://orcid.org/0009-0002-7440-0181, [6]https://orcid.org/0009-0009-0869-2957
(Received 14 February 2025; Revised 27 March 2025, Accepted 08 April 2025; Available online 25 June 2025)

Abstract - **User Information Systems (ISs) Trust has emerged as a central indicator of system adoption, continuance of use, and user satisfaction on the system itself. Trust is bounding with user's digital activities from participating in various e-commerce activities, healthcare, e-governance and much more. Gaining the ability and flexibility to measure and evaluate user trust is of high importance. This paper aims to present a particular set of evaluation criteria that are captured in a comprehensive framework which is trust in information systems. Different aspects of trust are shaped by the reliability and durability of the system, the user's belief of the system's skill to deliver intended results, usability, security, transparency and the general level of the system competence. The literature is rife with gaps as there is no single uniform parameter defined to measure trust which makes comparison ineffective and strategy refinement inconsistent.**

This research proposes a classification of trust evaluation that separates objective from subjective measurement criteria. Measuring ISs Trust objectivity can be evaluated by system uptime, response time, data accuracy and frequency of security incidents. Subjective measurement could range from user responses, satisfaction surveys, evaluation of user behaviors or actions, as well as emotional expression to their responses capturing emotional behaviors. Other measurements discussed here involve trust and sentiment analysis, predictive trust modeling and behavioral based evaluation which are increasingly being adapted to describe real world trust environments. Moreover, the paper investigates trust shaping in the scenario of context factors like user experience, expectational elements endemic to the domain and culture.

This research develops structured trust metrics which provide practitioners and researchers with effective design, evaluation, and enhancement approaches for information systems. As the paper ends, the author suggests a domain-agnostic trust evaluation model that retains adaptability across various technologies while ensuring systems and governance are centered around the users.

Keywords: **User Trust, Evaluation Metrics, Information Systems, Usability, Reliability, Security, Trust Assessment**

I. INTRODUCTION

User trust in information systems captures the readiness of a user to depend on the functionality, security, and integrity of a system while performing tasks or even making decisions without full control or comprehensive knowledge (Moreau & Sinclair, 2024). Trust is significant for acceptance, participation, and continuous interaction across myriad platforms such as commercial e-commerce portals, cloud-based services, healthcare portals, and financial services (Pragadeswaran et al., 2024). Trust is essential for system impact and effectiveness in the rapidly evolving technological environment of today's digital economy, particularly concerning automation technology and sophisticated information systems where user understanding is superficial (McKnight & Chervany, 2001; Corritore et al., 2003; Mayer et al., 1995).

Monitoring user trust evaluation is necessary because user confidence as a construct impacts user satisfaction, system uptake, and dependability of the service provider. With strong user trust, positive outcomes such as increased usage, personal data disclosure, and advocacy through word-of-mouth praises is likely to happen (Hlushenkova et al., 2024; Hariprasath et al., 2022). Absence of trust on the other hand often leads to system rejection, user anger, and damage to organizational reputation (Tandon & Thakur, 2025). Trust is heavily subjective and intricate in nature and yet, so

important in user systems which makes it difficult to assess and evaluate uniformly across multiple industries, systems and domains (Gefen et al., 2003; Söllner et al., 2016).

This document seeks to fill in the gaps by suggesting a systematic method of assessing user trust with measurable and context-specific parameters (Vincentelli & Schaumont, 2025). In doing so, the research advances the literature focused on improving the design and management of systems that are trustworthy (Pillai & Panigrahi, 2024).

Key contribution

- In a systematic analysis of more than a dozen trust measures—both objective (e.g. uptime, security incident rates) and subjective (e.g. satisfaction surveys, behavioral intention)—we highlight gaps, inconsistencies, as well as domain-specific biases that impede cross-study comparability.
- Formally grounded in theory and previous works, we suggest Trustworthiness (system integrity and competence level), Reliability (consistency and performance stability), and Transparency (clarity of operations and data, including handling) as the foundational metrics for a unified system trust assessment framework.
- We provide e-commerce, healthcare, and finance as examples of fields where practitioners can apply our guidelines and measurement frameworks, trusting that they will contextually surpass cultural expectations and user experience sensitivities while ensuring trust assessments are sophisticated.

