Journal of Contemporary Science and Technology Management
Volume 02, Issue 02, June 2026

Explainable AI and Managerial Trust: Investigating Transparency in Automated Business Decisions

Nurjonov Izzatbek

Department of Accounting, Mamun University, Khiva, Uzbekistan

Email: nurjanov.izzat@mamunedu.uz

Abstract

Explanations are added to automated business decisions on the assumption that transparency builds managerial trust and that trust improves the use of the decision system. This paper distinguishes trust from calibrated reliance, the acceptance of recommendations when they are correct and rejection when they are wrong, and argues that explanations should be evaluated by their effect on calibration rather than on trust alone. A simulation of 3,000 managerial decisions compares three explanation conditions for a recommender that is correct 75% of the time: no explanation, a faithful explanation whose cues track the recommendation's correctness, and a fluent but unfaithful explanation whose cues do not. Faithful explanations raise appropriate reliance from 63.8% to 73.5% and cut over-reliance from 17.9% to 11.5%. Fluent but unfaithful explanations raise acceptance to 88.9%, the highest of the three, yet raise over-reliance to 22.6%, the worst of the three, while lowering under-reliance. Trust, measured by acceptance, is therefore highest in the condition with the worst decisions. The paper derives criteria for explanation design, namely faithfulness, discriminability and actionability, proposes a measurement protocol based on reliance outcomes, and discusses implications for governance of automated decision systems in business.

Keywords: explainable AI; managerial trust; calibrated reliance; transparency; automated decision-making; over-reliance.

DOI: 10.66592/a1yw58p7

1. Introduction

Automated decision systems recommend or make decisions in credit, pricing, hiring, procurement and operations. Managers who oversee these systems must decide when to accept their outputs and when to override them. Explanations, descriptions of why the system produced a given output, are widely promoted as the means of building the trust that such oversight requires [1], [2]. Regulatory initiatives increasingly require them.

The premise that explanations build trust is well supported; the premise that trust improves decisions is not. Trust that leads a manager to accept recommendations indiscriminately is as harmful as distrust that leads to indiscriminate rejection. The relevant objective is calibrated reliance: accepting recommendations when the system is right and overriding when it is wrong [3], [4]. An explanation improves decisions only if it helps the manager distinguish the two cases.

This distinction matters because explanations can be persuasive without being informative. A fluent narrative attached to a wrong recommendation can increase its acceptance [5]. Explanations that are faithful to the model's reasoning carry cues that correlate with correctness; explanations generated to be convincing may not. This paper formalises the difference, examines it in a simulation with a known ground truth, and derives design and governance criteria.

Journal of Contemporary Science and Technology Management
Volume 02, Issue 02, June 2026

2. Background

2.1 Trust in automation

Lee and See [3] defined trust in automation as the attitude that an agent will help achieve one's goals under uncertainty, and distinguished appropriate trust, matched to the automation's capability, from over-trust and under-trust. Parasuraman and Manzey [6] reviewed automation bias, the tendency to accept automated recommendations without adequate verification. Both literatures imply that the objective of interface design is calibration, not maximal trust.

2.2 Explanation methods

Explanation methods range from inherently interpretable models [7] to post-hoc techniques such as feature attribution [1], [8]. Faithfulness, the degree to which an explanation reflects the model's actual reasoning, varies across methods and is often not validated. An unfaithful explanation may be plausible and fluent while bearing no relation to why the recommendation was produced.

2.3 Explanations and reliance

Empirical studies of human–AI decision-making have found that explanations sometimes improve and sometimes worsen decision accuracy, and that they often increase acceptance regardless of correctness [5]. The mixed findings are consistent with the distinction between faithful and unfaithful explanations: the former supply discriminating cues, the latter only persuasion.

2.4 Transparency in business decision contexts

Business decisions differ from the laboratory tasks on which much explanation research is based. Managers face volume, so verification time per decision is limited; they face accountability, so they need to defend acceptances and overrides to superiors and auditors; and they face asymmetric costs, since a wrongly accepted recommendation often causes a loss while a wrongly rejected one forgoes a gain. Each feature raises the stakes of calibration. Volume makes managers dependent on cues rather than full re-analysis; accountability makes a documented explanation attractive even when it is uninformative, because it provides cover; and cost asymmetry means that explanations which raise acceptance indiscriminately shift the error mix in the costly direction. The model below is designed to make these dynamics visible.

