

Trust by Design: Launching the *Journal of Cybersecurity and Intelligent Systems*

Parikshit N. Mahalle* 

Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Technology, Pune, Maharashtra, 411037, India

*Corresponding Author

Parikshit N. Mahalle

✉ eic.cdis@gr-journals.com

Published Online: 30 September 2026

Citation

P. N. Mahalle, Trust by design: launching the Journal of Cybersecurity and Intelligent Systems, *Journal of Cybersecurity and Intelligent Systems*, 2026, 1(1), 26506, <https://doi.org/10.64189/cis.26506>.

Open Access

This article is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/), which permits the non-commercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as appropriate credit to the original author(s) and the source is given by providing a link to the Creative Commons License and changes need to be indicated if there are any. The images or other third-party material in this article are included in the article's Creative Commons License, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons License and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this License, visit: <https://creativecommons.org/licenses/by-nc/4.0/>

© The Author(s) 2026

As critical infrastructure, from power grids to global finance, becomes intrinsically bound to complex digital ecosystems, security can no longer exist as a reactive afterthought. With AI, IoT, cloud computing, and blockchain becoming integral to digital infrastructure, the acceleration of cyber threats continuously matches the advancement of defensive capabilities.^[1-3] Cybersecurity can no longer be treated as a final layer added before deployment. It has to be a design principle that runs from application code to network edge, from data governance to supply chain.^[4,5]

With this mission in mind, we proudly introduce the inaugural issue of the *Journal of Cybersecurity and Intelligent Systems*, a multidisciplinary forum dedicated to advancing research in cybersecurity, cyber defense, and strategic technology. The journal addresses critical vulnerabilities in digital security, information warfare, and critical infrastructure protection. Our scope encompasses threat intelligence, ethical hacking, post-quantum cryptography, secure IoT and edge architectures, blockchain, explainable and ethical AI, and cyber law and governance. We invite original research, systematic reviews, and case studies that successfully bridge theoretical innovation with real-world defense applications. This first issue presents five contributions that follow a natural arc in building trustworthy systems. Defenders must first find and close weaknesses, then detect attacks, then verify who and what can be trusted, and finally govern how shared data is used. For each paper, we outline the approach, the findings, and where the work can be applied.

Bidve *et al.* developed an AI-driven framework that combines OWASP ZAP, Burp Suite Professional, FOCA, and Vega in a single Python-based interface. It automates reconnaissance, vulnerability scanning, analysis, reporting, and remediation recommendations, uses multithreading and multiprocessing to run assessments in parallel, and prioritizes vulnerabilities by severity. Their experiments showed that combining scanners improves the detection of common weaknesses such as SQL injection, cross-site scripting, broken authentication, cross-site request forgery, XML external entity attacks, insecure configurations, and API flaws. Compared with standalone tools, the framework offered broader coverage, better usability, stronger reporting, and greater efficiency. Its structured reports support compliance and risk management, and it lowers the cost and complexity of traditional penetration testing for modern web applications.^[6]

H. M. Khan *et al.* addressed trust in the pharmaceutical supply chain. Their system uses Solidity smart contracts on Ethereum to record each stage from raw material to retail. Soulbound Tokens act as non-transferable credentials so that only verified manufacturers and suppliers can participate. Thousands of product identifiers are batched off-chain into a single Merkle root stored on-chain, with cryptographic inclusion proofs for verification. For a 10,000-identifier batch, Merkle-based registration used 127,813 gas units against an estimated 350,000,000 for sequential registration, an estimated reduction of 99.96%. Over 50 local trials, verification averaged 2.188 ms and lifecycle queries 1.409 ms. These results were obtained in a local environment. The architecture applies to tamper-evident participant authorization, batch registration, and product verification against counterfeiting.^[7]

Chaudhari turned to threat detection in connected environments. The paper applies unsupervised learning, including Gaussian Mixture Models, to detect malware and network anomalies in the IoT-23 dataset, without the labeled data that supervised methods depend on. The study presents this as an adaptive and proactive defense that can identify novel and zero-day threats while limiting false positives, where signature-based systems struggle. The approach suits enterprise, cloud, and critical-infrastructure settings. Integrated with security information and event management (SIEM) systems, it can reduce manual intervention and response time.^[8]