This document contains five main parts. In Section I: Introduction, the importance of the concept of user trust in information systems is defined, alongside evaluating trust, as a critical factor for system adoption and user satisfaction. This section also sets the objectives of the research and outlines the key milestones of the study. Section II: Literature Review investigates prior scholarly investigations focusing on trust in information systems, analyzing evaluation methods applied in prior studies, and identifying gaps in existing metrics. Such a critical assessment provides a rationale for setting new criteria for evaluation. Section III: Proposed Evaluation Metrics classifies three principal components—trustworthiness, reliability, and transparency— as the primary metrics for user trust evaluation. For each metric, a discussion is presented on its definition, importance, and practical quantification methods. Section IV: Result and Discussion evaluates the consequences of applying the proposed metrics, any identified limitations to the framework, and provides suggestions for future work aimed at enhancing the evaluated framework. Finally, Section V: Conclusion highlights the key findings of the study, highlights the importance of evaluating user trust in systems and puts forward a recommendation for the incorporation of these metrics into the information system design and management processes to enable the creation of more trustful environments.

II. Literature Review

A user's trust in information systems has received attention in human-computer interaction, information security, and system design (Sato et al., 2019; Dorofte & Krein, 2024). Initial studies viewed trust as a user's psychological state concerning expectations about system reliability and trustworthiness (McKnight & Chervany, 2002). With the progression of digital systems, trust started to include components such as protective measures, privacy policies, and system agility (James et al., 2025). Numerous factors have been identified as influencing trust, such as perceived competence, dependability, and the user's prior experiences with a system (Pavlou, 2003).

Different approaches have been designed to measure user trust (Wu, 2024). Subjective evaluation techniques include surveys and interviews through which users express their attitudes and emotions, while objective grading evaluates performance metrics such as uptime, errors, delay, and breaches of security (Wang & Emurian, 2005; Tsai & Jing, 2025). Some studies have considered behavioral measures of trust indirect indicators such as session length, return frequency, and click rates (Bimal & Dhamala, 2024). These measures are often non-standardized and difficult to apply across different contexts (Leu, 2011).

Regardless of the contributions, a current trust evaluation framework, sequentially, suffers from several limitations (Al-Jame & Al-Fares, 2025). Primarily, some user-centered trust frameworks measure user perception of trust without incorporating system evaluation metrics and performance data; this leads to an incomplete evaluation. Secondly, the lack of standardized metrics makes it impossible to evaluate and measure the trust across diverse systems or platforms (Söllner et al., 2016). Finally, various cultural and contextual determinants of trust are frequently ignored, which produces models that are not necessarily global in scope (Belanger et al., 2002).

III. Proposed Method

Trust in an information system's functionality requires an approach that entwines a user's subjective views alongside objective system performance data. To meet this need, we outline a composite approach that integrates Trustworthiness, Reliability, and Transparency. Such an approach seeks to capture the user's trust via a single metric while balancing the emotional and technical factors that affect trust. The process begins with the collection of user opinion data and system log data which undergoes computation for each of the individual metric scores before culminating in a total trust score. The goal is empowered decision-making and system refinements. The approach is adaptable and flexible for different users and system interactions because of the collection of disparate data sources toward trust score computation. In addition, the

approach facilitates the active monitoring of trust shifts over extended periods. As a result, system designers and administrators are granted the means to diagnose trust issues and apply trust-centered solutions effectively.

