

Zero-Trust Security Adoption and Its Implications for Digital Business Continuity

Iroda Bakhromova

Tashkent Institute of Irrigation and Agricultural Mechanization Engineers National Research University

Abstract

Perimeter-based security assumes that what is inside the network can be trusted, an assumption that remote work, cloud services and supply-chain integration have made untenable. Zero-trust architecture replaces it with continuous verification of every access request, least-privilege authorisation and segmentation that limits movement between systems. The security case for zero trust is well made; its implications for business continuity, the capacity to keep services running during an attack, are less examined. This paper models an attack that gains an initial foothold and attempts lateral movement across an enterprise network of 200 hosts, and examines how zero-trust maturity, which reduces both the connectivity available to the attacker and the probability that each hop succeeds, changes the blast radius and the availability of critical services. In 100 simulated attacks per maturity level, an enterprise with no zero-trust controls sees 99% of hosts compromised and 99% of critical services unavailable; at 50% maturity the mean compromised share is 35% (69% at the 95th percentile); at full maturity it is 1%. Continuity therefore improves nonlinearly with maturity, with most of the gain between 25% and 75%. The paper interprets the mechanism, sets out an adoption path that prioritises the segmentation and verification controls with the largest continuity effect, and discusses the operational costs and failure modes of zero trust, including the risk that verification infrastructure itself becomes a single point of failure.

Keywords: Zero-trust architecture; business continuity; lateral movement; network segmentation; blast radius; security adoption.

Introduction

Enterprise security was long organised around a perimeter: a hardened boundary between a trusted internal network and an untrusted outside. The model has failed on two counts. Attackers who breach the perimeter, through phishing, stolen credentials or compromised suppliers, find a trusted interior in which they can move freely to the systems they value; and the perimeter itself has dissolved as applications move to the cloud, employees work remotely and partners connect directly [1]. Zero-trust architecture responds by removing the assumption of trust: every access request is verified on the basis of identity, device and context, authorisation is limited to what the request needs, and the network is segmented so that access to one system does not imply access to others [2], [3].

Zero trust is usually justified in terms of breach prevention and data protection. This paper examines a different consequence: business continuity. Many

of the most damaging attacks, ransomware above all, cause harm not by stealing data but by moving laterally across an enterprise until enough systems are disabled to halt operations. The containment that zero trust provides should limit this movement and so preserve the operation of critical services during an attack. How much it does so, and how the benefit scales with maturity, is the question addressed.

The paper models lateral movement on a simulated enterprise network, examines the blast radius and critical-service availability as functions of zero-trust maturity, and derives an adoption path and implementation guidance oriented to continuity.

Background

Zero-trust principles

Zero-trust architecture [2],[3] rests on three principles: verify explicitly, using all available signals about identity, device, location and behaviour for every access decision; use least-privilege access,

granting the minimum rights needed for the minimum time; and assume breach, designing so that compromise of one component does not compromise others. The principles are realised through identity and access management, device posture assessment, micro-segmentation, policy enforcement points and continuous monitoring.

Lateral movement and ransomware

Post-compromise attack stages involve reconnaissance, credential harvesting and movement to additional systems [4]. Ransomware operators move laterally to reach backups, domain controllers and operational systems before encrypting, so that the damage is proportional to the share of the estate they reach. Containment that limits movement limits damage directly.

Business continuity

Business continuity management plans for the maintenance of critical functions during disruption [5]. For cyber incidents, continuity depends on how many systems are affected and how quickly they can be restored. Controls that reduce the first, by containing the attack, complement those that address the second, such as backup and recovery, and are the focus of this paper.

Continuity versus prevention

Prevention controls aim to stop the initial compromise; containment controls aim to limit what a compromise can reach. The two are complementary but respond differently to the attacker's adaptation. Prevention degrades as attackers find new entry techniques, and a determined attacker will eventually obtain a foothold; containment degrades only if the attacker can defeat segmentation and verification on each hop, which must be done repeatedly. Zero trust is therefore a continuity strategy that remains effective under the assumption that prevention will sometimes fail, which is the assumption the "assume breach" principle encodes and which recent incident experience supports.