3. Model

A recommender is correct with probability π. For each decision, the manager observes a cue c whose distribution depends on correctness: when the recommendation is correct, $c \sim N(0.7, 0.2^2)$; when incorrect, $c \sim N(0.4, 0.2^2)$. The cue represents whatever the explanation reveals that correlates with correctness, such as the plausibility of the attributed features. The manager accepts the recommendation with probability

$$P(\text{accept} \mid c) = 1 / (1 + \exp(-(\alpha + \beta(c - 0.5))), \quad (1)$$

where α sets the baseline acceptance and β the manager's sensitivity to the cue. Explanation conditions differ in α and β. With no explanation the cue is barely visible (β small, α moderate). A faithful explanation makes the cue salient (β large). A fluent but unfaithful explanation raises baseline acceptance (α large) without making the cue salient (β small). Reliance outcomes are classified as appropriate (accept correct or reject incorrect), over-reliance (accept incorrect) and under-reliance (reject correct).

Journal of Contemporary Science and Technology Management
Volume 02, Issue 02, June 2026

4. Simulation Design

The harness generates 3,000 decisions with $\pi = 0.75$ under each condition. Parameters are $(\alpha, \beta) = (1.0, 0.5)$ for no explanation, (0.5, 6.0) for the faithful explanation and (2.0, 0.3) for the fluent but unfaithful explanation. Acceptance rate, the three reliance outcomes and the discrimination of the acceptance probability with respect to correctness (AUC) are reported. The parameters are design values that encode the hypothesised effects of each explanation type; the harness quantifies their consequences for reliance.

5. Results

5.1 Reliance outcomes

Table 1 and Figure 1 report outcomes. Without explanations, managers accept 74.1% of recommendations, close to the system's accuracy, but because acceptance is barely related to correctness, only 63.8% of decisions reflect appropriate reliance; over- and under-reliance are both near 18%. Faithful explanations raise appropriate reliance to 73.5%, reduce over-reliance to 11.5% and under-reliance to 15.0%, and slightly lower acceptance to 70.8%. Fluent but unfaithful explanations raise acceptance to 88.9%, the highest of the three, and reduce under-reliance to 8.4%, but raise over-reliance to 22.6%, the highest of the three; appropriate reliance (69.0%) lies between the other conditions.

Table 1. Reliance outcomes by explanation condition (3,000 simulated decisions each; recommender accuracy 75%).

Explanation condition	Acceptance rate	Appropriate reliance	Over-reliance	Under-reliance
No explanation	74.1%	63.8%	17.9%	18.3%
Faithful explanation	70.8%	73.5%	11.5%	15.0%
Fluent but unfaithful explanation	88.9%	69.0%	22.6%	8.4%