M. S. Khan *et al.* proposed a decentralized data trust system for privacy-preserving federated learning, aimed at sensitive and regulated domains such as healthcare. It has four layers: federated training, privacy protection through secure aggregation and differential privacy, blockchain-based governance through smart contracts, and contribution-aware incentives using an approximate Shapley value. A comparative analysis against conventional federated learning, blockchain-enabled federated learning, and data marketplaces shows broader coverage of privacy, auditability, trust, incentives, and regulatory traceability. The work is conceptual, and the authors plan quantitative validation of model utility, communication overhead, scalability, and incentive cost. Its applications lie in collaborative AI where data cannot be shared, accountability is required, and participants must be fairly rewarded.^[9]

S. Mohammed *et al.* addressed security within the application itself. They enhanced the standard OAuth 2.0 framework with comprehensive JSON Web Token (JWT) encryption in Spring Boot, using Spring Security. Confidential user data, claims, and user roles stay protected inside the token payload even if a token is breached, and role-based access control is managed on top. The system was evaluated with unit tests and manual penetration testing. The results show that encrypted

JWTs protect token contents and secure the access-control mechanism, mitigating token interception, replay attacks, and privilege escalation. The approach applies to any web application or API that needs secure authentication and authorization.^[10]

Together, these papers show that trust can be engineered through automation, cryptography, and intelligent analytics, and that defending critical systems means securing every layer. They also remind us that promising architectures must be validated at scale and under real-world conditions, a challenge we hope future submissions will take up.

We are committed to a rigorous and efficient peer review process that ensures every published work meets the highest scientific, methodological, and ethical standards. On behalf of the Editorial Office, we extend a heartfelt welcome to our readers, authors, and reviewers. We invite you to contribute your work and help shape this journal into a leading forum for secure and intelligent digital systems.

Conflict of Interest

There is no conflict of interest.

Artificial Intelligence (AI) Use Disclosure

The authors declare that artificial intelligence (AI)-assisted tools were used only for language refinement, grammar improvement, and manuscript structuring purposes during the preparation of this work. All technical content, experimental implementation, results, and interpretations were independently developed and verified by the authors.

References

- [1] S. K. Sahu, K. Mazumdar, Exploring security threats and solutions techniques for Internet of Things (IoT): from vulnerabilities to vigilance, *Frontiers in Artificial Intelligence*, 2024, 7, 1397480, doi: 10.3389/frai.2024.1397480
- [2] H. Chen, M. Pendleton, L. Njilla, S. Xu, A survey on Ethereum systems security: vulnerabilities, attacks, and defenses, *ACM Computing Surveys*, 2020, 53, 67, doi: 10.1145/3391195.
- [3] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025, 2025, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>, Accessed 29 September 2026.
- [4] CISA, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software, 2023, <https://www.cisa.gov/resources-tools/resources/secure-by-design>, Accessed 29 September 2026.
- [5] M. Souppaya, K. Scarfone, D. Dodson, Secure

- Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, *NIST Special Publication*, 2022, 800-218, doi: 10.6028/NIST.SP.800-218.
- [6] V. Bidve, K. Kakade, V. Kimbahune, K. Vhatkar, An AI-driven integrated framework for automated web application penetration testing using multi-tool vulnerability assessment, *Journal of Cybersecurity and Intelligent Systems*, 2026, **1**, 26501, doi: 10.64189/cis.26501.
- [7] H. M. Khan, S. Jafri, A. Z. N. Kalam, A. A. M. Irfan, Scalable zero-trust supply chain management with soul-bound tokens and Merkle tree batching, *Journal of Cybersecurity and Intelligent Systems*, 2026, **1**, 26502, doi: 10.64189/cis.26502.
- [8] H. N. Chaudhari, Unsupervised Gaussian Mixture Model (GMM)-based malware detection in IoT networks, *Journal of Cybersecurity and Intelligent Systems*, 2026, **1**, 26503, doi: 10.64189/cis.26503.
- [9] M. S. Khan, S. Khan, S. Shaikh, Decentralized data trust system for privacy-preserving federated learning, *Journal of Cybersecurity and Intelligent Systems*, 2026, **1**, 26504, doi: 10.64189/cis.26504.
- [10] S. Mohammed, A. I. M. Lassakeur, P. Rutravigneshwaran, Design and Implementation of Spring Security Framework Using OAuth 2.0 for Spring Boot Applications, *Journal of Cybersecurity and Intelligent Systems*, 2026, **1**, 26505, doi: 10.64189/cis.26505.

Publisher Note: The views, statements, and data in all publications solely belong to the authors and contributors. GR Scholastic is not responsible for any injury resulting from the ideas, methods, or products mentioned. GR Scholastic remains neutral regarding jurisdictional claims in published maps and institutional affiliations.