Model

The enterprise network has $N = 200$ hosts, of which the first 20 provide critical services. Zero-trust maturity $m \in [0, 1]$ affects the network in two ways:

$$p_{\text{edge}} = 0.04(1 - 0.7m), p_{\text{hop}} = 0.5(1 - 0.85m), (1)$$

where p_{edge} is the probability that two hosts can communicate (segmentation reduces it) and p_{hop} is the probability that an attacker on one host can compromise a connected host in one step (verification and least privilege reduce it). An attack begins at a random host and attempts to spread for six steps. The outcomes are the share of hosts compromised and the share of critical services unavailable. Hypotheses: H1, blast radius falls with maturity; H2, the fall is nonlinear, with a threshold region in which most of the benefit is realised; H3, critical-service availability tracks the blast radius.

Simulation Design

For each maturity level in $\{0, 0.25, 0.5, 0.75, 1.0\}$, 100 attacks are simulated on independently generated networks. The mean and 95th-percentile compromised share and the mean share of critical services unavailable are reported. The edge and hop probabilities are design values chosen so that the unprotected network is fully compromisable within six steps; the harness examines how containment scales with maturity.

Results

Blast radius

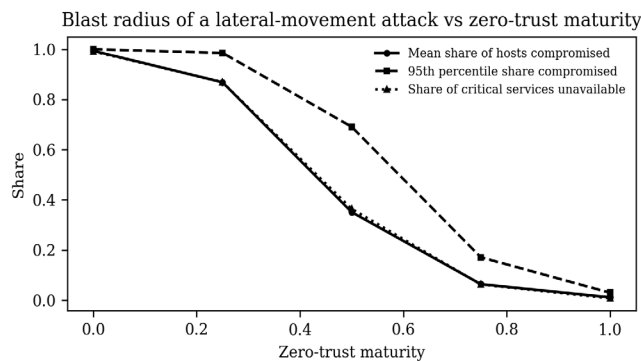
Table 1 and Figure 1 report outcomes. With no zero-trust controls, 99% of hosts are compromised on average and in essentially every run. At 25% maturity the mean falls to 87%, but the 95th percentile remains 99%: partial controls narrow the typical attack little and the worst case not at all. At 50% maturity the mean falls to 35% and the 95th percentile to 69%; at 75% to 6% and 17%; and at full maturity to 1% and 3%. The relationship is strongly nonlinear (H1, H2): the first quarter of maturity buys almost nothing, the middle half buys almost everything.

Critical services

The share of critical services unavailable tracks the mean compromised share closely at every level (H3), because critical hosts are not specially protected in the model. An enterprise that applied zero-trust controls preferentially to critical services would see their availability improve ahead of the overall blast radius, which is the basis of the adoption path below.

Table 1: Blast radius and critical-service availability by zero-trust maturity (100 simulated attacks per level; 200-host network)

<i>Zero-trust maturity</i>	<i>Mean share of hosts compromised</i>	<i>95th-percentile share compromised</i>	<i>Share of critical services unavailable</i>
0.00	99.3%	100.0%	99.1%
0.25	86.8%	98.5%	86.8%
0.50	35.1%	69.1%	36.4%
0.75	6.4%	17.1%	6.3%
1.00	1.2%	3.0%	0.8%

**Figure 1:** Mean and 95th-percentile share of hosts compromised, and share of critical services unavailable, against zero-trust maturity

Mechanism

The nonlinearity arises from percolation, the same threshold behaviour that governs epidemic spread on networks [6]: an attack spreads across the network only if the product of connectivity and per-hop success keeps each compromised host infecting, on average, at least one new host. Above that threshold the attack reaches most of the network; below it, the attack dies out after a few hops. Zero-trust controls reduce both factors, and their product crosses the threshold in the middle of the maturity range, which is why the benefit is concentrated there.

Sensitivity

The location of the threshold depends on the baseline connectivity and hop success, which vary across enterprises: a flat, highly connected network crosses the threshold at higher maturity than one that is already partly segmented. The nonlinearity itself is robust, since it follows from percolation rather than from the particular parameters, and its practical implication, that partial adoption yields disproportionately little, holds wherever the

unprotected network is above the threshold, which is the condition under which an enterprise has reason to adopt zero trust at all.