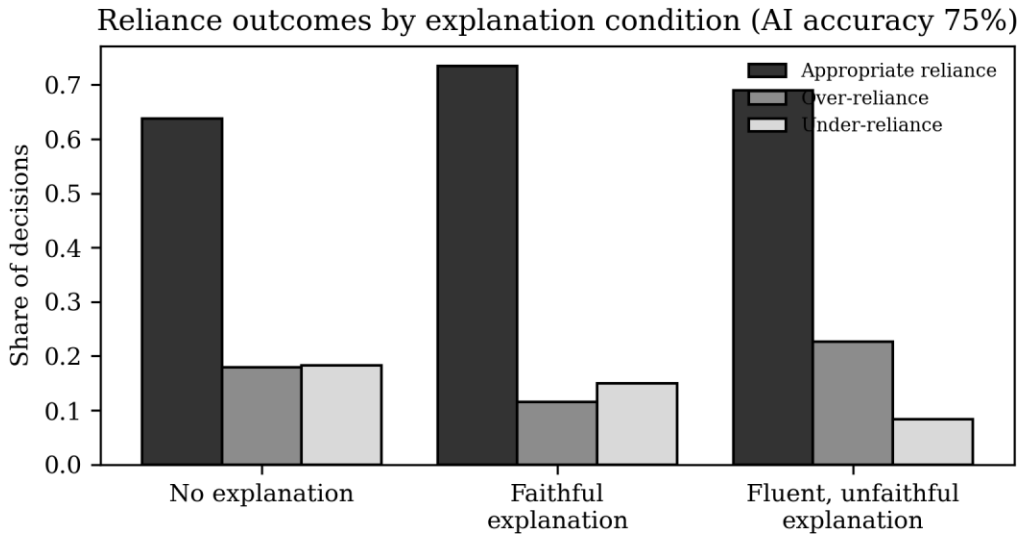

Figure 1. *Appropriate reliance, over-reliance and under-reliance by explanation condition.*

5.2 Trust versus calibration

If trust is measured by acceptance, the fluent but unfaithful explanation builds the most trust. If decisions are measured by reliance outcomes, it produces the most over-reliance, which in business settings is the costlier error: accepting a wrong credit, pricing or procurement decision typically costs more than rejecting a right one. The faithful explanation builds slightly less trust than no explanation at all but produces the best decisions. Trust and decision quality are therefore not aligned across conditions, and evaluation on trust alone would select the wrong design.

5.3 The asymmetry of errors

The unfaithful explanation trades under-reliance for over-reliance almost one for one: under-reliance falls by 9.9 points and over-reliance rises by 4.7 relative to no explanation, for a net gain in appropriate reliance of 5.2 points. Whether this is an improvement depends on the relative cost of the two errors. Where accepting wrong recommendations is more costly, as in most business decisions with asymmetric downside, the unfaithful explanation worsens expected outcomes despite raising appropriate reliance in aggregate.

5.4 Discrimination of the acceptance rule

The AUC of the acceptance probability with respect to correctness is 0.84 with no explanation, 0.87 with the faithful explanation and 0.86 with the unfaithful one. The similarity of the last two values shows that discrimination alone does not capture the difference between conditions: the unfaithful explanation shifts the whole acceptance distribution upward without changing its ordering much, so its harm appears in the over-reliance rate rather than in the AUC. Calibration measures that account for the level of acceptance, not only its ordering, are therefore required when evaluating explanations.

6. Design Criteria for Explanations

Three criteria follow. Faithfulness: the explanation must reflect the model's actual reasoning, so that its cues correlate with correctness; this is a property of the explanation method and should be validated by testing whether explanation features predict errors. Discriminability: the explanation must present cues in a form managers can use to distinguish reliable from unreliable recommendations, for instance by flagging when inputs lie outside the training distribution or when attributions rest on weak features. Actionability: the explanation should indicate what the manager could check or change, which converts a passive narrative into a verification prompt.

A fourth, negative criterion is that explanations should not be optimised for persuasiveness. Fluency and confidence raise acceptance without raising calibration, and an explanation generator rewarded for user acceptance will learn to persuade.

7. Measurement and Governance

7.1 Measuring reliance rather than trust

Organisations deploying automated decisions should log, for each decision, the recommendation, the explanation shown, the manager's action and the eventual outcome. From these logs the four reliance cells in Table 1 can be computed by explanation condition and by manager, and explanation designs can be compared on over-reliance rather than on acceptance or satisfaction surveys.

7.2 Governance implications

Transparency requirements should specify faithfulness, not merely the presence of an explanation. An audit of an automated decision system should include a test of whether its explanations discriminate correct from incorrect outputs. Where explanations are generated by a separate model, as is increasingly common with language-model narratives, the audit should treat the explanation generator as a decision-relevant component subject to the same validation as the recommender.

7.3 Training managers

Managers should be trained to use explanations as verification prompts rather than as assurances, to recognise that fluent explanations are not evidence of correctness, and to maintain override rates consistent with the system's known error rate. Feedback on individual reliance outcomes supports this calibration.

7.4 Explanation strategy by decision type

The criteria apply with different weight across decision types. For high-volume, low-stakes decisions, discriminability dominates: a simple reliability flag may calibrate reliance better than a detailed narrative that managers have no time to read. For low-volume, high-stakes decisions, faithfulness and actionability dominate, because the manager will scrutinise the explanation and act on it. For decisions subject to regulatory review, the explanation must additionally be reproducible from the logged model state. A single explanation design is unlikely to serve all three, and organisations should expect to maintain several.