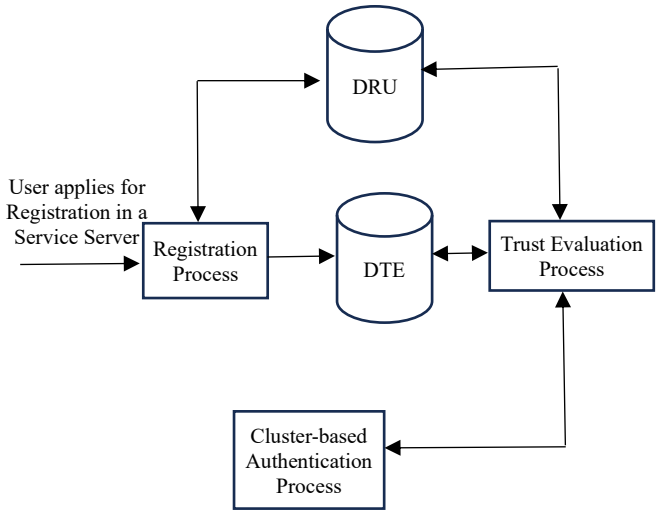

Fig. 1 Flowchart of the User Trust Evaluation Process

Fig. 1 shows a simplified flow diagram depicting a user trust evaluation process in and information system. The figure starts from the user registering a service. At this point, the user begins interacting with the system. The steps commence with the User Registration request. This request initiates the Registration Process, which performs two key functions; it verifies user credentials as well as captures details of the user. These processes involve two important data stores, the DTE (Data Trust Engine) and the DRU (Data Registration Unit). The DTE stores data that relate to trusting the user which is important for the trust evaluation, while the DRU keeps registration and user specific data. Trust Evaluation Process fetches these data stores after user registration to check how trustworthy a user is based on trust data. Lastly, the flowchart includes a Clustered Based Authentication Process where users are authenticated based on grouping similarity of trust profiles assigned to them for verification with their profiles. The feedback loop between trust evaluation and cluster based authentication emphasizes the ever-changing nature of trust management.

The evaluation framework proposes a system based algorithmic approach. As a starting step, subjective data is collected through surveys to measure user trust perception regarding competence and the security of the system. Concurrently, objective data such as system uptime, error rates, and frequency of failures, are collected for measuring reliability. Privacy and transparency are measured in terms of how effectively the system communicates the underlying data and privacy policy. Every metric is normalized and assigned a value based on the system context. A trust score is calculated via a weighted average approach based on the metrics added, proving evaluation in various domains while maintaining consistency.

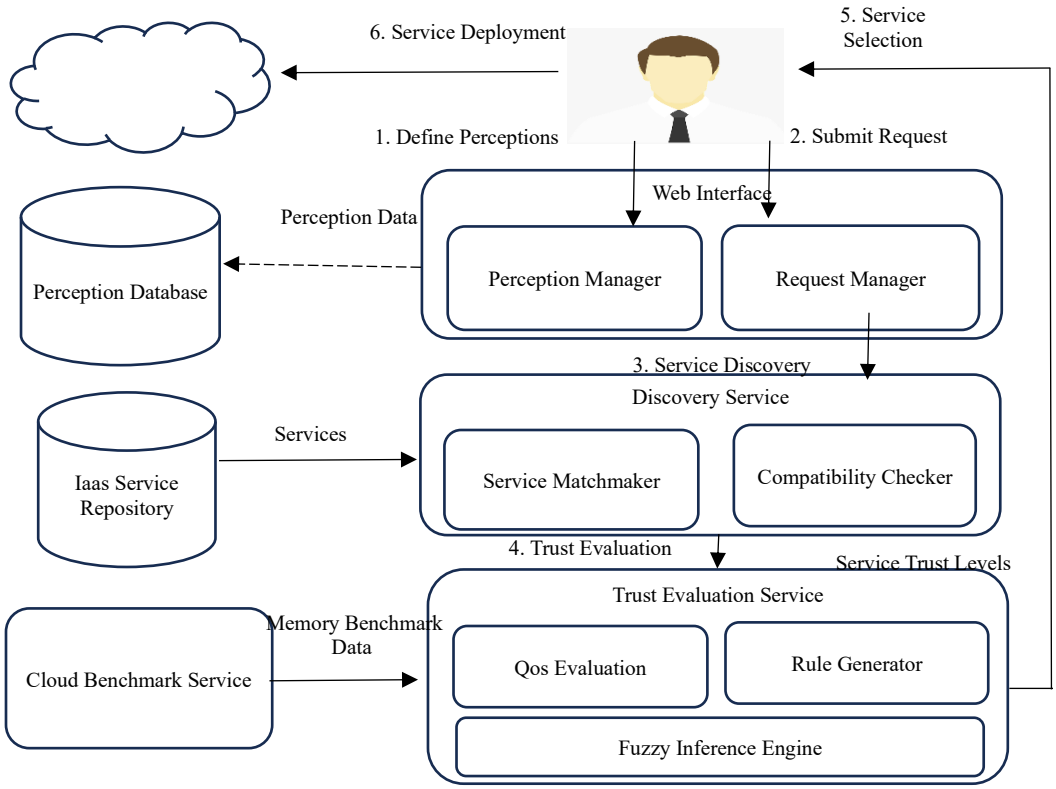

Fig. 2 Architecture Diagram of the User Trust Evaluation System

Fig. 2 provides an overview of the architectural structure directed towards evaluating user trust within a cloud-based information system environment. Per the user interface, users articulate their trust requirements and submit requests on the