Adoption Path for Continuity

Segment critical services first

Because continuity depends on critical-service availability, the first segmentation boundaries should isolate the hosts that provide critical services, together with backups and identity infrastructure, from the general estate. This moves those hosts across the percolation threshold ahead of the rest and yields continuity gains at low overall maturity.

Verify high-privilege access

Per-hop success depends most on whether privileged credentials can be used from an arbitrary host. Enforcing strong, context-aware verification for administrative access and for access to critical segments reduces p_{hop} where it matters most, at modest cost compared with enterprise-wide rollout.

Extend segmentation and verification across the estate

With critical services protected, extending micro-segmentation and verification to the general estate drives the overall blast radius down. The simulation suggests that the enterprise should target the upper half of the maturity scale, since the lower half delivers little; a programme that stalls at 25% maturity has incurred cost without containment.

Test with lateral-movement exercises

Maturity should be measured by exercised containment, not by control inventory: red-team exercises that start from a compromised host and measure how far they can reach are the direct analogue of the simulation and should be run at each stage of adoption.

Costs and Failure Modes

Zero trust imposes operational costs: policy definition and maintenance, device management, user friction from repeated verification, and latency from policy enforcement. It also introduces failure modes. Verification infrastructure, including identity providers and policy engines, becomes a dependency for every access; its outage halts the enterprise as effectively as an attack, so it must be designed with the redundancy that continuity requires. Over-restrictive policies can block legitimate access during incidents, when flexibility is most needed; break-glass procedures with logging address this. And segmentation that is defined once and not maintained decays as systems change, returning the enterprise toward the connected state the model shows to be fragile.

Organisational adoption

Beyond technical cost, zero trust changes how access is governed. Business units accustomed to broad access must justify specific needs; application owners must define the flows their systems require; and security teams must maintain policies as the estate changes. Programmes that treat zero trust purely as a technology deployment stall at the policy-definition stage, which is where the simulation locates the maturity levels that deliver little containment. Executive sponsorship, a phased scope beginning with critical services, and a policy-ownership model that places definition with application owners and enforcement with security are the organisational prerequisites for reaching the maturity range in which continuity benefits appear.

Measuring maturity

The single maturity index in the model combines segmentation coverage and verification strength. Enterprises can measure each from their own environment: the share of host pairs that can communicate (from network policy or flow data) and the share of access decisions subject to context-aware verification (from identity systems). The product of the two, relative to the unprotected state, approximates the factor by which lateral movement is suppressed and indicates where the enterprise stands relative to the percolation threshold.

Relationship to recovery

Containment and recovery are the two halves of cyber continuity. The simulation shows containment limiting the number of systems affected; recovery capability determines how quickly the affected systems return. An enterprise with strong containment and weak recovery suffers small but prolonged disruptions; one with weak containment and strong recovery suffers large but brief ones. Because the cost of disruption typically rises faster than linearly with its breadth, as interdependent processes fail together, containment usually deserves priority, but the two should be planned jointly and the critical-service segment should be the first to receive both.

Limitations

The network model is a random graph with uniform hosts, a single attacker entry point and a fixed attack duration; real enterprises have structured networks, multiple entry points and adaptive attackers. Zero-trust maturity is a single index that scales both connectivity and hop success; implementations vary in which they reduce. Recovery and backup, which complete the continuity picture, are not modelled. All reported values are simulation outputs.

Conclusion

Zero-trust adoption protects business continuity by containing lateral movement, and the containment is strongly nonlinear in maturity: in simulation, partial adoption left the enterprise almost fully compromisable, the middle of the maturity range delivered most of the benefit, and full adoption limited attacks to a handful of hosts. Enterprises should adopt zero trust with continuity in mind, segmenting and verifying critical services first, pushing through the maturity threshold rather than stalling below it, testing containment through exercises, and designing the verification infrastructure itself for resilience.