7.5 Field validation

The simulation's propositions can be tested in a field experiment that randomises explanation conditions across managers using the same decision system, records acceptances and outcomes, and computes the reliance cells by condition. Faithful explanations can be constructed from validated attribution methods and unfaithful ones from narrative generators not conditioned on the model; a no-explanation control completes the design. Because outcomes may take weeks to resolve, the experiment should run long enough for the over-reliance costs to materialise in measured losses.

8. Limitations

The harness encodes the three explanation types through two parameters and assumes a single correctness cue; real explanations are richer and managers' use of them more varied. The recommender's accuracy and the cue distributions are design values. Reliance outcomes are weighted equally in the appropriate-reliance measure, whereas business costs are asymmetric. All reported values are simulation outputs.

9. Conclusion

Explanations should be judged by whether they help managers rely on automated decisions when they are right and override them when they are wrong. In a controlled simulation, faithful explanations improved calibration and reduced over-reliance, while fluent but unfaithful explanations produced the most trust and the most over-reliance. Transparency that builds trust without building calibration can make automated business decisions worse. Explanation design, measurement and governance should therefore centre on faithfulness, discriminability and reliance outcomes.

References

[1]. Gupta, A. (2024). Cloud security in the era of big data: Protecting large-scale storage systems, ensuring query privacy, and safeguarding data lakes against emerging threats. International Journal of Innovative Research in Science, Engineering and Technology, 13(11). https://doi.org/10.15680/IJIRSET.2024.131100217

[2]. Bhaskara Raju Rallabandi. (2023). CLOSED-LOOP DIGITAL-TWIN MANAGEMENT FOR HYBRID 5G-NTN NETWORKS. American Journal of Management and IOT Medical Computing, 2(3), 30–35. https://doi.org/10.64751/ajmimc.2023.v2.n3.pp30-35

[3]. Mahadasu, S. S. (2024). Closed-loop sustainability orchestration for energy-aware RAN, edge, and data-center workloads in 5G-Advanced networks. International Journal of Engineering Research and Science & Technology, 20(2), 1392–1398. https://doi.org/10.62643/ijerst.2024.v20.n2.4407

[4]. Kumar, Ashok, and Arpit Jain. "Image smog restoration using oblique gradient profile prior and energy minimization." Frontiers of Computer Science 15, no. 6 (2021): 156706.

[5]. Talasila, D. (2020). Deployment of shift-left security practices in agile development for embedding security controls early in the lifecycle and reducing technical debt through dev-centric training. Turkish Online Journal of Qualitative Inquiry, 11(1), 643–651. https://doi.org/10.69980/jzqq0t93

[6]. Chatrath, A. (2020). The role of policy-as-code in DevSecOps: Automating compliance, governance, and risk management in cloud-native and hybrid IT environments. International Journal of Innovative Research in Computer and Communication Engineering, 8(1). https://doi.org/10.15680/IJIRCCE.2020.0801020

[7]. Gupta, A. (2022). The role of artificial intelligence in transforming healthcare delivery: A critical analysis of machine learning models, predictive diagnostics, and ethical challenges in medical decision-making. NeuroQuantology, 20(3), 1383–1399. https://doi.org/10.48047/nq.2022.20.3.NQ23005

[8]. Ahuja, R. (2023). The role of artificial intelligence and machine learning in DevSecOps: Leveraging predictive analytics, automated threat detection, and anomaly identification for secure software delivery pipelines. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 381–389. https://www.ijritcc.org/index.php/ijritcc/article/view/11946

[9]. Harshitha, G., Kumar, S., Rani, S., & Jain, A. (2021, November). Cotton disease detection based on deep learning techniques. In 4th Smart Cities Symposium (SCS 2021) (Vol. 2021, pp. 496–501). IET.