Web Interface using two modules as workflows, which are the Perception Manager and the Request Manager. The Perception Manager fetches and computes perception data held in the Perception Database that captures subjective insights from users concerning trust. The request module engages with the Discovery Service where certain components like the Service Matchmaker and Compatibility Checker fetch, Service Matchmaker and Compatibility Checker, identify adequate and compatible services regarding user requests. The Trust Evaluation Service, a hidden subsystem within the architecture, is pivotal and is further divided into parts: the QoS Evaluator which determines service quality parameters, the Rule Generator which produces trust rules, and a Fuzzy Inference Engine which applies fuzzy logic to trust evaluation. Also, the Cloud Benchmark Service supplies trust scoring enhanced by historical benchmark data, therefore trust score computation becomes reliable. With the layered architecture, the cloud system fulfills the trust assessment needs that are qualitative and quantitative which enables adaptive deployment of services and increases reliance by users on the system.

Mathematically, the User Trust Score is formulated as:

$$UTS = w_1 \times T_r + w_2 \times R_l + w_3 \times T_p$$

where T_r represents Trustworthiness, R_l denotes Reliability, and T_p indicates Transparency. The weights w_1 , w_2, and w_3 sum to one, reflecting their relative importance. Trustworthiness is calculated as the average normalized user survey score. Reliability combines normalized measures of uptime, error rate, and downtime frequency with their respective weights. Transparency is computed as the average score of data disclosure clarity, privacy policy clarity, and user control clarity. This formula encapsulates both qualitative and quantitative dimensions of trust, providing a robust, adaptable, and interpretable metric to guide system design and trust management.

IV. Result and Discussion

Evaluating user trust through the proposed metrics—Trustworthiness, Reliability, and Transparency—offered users' perception of information systems and their interaction with information systems. Understanding trust dynamics was made possible using the consolidated trust score which captured subjective user feedback to system data. Initial findings suggest strong positive correlation between confidence and higher transparency while reliability affects long-term trust retention. Sustainability of trust was dominated by transparency. These results support the claim testifying to the need for sophisticated evaluation approaches that encompass more than mere user feedback in their assessment of multiple user metrics.

Additionally, the detection of trust shifts over time for users was accurately captured through the designed method, which is beneficial to system administrators focused on boosting user experience and performance. Aspects needing improvement such as enhanced communication regarding system updates or increased system uptime can be better managed through the trust assessment methodology which, coupled with ongoing data monitoring and assessment, highlights precision optimally. The perception of trust and demographic differences were some of the subjective limitations identified suggesting tailored approaches to user-centric trust models.