References

1. Rangappa, A. S. (2020). Deployment of cross-platform code scanning tools in polyglot DevSecOps projects for uniform security testing and language-agnostic vulnerability coverage. *Journal of Critical Reviews*, 7(11), 5000–5006.

- <https://doi.org/10.69980/jcr.v7:i11.13402>
2. Mahadasu, S. S. (2025). AI-enhanced service management and orchestration for rApp and xApp lifecycle automation in Open RAN. *Communications on Applied Nonlinear Analysis*, 32(2s), 794–807. <https://doi.org/10.52783/cana.v32.6716>
3. Khan, S. (2022). Sales force security in mobile and remote work environments: Addressing authentication challenges, secure synchronization, and device-level threats. *International Journal of Innovative Research in Computer and Communication Engineering*, 10(12), 8735–8743. <https://doi.org/10.15680/IJIRCCCE.2022.1012040>
4. Chatrath, A. (2024). The role of encryption and key management in cloud security: Balancing performance, scalability, and confidentiality in multi-tenant and distributed data storage systems. *International Journal of Innovative Research in Science, Engineering and Technology*, 13(7). <https://doi.org/10.15680/IJIRSET.2024.1307187>
5. 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.
6. Bhanushali, B. (2023). Blockchain for trade finance: Enhancing cross-border payment transparency, reducing processing time, and mitigating fraud through distributed ledger systems. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(9), 5690–5697. <https://www.ijritcc.org/index.php/ijritcc/article/view/11932>
7. 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.
8. Bhanushali, B. (2024). Tokenization of real-world assets through block chain for improving liquidity, enabling fractional ownership, and reducing transaction costs in global financial markets. *International Journal of Advanced Research in Education and Technology*, 11(4), 1809–1816. <https://doi.org/10.15680/IJARETY.2024.1104071>
9. Dwivedi, D. (2020). Adoption of secure software updates in application lifecycle for preventing supply chain tampering and maintaining trust through cryptographically signed patches. *Journal of Critical Reviews*, 7(10), 6974–6980. <https://doi.org/10.69980/jcr.v7:i10.13406>
10. 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.
11. Chatrath, A. (2021). Implementation of AI in recruitment platforms for improving candidate screening and diversity inclusion through bias-free resume parsing and skill matching. *International Journal of Innovative Research in Computer and Communication Engineering*, 9(12). <https://doi.org/10.15680/IJIRCCCE.2021.0912046>
12. Mahadasu, S. S. (2024). Open RAN-based on-demand 6G agricultural networks: Adaptive edge infrastructure for autonomous farming systems. *International Journal of Data Science and IoT Management System*, 3(4), 96–102. <https://doi.org/10.64751/ijdim.2024.v3.n4.1289>
13. Jain, J., & Jain, A. (2022). Securing e-Healthcare Images Using an Efficient Image Encryption Model. *Scientific Programming*, 2022(1), 6438331.
14. Aggarwal, A. (2021). Implementation of machine learning in cloud SIEM solutions for enhancing threat detection accuracy and reducing alert fatigue through correlation-based anomaly detection. *NeuroQuantology*, 19(10). <https://doi.org/10.48047/nq.2021.19.10.NQ21226>
15. Devulapalli, N. (2020). Implementation of compliance-as-code in regulated DevSecOps environments for automating audit readiness and reducing human error through scripted control validation. *Journal of Critical Reviews*, 7(1), 2651–2657. <https://doi.org/10.69980/jcr.v7:i1.13405>
16. Dwivedi, D. (2019). The use of homomorphic encryption in cloud security: Enabling secure data processing, confidential query execution, and privacy-preserving cloud applications. *International Journal of Innovative Research in Science, Engineering and Technology*, 8(4), 4690–4698. <https://doi.org/10.15680/>