[10]. Bhanushali, B. (2020). The industry needs a validated model to justify the immense cost of migrating from manual, periodic KYC (know your customer) to automated. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 3(11), 1799–1805. https://doi.org/10.15680/IJMRSET.2020.0311009

[11]. Kanabar, K., Dey, R., Mahajan, R., Jadhav, P. V., Khan, M., & Karimullah, S. (2026). Comprehensive guide to blockchain technology: Ecosystems, implementation, governance, and innovations. In A. K. Singh, S. Saxena, & A. K. Haghi (Eds.), Cybernetic shield: Securing the future of machine intelligence (pp. 175–182). CRC Press. https://doi.org/10.1201/9781003567585-16

[12]. Jain, Jaishree, Arpit Jain, Saurabh Kumar Srivastava, Chaman Verma, Maria Simona Raboaca, and Zoltán Illés. "Improved security of e-healthcare images using hybridized robust zero-watermarking and hyper-chaotic system along with RSA." Mathematics 10, no. 7 (2022): 1071.

[13]. Mahadasu, S. S. (2022). Cross-domain service assurance for private 5G networks using streaming telemetry and dependency-aware event correlation. International Journal of Data Science and IoT Management System, 1(3), 51–56. https://doi.org/10.64751/ijdim.2022.v1.n3.1290

[14]. Bhaskara Raju Rallabandi. (2022). SYNC-ADAPTIVE RESOURCE SCHEDULING IN PRIVATE 5G FOR TIME-CRITICAL APPLICATIONS. International Journal of Data Science and IoT Management System, 1(2), 40–45. https://doi.org/10.64751/ijdim.2022.v1.n2.pp40-45
[15]. Talasila, D. (2021). A risk-based framework for database security: Identifying, classifying, and prioritizing threats for adaptive security policy enforcement. International Journal on Recent and Innovation Trends in Computing and Communication, 9(1), 54–61. https://www.ijritcc.org/index.php/ijritcc/article/view/11919
[16]. Devulapalli, N. (2023). Database security and big data analytics: Protecting large-scale data warehouses, ensuring query privacy, and mitigating emerging threats in real-time analytics systems. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7), 622–629. https://www.ijritcc.org/index.php/ijritcc/article/view/11939
[17]. Jadhav, P. V., Krishnan, S. B., Dey, R., & Chakrabarti, P. (2026). Combining deep learning and statistical models: LSTM-ARIMA ensemble for financial forecasting. IAENG International Journal of Computer Science, 53(1), 236–246. https://www.iaeng.org/IJCS/issues_v53/issue_1/IJCS_53_1_24.pdf
[18]. Rangappa, A. S. (2022). The use of blockchain for auditable and tamper-proof database security logs: Enhancing transparency and trust in data access monitoring. International Journal on Recent and Innovation Trends in Computing and Communication, 10(9), 254–261. https://www.ijritcc.org/index.php/ijritcc/article/view/11925
[19]. Kumar, S., Jain, A., & Moparthi, N. R. (2022). Enhanced method of object tracing using extended Kalman filter via binary search algorithm.
[20]. Chatrath, A. (2021). Bias, fairness, and ethics in artificial intelligence: A comprehensive study of algorithmic discrimination, transparency challenges, and governance frameworks. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 4(1). https://doi.org/10.15680/IJMRSET.2021.0401014
[21]. Talasila, D. (2024). Adoption of data loss prevention strategies in SaaS platforms for safeguarding confidential information and preventing unauthorized transfers through real-time content inspection. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 7(7), 13537–13545. https://doi.org/10.15680/IJMRSET.2024.0707293
[22]. Rangappa, A. S. (2023). An analytical study of role-based access control (RBAC) and attribute-based access control (ABAC) in database security for multi-tenant and cloud-based architectures. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 812–819. https://www.ijritcc.org/index.php/ijritcc/article/view/11943
[23]. Kumar, S., Sharma, K., Kumar, P. A., Jain, A., Bhagat, S. K., & Singh, P. (2024, September). An improved particle swarm approach for energy-aware location-aided routing in mobile ad-hoc network. In 2024 7th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 7, pp. 1119–1124). IEEE.
[24]. Mahadasu, S. S., & Rallabandi, B. R. (2023). Federated learning for privacy-preserving RAN optimization across multi-site enterprise 5G networks. International Journal of Engineering Science and Advanced Technology, 23(4), 53–57. https://doi.org/10.64771/ijesat.2023.v23.i04.pp3847
[25]. Bhanushali, B. (2020). Effective sanctions screening and false positive identification. International Journal of Innovative Research in Science, Engineering and Technology, 9(4), 8306–8313. https://doi.org/10.15680/IJIRSET.2020.0904179
[26]. Ahuja, R. (2022). Application of static application security testing (SAST) in CI/CD pipelines for early detection of insecure coding practices through syntax tree analysis and custom rule sets. International Journal on Recent and Innovation Trends in Computing and Communication, 10(2), 80–87. https://www.ijritcc.org/index.php/ijritcc/article/view/11922