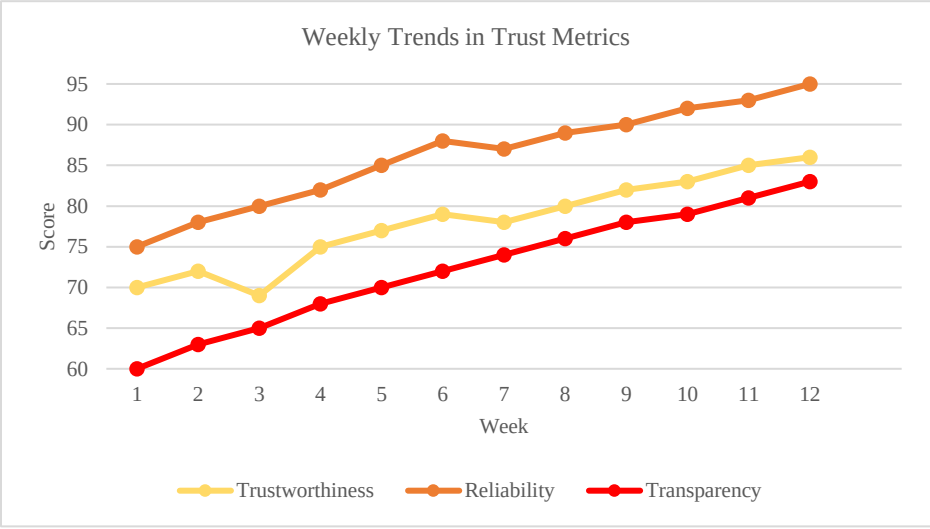

Fig. 3 Weekly Trends in Trust Metrics

Fig. 3 represents Trustworthiness, Reliability, and Transparency user trust metrics as a line graph over 12 weeks. It shows steadily growing user trust across all three parameters, depicting improvement as the system develops. Trustworthiness starts at 70, moderate to user expectations, and increases to 86 by Week 12. This change demonstrates rising user confidence regarding the system's integrity and ethical conduct. Reliability improves from 75 to 95 and portrays the system's enhanced technical stability, uptime, and overall consistent performance fat Reliability. Transparency begins at the lowest value of 60 but rises steadily to 83, indicating the system's gradual increase in

openness and communicativeness. Converging metrics at later weeks demonstrate users controlled development in all trust dimensions which is important for user retention and satisfaction over time.

TABLE I STATISTICAL OVERVIEW AND CORRELATIONS

Metric	Average Score	Standard Deviation	Correlation with User Satisfaction
Trustworthiness	78	6.5	0.82
Reliability	85	5.2	0.89
Transparency	72	7.1	0.76
Overall Trust	78.3	5.9	0.88

Table I encapsulates the comprehensive statistical report of the three principal metrics of trust Trustworthiness, Reliability and Transparency as well as the aggregate User Trust Score (UTS). It shows the average values, standard deviation, and correlation coefficient of each metric with overall user satisfaction. Reliability recorded the highest average score of 85 and also exhibited the strongest positive correlation (0.89) with user satisfaction. This indicates that system stability and consistent performance has the greatest impact on trust. Trustworthiness follows with an average of 78 and strongly correlates at 0.82, which indicates the growing user confidence regarding the ethical conduct and credibility of the system. Transparency, though recording the lowest average score of 72, still boasts a respectable correlational score of 0.76 and indicates the role it plays in the formation of trust. Users may hold disparate views owing to inconsistent communication and system opacity that muddle their understanding. The standard deviation figures show that Transparency (7.1) has the highest lack of consistency with regard to user specific accounts of how the system is openly and clearly displayed to the user. In contrast, Reliability (4.2) shows the least variation which suggests dominant positive experiences across respondents. The User Trust Score (UTS) which was calculated using a weighted formula is 78.3 which is consistent with the satisfaction metrics.

V. CONCLUSION

In the successful adoption and continual utilization of information systems, user trust is a fundamental pillar. As systems increasingly integrate into everyday life, and especially in sensitive areas such as healthcare, finance, and governance, the understanding and assessment of trust requires a distinctly user-centered approach. This paper Proposed Trustworthy, Reliable, and Transparent metrics Multi-metric Evaluation Framework to offer a methodical and measurable approach to user trust which is structured in nature. These metrics were chosen due to their dual relevance in psychological and technical domains which is critical in capturing the comprehensive perception and interaction of users with digital systems.

The analysis and the graphics support the findings which explain how trust metrics change over time and differ for users on different levels. We introduced the User Trust Score (UTS) which synthesizes core indicators into a single value, aiding system enhancements as well as decision making by other stakeholders. In addition, the data emphasizes that improvement of the system's reliability and the transparency of the communication have a notable positive influence on the user trust. On the other hand, trust is flexible and situation specific. Hence, this model should be extended with adaptive and context-sensitive variables like equity, tailoring, and safeguarding for context-variables to improve the model for the next steps. If trust assessment is treated as a continuous process, it will be possible for the developers to have the systems designed in a way that they would operate as intended and at the same time, meet the ethical and emotional expectations of the users.

REFERENCES

[1] Al-Jame, F., & Al-Fares, R. A. (2025). Integrating Circular Economy Principles into Strategic Management Practices. *International Academic Journal of Innovative Research, 12*(1), 25–30. https://doi.org/10.71086/IAJIR/V12I1/IAJIR1205

[2] Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3–4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

[3] Bimal, & Dhamala, K. (2024). Pharmacist-Delivered Interventions on Pain Management: Review and Cluster-Randomized Trial. *Clinical Journal for Medicine, Health and Pharmacy, 2*(4), 11-20.

