Journal of Integrated Science, Technology and Management

Research Article

Cybersecurity Awareness and Employee Behavior: An Organizational Risk Management Framework

Shakhlo Samanova

Department of General sciences, Mamun University, Khiva, Uzbekistan

ARTICLE INFO

Article history:

Received: 12 April, 2026

Revised: 20 April, 2026

Accepted: 09 June, 2026

Published: 25 June, 2026

Keywords:

Cybersecurity awareness; employee behaviour; phishing; workload; nudges; human risk management.

DOI:

10.66592/rdcvpa89

ABSTRACT

Most cyber incidents begin with an employee action, and organisations respond with awareness training on the assumption that knowledge changes behaviour. The evidence is mixed: trained employees still click on phishing links, particularly under time pressure. This paper develops a risk management framework in which awareness training raises security knowledge, knowledge reduces unsafe behaviour, workload raises unsafe behaviour and weakens the protective effect of knowledge, and behavioural nudges at the point of decision reduce unsafe behaviour independently of knowledge. The framework is examined in a simulation of 2,000 employees in which phishing click behaviour follows the hypothesised process. Click rates fall from 47% to 22% with training among low-workload employees but only from 80% to 44% among high-workload employees; the training–workload interaction is negative, so training is less effective where it is most needed; and nudges cut click rates from 55% to 43% across all employees. The paper argues that awareness programmes should be managed as one component of a behavioural risk system that also controls workload exposure and embeds nudges, that programme effectiveness should be measured by observed behaviour rather than training completion, and that residual human risk should be quantified and transferred to technical controls. The contribution is a framework that connects awareness to organisational risk management rather than treating it as a compliance activity.

Introduction

Cybersecurity incident reports consistently attribute a majority of breaches to human actions: clicking malicious links, disclosing credentials, misdirecting data or circumventing controls. The standard organisational response is security awareness training, delivered annually or more often, and increasingly supplemented by simulated phishing campaigns. Training is mandated by many regulatory and audit frameworks, and completion rates are a common security metric.

Whether training changes behaviour is less certain. Research in the protection-motivation and planned-behaviour traditions finds that knowledge and intentions predict secure behaviour only moderately [1], [2], and field evidence shows that trained employees continue to fall for phishing at substantial rates. Two explanations stand out. First, security behaviour is governed by situational factors, above all workload and time pressure, which crowd out deliberate judgement regardless of knowledge [3]. Second, awareness programmes aim at knowledge rather than at the moment of decision, whereas much unsafe behaviour is habitual and responds to cues at that moment [4].

This paper proposes a framework that treats employee security behaviour as an organisational risk to be managed, not a training deficiency to be corrected. The framework specifies the behavioural process, identifies three intervention points, and connects residual human risk to technical controls and risk acceptance. It is examined in a simulation with a known behavioural process, and implications for programme design and measurement are derived.

***Corresponding Author:** Shakhlo Samanova

Address: Department of General sciences, Mamun University, Khiva, Uzbekistan

Email ✉**:** shakhlo.s@mamunedu.uz

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

© 2026, Shakhlo Samanova, This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

Background

Awareness, knowledge and behaviour

Protection motivation theory [1] holds that protective behaviour follows from perceived threat and perceived efficacy; awareness training raises both. Studies applying the theory of planned behaviour [2] find that attitudes and norms predict intentions, but that the intention–behaviour gap is large for security, because the protective behaviour competes with the primary task, and employees readily rationalise violations when the task demands it [5].

Workload and the compliance budget

Beautement, Sasse and Wonham [3] introduced the compliance budget: employees have finite capacity for security effort, and when workload consumes it, compliance falls. Time pressure also shifts decision-making from deliberate to heuristic processing, in which phishing cues are missed. Workload is therefore both a direct driver of unsafe behaviour and a moderator that weakens the effect of knowledge.

Nudges and point-of-decision interventions

Behavioural interventions that act at the moment of decision, such as warnings on external email, delayed delivery of suspicious messages, friction before credential entry and just-in-time reminders, can reduce unsafe actions without relying on recall of training [4]. They are effective for habitual behaviour precisely because they do not require deliberation.

Human risk in risk management

Risk management frameworks treat human error as a threat source but rarely model it quantitatively. Treating employee behaviour as a measurable risk with controllable drivers allows it to be managed with the same logic as technical vulnerabilities: estimate exposure, reduce likelihood through controls, and transfer or accept the residual.

Why training-centred programmes persist

Training-centred programmes persist for institutional reasons. Completion rates are easy to measure and to report to auditors and regulators; the training budget sits with a single function; and training places responsibility for incidents on the employee rather than on the design of the work environment. Workload management and point-of-decision interventions, by contrast, require cooperation from line management and IT, and their effects are visible only in behavioural data that many organisations do not collect. The framework below is intended to make these interventions comparable with training on a common risk metric so that resources can be allocated across them.

Framework

The framework specifies the behavioural process and three intervention points. Knowledge K depends on training T; the probability of unsafe behaviour (here, clicking a phishing link) depends on knowledge, workload W, their interaction and nudges N:

$$K = 0.2 + 0.6\,T + u,\ \text{logit}\,P(\text{click}) = \beta_0 - \beta_K K + \beta_W W + \beta_{WK} W(1 - K) - \beta_N N. \quad (1)$$

The intervention points are: training (raising K), workload management (lowering W for high-exposure roles) and nudges (raising N). Hypotheses: H1, training reduces unsafe behaviour; H2, workload increases it; H3, workload weakens the effect of training (negative interaction); H4, nudges reduce unsafe behaviour independently of training.

Residual risk after interventions is the predicted click probability aggregated across employees weighted by exposure; the framework requires that residual risk be compared with the capacity of technical controls (filtering, isolation, multi-factor authentication) to contain the consequences, and that any remainder be explicitly accepted.