[27]. Chatrath, A. (2020). DevSecOps for financial services: An in-depth study of secure CI/CD practices, regulatory compliance, and real-time threat monitoring in cloud-based FinTech applications. International Journal of Innovative Research in Science, Engineering and Technology, 9(11). https://doi.org/10.15680/IJIRSET.2020.0911098

[28]. Devulapalli, N. (2024). The role of homomorphic encryption in database security: Enabling confidential query processing, secure data sharing, and privacy-preserving analytics. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 7(8), 14319–14326. https://doi.org/10.15680/IJMRSET.2024.0708082

[29]. Gupta, A. (2024). Containerization, virtualization, and cloud security: Analyzing vulnerabilities in Kubernetes, Docker, and hypervisor-based architectures with mitigation strategies. International Journal of Advanced Research in Education and Technology, 11(3), 1322–1331. https://doi.org/10.15680/IJARETY.2024.1103067

[30]. Aggarwal, A. (2020). Deployment of multi-factor authentication in cloud-based enterprise applications for preventing credential theft and unauthorized access through adaptive verification layers. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 3(8). https://doi.org/10.15680/IJMRSET.2020.0308009

[31]. Jain, A. (2024, December). Energy-Efficient Signal Processing Architectures for IoT Networks Design. In 2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN) (pp. 362–367). IEEE.

[32]. Khan, S. (2017). The role of privacy-preserving techniques in database security: Secure multi-party computation, differential privacy, and homomorphic encryption. The Research Journal, 3(4), 29–35.

[33]. Dwivedi, D. (2023). The technical and ethical challenges of building safe agentic AI systems: Balancing autonomy, predictability, alignment, and human oversight in next-generation AI models. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 2024–2031. https://www.ijritcc.org/index.php/ijritcc/article/view/11928

[34]. Aggarwal, A. (2019). Application of secure Virtual Private Cloud (VPC) architectures in public cloud infrastructure for strengthening network isolation and segmenting trust zones through fine-tuned routing. International Journal of Multidisciplinary and Scientific Emerging Research, 7(1), 423–431. https://doi.org/10.15662/IJMSERH.2019.0701048

[35]. Bhaskara Raju Rallabandi. (2024). DESIGNING NTN–TERRESTRIAL 6G EXPERIMENTS FOR AGRICULTURE AND SMART GRIDS. American Journal of Management and IOT Medical Computing, 3(3), 27–32. https://doi.org/10.64751/ajmimc.2024.v3.n3.pp27-32

[36]. Jain, J., & Jain, A. (2022). Securing e-Healthcare Images Using an Efficient Image Encryption Model. Scientific Programming, 2022(1), 6438331.

[37]. Mahajan, R., Kanabar, K., Dey, R., Jadhav, P. V., Khan, M., & Ghantasala, G. S. P. (2026). Exploring big tech vulnerabilities: Transparent blockchain harvesting. In A. K. Singh, S. Saxena, & A. K. Haghi (Eds.), Cybernetic shield: Securing the future of machine intelligence (pp. 167–174). CRC Press. https://doi.org/10.1201/9781003567585-15

[38]. Jain, Arpit, Nageswara Rao Moparthi, A. Swathi, Yogesh Kumar Sharma, Nitin Mittal, Ahmed Alhussen, Zamil S. Alzamil, and MohdAnul Haq. "Deep Learning-Based Mask Identification System Using ResNet Transfer Learning Architecture." Computer Systems Science & Engineering 48, no. 2 (2024): 341.