- IJRSET.2019.0804136
17. Gupta, A. (2021). Deployment of advanced endpoint detection in remote work environments for preventing malware intrusions and data exfiltration through behavioral analytics and AI-driven responses. *NeuroQuantology*, 19(9), 1206–1224. <https://doi.org/10.48047/nq.2021.19.9.NQ21199>
 18. Mahadasu, S. S. (2024). Real-time network digital twin synchronization for predictive capacity planning in multi-vendor private 5G systems. *International Journal of Engineering Research and Science & Technology*, 20(4), 483–488. <https://doi.org/10.62643/ijerst.2024.v20.n4.4405>
 19. Gupta, A. (2021). Application of cyber deception strategies in military networks for enhancing operational security and misleading attackers through adaptive honeypots and decoy systems. *NeuroQuantology*, 19(4), 317–333. <https://doi.org/10.48047/nq.2021.19.4.NQ21068>
 20. Talasila, D. (2023). Enhancing cloud security with intrusion detection and prevention systems (IDPS): Comparative evaluation of signature-based, anomaly-based, and AI-powered detection models. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(3), 828–836. <https://www.ijritcc.org/index.php/ijritcc/article/view/11945>
 21. 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.
 22. 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>
 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. Chatrath, A. (2021). Integration of AI-powered forensic analysis in cloud breach investigations for accelerating root cause identification and evidence collection through log correlation techniques. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 10(8). <https://doi.org/10.15662/IJAREEIE.2021.1008051>
 25. Aggarwal, A. (2021). Utilization of continuous vulnerability scanning in DevSecOps pipelines for preemptive threat detection and secure code deployment through automated security checks. *NeuroQuantology*, 19(1), 427–442. <https://doi.org/10.48047/nq.2021.19.1.NQ21055>
 26. Khan, S. (2022). The use of artificial intelligence in ESG (environmental, social, and governance) investing: A study on AI models for sustainability analytics in asset and wealth management. *International Journal of Multidisciplinary and Scientific Emerging Research*, 10(1), 431–439. <https://doi.org/10.15662/IJMSEERH.2022.1001046>
 27. Devulapalli, N. (2019). Post-quantum cryptography for database security: Preparing for the impact of quantum computing on encrypted data storage and secure queries. *Journal of Critical Reviews*, 6(1), 614–620. <https://doi.org/10.69980/jcr.v6.i1.13396>
 28. Khan, S. (2019). Sales force security compliance: An in-depth study of GDPR, HIPAA, and PCI-DSS enforcement in cloud-based CRM systems and their implications for global enterprises. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 8(9), 2211–2219. <https://doi.org/10.15662/IJAREEIE.2019.0809010>
 29. Talasila, D. (2020). Deployment of dynamic data masking in cloud-based applications for protecting sensitive information and enhancing privacy controls through contextual access filtering. *Journal of Critical Reviews*, 7(9), 4056–4062. <https://doi.org/10.69980/jcr.v7.i9.13403>
 30. Jain, Arpit, Nageswara Rao Moparthy, 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.
31. Anchala, S. (2023). Utilization of blockchain technology in cloud storage systems for enhancing data integrity and preventing unauthorized modifications through decentralized validation. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(5), 629–637. <https://www.ijritcc.org/index.php/ijritcc/article/view/11942>
32. Gupta, A. (2021). Implementation of cyber threat hunting in hybrid cloud environments for early breach detection and threat containment through behavior-based analysis tools. *NeuroQuantology*, 19(12), 1312–1329. <https://doi.org/10.48047/nq.2021.19.12.NQ21342>
33. Bhaskara Raju Rallabandi. (2019). Comprehensive Design and Field Performance Assessment of Early 5G NSA Private Networks for Industrial IoT Campuses. *International Journal of Engineering Research and Science & Technology*, 15(1), 22–26. <https://doi.org/10.62643/ijerst.2019.v15.n1.pp22-26>
34. Jain, Arpit, Adesh Kumar, and Sanjeev Sharma. “Comparative design and analysis of mesh, torus and ring NoC.” *Procedia Computer Science* 48 (2015): 330–337.
35. Mahajan, R. A., Dey, R., Khan, M., Mohd Su’ud, M., Alam, M. M., & Jadhav, P. (2025). Enhancing personalization in IoT-based health monitoring via generative AI and transfer learning. *Egyptian Informatics Journal*, 32, Article 100788. <https://doi.org/10.1016/j.eij.2025.100788>
36. Bhanushali, B. (2022). Blockchain-driven carbon credit trading systems for improving environmental transparency, reducing double counting, and ensuring accountability in climate finance. *International Journal on Recent and Innovation Trends in Computing and Communication*, 10(11), 292–300. <https://www.ijritcc.org/index.php/ijritcc/article/view/11927>
37. Anchala, S. (2020). Cloud security challenges in supply chain systems: Addressing vendor risks, data integrity, and third-party service provider vulnerabilities. *Journal of Critical Reviews*, 7(2). <https://doi.org/10.69980/jcr.v7:i2.13401>
38. Mahadasu, S. S. (2025). Distributed AI-RAN inference placement for joint radio optimization and edge workload acceleration. *International Journal of AI Electronics and Nexus Energy*, 1(1), 39–44. <https://doi.org/10.64751/7ep35m50>
39. Dwivedi, D. (2022). Application of AI-powered vulnerability scanners in legacy applications for identifying unpatched security flaws and weak dependencies through semantic code analysis. *International Journal on Recent and Innovation Trends in Computing and Communication*, 10(12), 617–623. <https://www.ijritcc.org/index.php/ijritcc/article/view/11918>
40. 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>
41. Anchala, S. (2023). Integration of confidential computing in multi-cloud environments for enhancing data privacy and regulatory compliance through encrypted processing and isolated execution. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(9), 5698–5709. <https://www.ijritcc.org/index.php/ijritcc/article/view/11933>
42. Aggarwal, A. (2022). Cloud security in artificial intelligence workloads: Protecting model training, data confidentiality, and AI-generated insights in cloud-based machine learning pipelines. *NeuroQuantology*, 20(3), 1367–1382. <https://doi.org/10.48047/nq.2022.20.3.NQ23004>
43. Rangappa, A. S. (2021). Database security in cloud environments: Exploring multi-tenant risks, data isolation challenges, and compliance mechanisms in hybrid and public clouds. *International Journal on Recent and Innovation Trends in Computing and Communication*, 9(2), 50–57. <https://www.ijritcc.org/index.php/ijritcc/article/view/11921>
44. Talasila, D. (2023). Implementation of cloud-based disaster recovery models for minimizing business downtime and ensuring operational continuity through geographically distributed