[4] Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies, 58*(6), 737–758. https://doi.org/10.1016/S1071-5819(03)00041-7

[5] Dorofte, M., & Krein, K. (2024). Novel approaches in AI processing systems for their better reliability and function. *International Journal of Communication and Computer Technologies, 12*(2), 21-30. https://doi.org/10.31838/IJCCTS/12.02.03

[6] Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90. https://doi.org/10.2307/30036519

[7] Hariprasath, S., Senthilkumar, P., & Singaravel, G. (2022). Artificial Intelligence in Medicine Application and its Security Process A Review Methodology. *International Journal of Advances in Engineering and Emerging Technology, 13*(2), 193–197.

[8] Hlushenkova, A., Kalinin, O., Navrozova, Y., Navolokina, A., Shcherbyna, V., & Doroshenko, T. (2024). Management of Strategies for Shaping the Innovative and Investment Potential of Enterprises as a Factor Ensuring Their Economic Security. *Indian Journal of Information Sources and Services, 14*(3), 16–22. https://doi.org/10.51983/ijiss-2024.14.3.03

[9] James, C., Michael, A., & Harrison, W. (2025). Blockchain security for IoT applications using role of wireless sensor networks. *Journal of Wireless Sensor Networks and IoT, 2*(2), 58-65.

[10] Leu, F.Y. (2011). Guest Editorial: Emerging Security Technologies and Applications. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*(3),1-3.

[11] Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

[12] McKnight, D. H., & Chervany, N. L. (2001, January). Conceptualizing trust: A typology and e-commerce customer relationships model. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences* (pp. 10-pp). IEEE. https://doi.org/10.1109/HICSS.2001.927053

[13] McKnight, D. H., & Chervany, N. L. (2002). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 6*(2), 35–59. https://doi.org/10.1080/10864415.2002.11044235

[14] Moreau, I., & Sinclair, T. (2024). A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics, 2*(4), 30-36.

[15] Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

[16] Pillai, N., & Panigrahi, I. (2024). Global Health Security and SDG 3: Strengthening Pandemic Preparedness through South-south Cooperation. *International Journal of SDG's Prospects and Breakthroughs, 2*(2), 10-13.

[17] Pragadeswaran, S., Subha, N., Varunika, S., Moulishwar, P., Sanjay, R., Karthikeyan, P., Aakash, R., & Vaasavathathaii, E. (2024). Energy Efficient Routing Protocol for Security Analysis Scheme Using Homomorphic Encryption. *Archives for Technical Sciences, 2*(31), 148–158. https://doi.org/10.70102/afts.2024.1631.148

[18] Sato, S., Hirose, S., & Shikata, J. (2019). Sequential Aggregate MACs from Any MACs: Aggregation and Detecting Functionality. *Journal of Internet Services and Information Security, 9*(1), 2-23.

[19] Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems, 25*(3), 274–287. https://doi.org/10.1057/ejis.2015.19

[20] Tandon, B., & Thakur, M. (2025). An Overview of Adaptive Signal Processing Methods for 6G Wireless Communication Networks. *International Academic Journal of Science and Engineering, 12*(1), 12–15. https://doi.org/10.71086/IAJSE/V12I1/IAJSE1203

[21] Tsai, X., & Jing, L. (2025). Hardware-based security for embedded systems: Protection against modern threats. *Journal of Integrated VLSI, Embedded and Computing Technologies, 2*(2), 9–17. https://doi.org/10.31838/JIVCT/02.02.02

[22] Vincentelli, B., & Schaumont, K. R. (2025). A review of security protocols for embedded systems in critical infrastructure. *SCCTS Journal of Embedded Systems Design and Applications, 2*(1), 1–11.

[23] Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior, 21*(1), 105–125. https://doi.org/10.1016/j.chb.2003.11.008

[24] Wu, Z. (2024). Integrating Biotechnology Virtual Labs into Online Education Platforms: Balancing Information Security and Enhanced Learning Experiences. *Natural and Engineering Sciences, 9*(2), 110-124. https://doi.org/10.28978/nesciences.1569211