[39]. Mahadasu, S. S. (2024). AI-native wireless digital twins for precision agriculture: Edge intelligence and predictive farm operations in 6G ecosystems. International Journal of Data Science and IoT Management System, 3(1), 65–72. https://doi.org/10.64751/ijdim.2024.v3.n1.1287

[40]. Devulapalli, N. (2023). Database security in disaster recovery and business continuity planning: Ensuring data availability, backup integrity, and secure failover mechanisms. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 820–827. https://www.ijritcc.org/index.php/ijritcc/article/view/11944
[41]. Khan, S. (2018). The role of zero-trust models in database security: Eliminating implicit trust and enforcing continuous verification in enterprise data access systems. International Journal of Research in Electronics and Computer Engineering, 6(1), 1622–1628.
[42]. Anchala, S. (2019). The evolution of DevSecOps in software supply chain security: Addressing dependencies, open-source vulnerabilities, and the prevention of software supply chain attacks. International Journal of Multidisciplinary and Scientific Emerging Research, 7(1), 415–422. https://doi.org/10.15662/IJMSERH.2019.0701047
[43]. Kaur, M., AlZubi, A. A., Jain, A., Singh, D., Yadav, V., & Alkhayyat, A. (2023). DSCNet: deep skip connections-based dense network for ALL diagnosis using peripheral blood smear images. Diagnostics, 13(17), 2752.
[44]. Anchala, S. (2020). Adoption of secure access service edge (SASE) in distributed enterprises for ensuring cloud application protection and network optimization through unified security frameworks. Turkish Online Journal of Qualitative Inquiry, 11(4), 2964–2973. https://doi.org/10.69980/60m26411
[45]. Dwivedi, D. (2023). Integration of secure file upload mechanisms in user-facing applications for preventing malware injections and file-based exploits through content-type validation. International Journal on Recent and Innovation Trends in Computing and Communication, 11(6), 768–775. https://www.ijritcc.org/index.php/ijritcc/article/view/11940
[46]. Ahuja, R. (2023). Implementation of AI-driven input validation in user interfaces for preventing injection attacks and ensuring data sanitation through adaptive filtering and pattern recognition. International Journal on Recent and Innovation Trends in Computing and Communication, 11(8), 884–891. https://www.ijritcc.org/index.php/ijritcc/article/view/11936
[47]. Bhanushali, B. (2020). Enhancing alert investigation process with feedback loop to increase efficiently and model tuning. International Journal of Innovative Research in Computer and Communication Engineering, 8(8), 3366–3373. https://doi.org/10.15680/IJIRCCE.2020.0808100
[48]. Rangappa, A. S. (2024). Generative AI in human-machine collaboration: Exploring co-creation dynamics, shared agency, and the role of human oversight in AI-augmented creative and analytical tasks. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 13(4), 985–992. https://doi.org/10.15662/IJAREEIE.2024.1304077
[49]. Aggarwal, A. (2026). Adoption of end-to-end encryption in cloud communication channels for ensuring data confidentiality and trustworthiness through secure protocol enforcement. Journal of Critical Reviews, 7(12), 5493–5499. https://doi.org/10.69980/jcr.v7:i12.13407
[50]. Jain, Arpit, Adesh Kumar, and Sanjeev Sharma. "Comparative design and analysis of mesh, torus and ring NoC." Procedia Computer Science 48 (2015): 330–337.
[51]. Dwivedi, D. (2024). Deployment of AI-based CAPTCHA systems in web applications for preventing automated bot attacks and brute force attempts through adaptive human verification. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 7(7), 13529–13536. https://doi.org/10.15680/IJMRSET.2024.0707292
[52]. Anchala, S. (2019). Database security in e-governance systems: Protecting citizen records, ensuring transparency, and managing public trust in cloud-based platforms. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 2(11), 2268–2276. https://doi.org/10.15680/IJMRSET.2019.0211014

[53]. Khan, S. (2016). A study of data provenance and integrity in database security: Ensuring authenticity, non-repudiation, and accountability in data lifecycle management. International Journal of Research in Electronics and Computer Engineering, 4(3), 180–186.