- backup systems. International Journal on Recent and Innovation Trends in Computing and Communication, 11(8), 867–874. <https://www.ijritcc.org/index.php/ijritcc/article/view/11934>
45. Devulapalli, N. (2020). The evolution of database security from centralized architectures to distributed cloud-native systems: A comparative and historical perspective. Turkish Online Journal of Qualitative Inquiry, 11(4), 2954–2963. <https://doi.org/10.69980/j1064z97>
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. Kumar, S., Jain, A., & Moparthy, N. R. (2022). Enhanced method of object tracing using extended Kalman filter via binary search algorithm.
48. Bhaskara Raju Rallabandi. (2023). AGENTIC-AI xAPPS: O-RAN MULTI-AGENT CONTROL FOR ENTERPRISE POLICY, SCHEDULING & SPECTRUM. International Journal of Data Science and IoT Management System, 2(4), 54–58. <https://doi.org/10.64751/ijdim.2023.v2.n4.pp54-58>
49. 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.
50. Bhaskara Raju Rallabandi. (2019). Enhancing 5G NSA Performance with Lightweight Network Data Analytics Loops. International Journal of Engineering Research and Science & Technology, 15(4), 57–61. <https://doi.org/10.62643/ijerst.2019.v15.n4.pp57-61>
51. Rangappa, A. S. (2020). Integration of behavioral analytics in developer workflows for detecting insider threats and malicious activities through activity monitoring and contextual profiling. International Journal of Innovative Research in Science, Engineering and Technology, 9(1), 13375–13383. <https://doi.org/10.15680/IJIRSET.2020.0901064>
52. Bhaskara Raju Rallabandi. (2024). 6G Cross-Layer Intent Engine: Automated Translation from Business Requirements to Network Policies and Real-Time Scheduling Controls. International Journal of Data Science and IoT Management System, 3(1), 44–48. <https://doi.org/10.64751/ijdim.2024.v3.n1.pp44-48>