Simulation Design

The harness generates 2,000 employees with training intensity and workload uniform on [0, 1] and nudges assigned at random with probability 0.5. Knowledge and click behaviour follow Equation (1) with $\beta_0 = 0.5$, $\beta_K = 2.5$, $\beta_W = 1.5$, $\beta_{WK} = 1.2$ and $\beta_N = 0.8$. A logistic regression of click on training, workload, nudges and the training–workload interaction is estimated, and click rates are tabulated by training and workload groups. Parameters are design values encoding the hypotheses; the harness examines the resulting magnitudes and the interaction.

Results

Training, workload and their interaction

The overall simulated click rate is 49%. Table 1 reports click rates by group. Among low-workload employees, training reduces the click rate from 47% to 22%; among high-workload employees, from 80% to 44%. The reduction is larger in absolute terms under high workload (36 versus 25 points) but the residual rate remains twice as high, and the logistic interaction coefficient is negative (–0.99), indicating that training's effect on the logit scale is weaker under high workload (H3). Workload alone has a large positive coefficient (2.64) (H2), and training a large negative one (–1.45) (H1).

Figure 1 shows the pattern. Both curves decline with training, but the high-workload curve lies far above the low-workload curve throughout, and at the highest training intensities the gap narrows only modestly. Training alone cannot bring high-workload employees to the click rate that low-workload employees reach with little training.

Table 1: Simulated phishing click rates by training intensity and workload (2,000 employees)

Group	*Low training (< 0.33)*	*High training (> 0.67)*	*Reduction*
Low workload (< 0.33)	47.4%	21.7%	−25.7 points
High workload (> 0.67)	79.5%	43.9%	−35.6 points

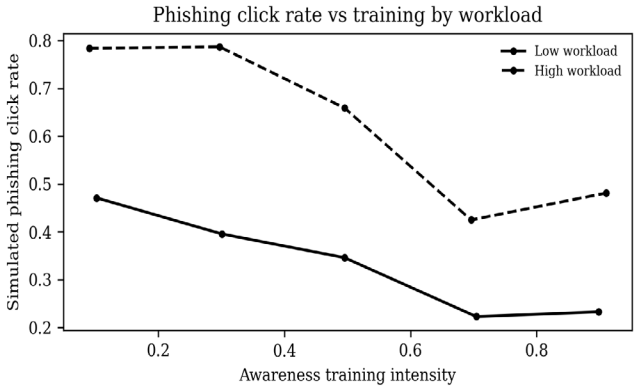


Figure 1: Simulated phishing click rate against awareness training intensity for low- and high-workload employees.

Nudges

Employees who receive nudges click at 43% against 55% for those who do not, a reduction of 12 points (H4). The logistic coefficient (−0.60) is independent of training and workload in the model, so the nudge effect applies equally to trained and untrained, busy and unhurried employees.

Residual risk

With high training, no nudges and the simulated workload distribution, the average predicted click rate remains above 30%. For an organisation receiving targeted phishing weekly, that residual implies that a successful compromise of at least one employee is near-certain over a year, which is the quantity the framework asks organisations to confront: training reduces human risk but leaves a residual that must be contained by technical controls or accepted.

Sensitivity

The relative size of the three effects depends on the design coefficients, but the structural result does not: as long as the workload–knowledge interaction is positive in Equation (1), training's protective effect is smaller where workload is higher, and as long as the nudge term is additive, nudges help regardless of training. The absolute click rates are high by design so that the mechanisms are visible; organisations with mature programmes will observe lower rates with the same qualitative pattern.

Implications for Risk Management

Manage the three intervention points together

Training, workload management and nudges address different parts of the process and are complementary. Programmes that rely on training alone leave workload-driven behaviour untouched and miss the point-of-decision channel. Organisations should identify high-exposure, high-workload roles, such as finance, procurement and executive assistants, and apply workload buffers and nudges to them specifically.

Measure behaviour, not completion

Training completion is an input measure. The framework's output measures are observed click rates from simulated phishing, reporting rates for suspicious messages, and credential-entry events on untrusted pages, tracked by role, workload and intervention. These measures make the relationships in Figure 1 observable in the organisation's own data and allow programme resources to be directed where behaviour is worst.

Quantify and allocate residual risk

Residual human risk should enter the organisation's risk register with an estimated likelihood, as for technical vulnerabilities, and should be matched against the technical controls that limit consequences: email filtering, link isolation, multi-factor authentication, least privilege and rapid revocation. Where those controls cannot contain the consequences of the residual, the organisation is accepting the risk and should say so.

Programme design

Awareness content should be short, frequent and role-specific rather than annual and generic; simulated phishing should be used for measurement and just-in-time teaching rather than for sanction, since punitive use suppresses reporting; and nudges should be reviewed for habituation, with warning designs rotated to maintain attention.

Culture and reporting

The model treats behaviour as individual, but security behaviour is shaped by norms. An organisation in which reporting a suspected phishing message is routine and praised obtains an additional control: early reports allow the security function to block a campaign before most employees see it, which reduces exposure rather than click probability. Programmes should therefore track reporting rates alongside click rates and should treat a high reporting rate as a success measure in its own right. Punitive responses to clicks depress reporting and forfeit this control.

Role-based exposure

Exposure to targeted attacks is concentrated in roles with payment authority, access to sensitive data or public

visibility. The framework's residual-risk calculation weights click probability by exposure, which concentrates attention on a small number of roles. For these roles, the appropriate response is often a technical one, such as mandatory out-of-band verification for payment changes, that removes the consequence of a click rather than attempting to eliminate the click itself.

Field validation

The framework can be tested with the data organisations already collect from simulated phishing campaigns, supplemented by workload indicators from workflow or calendar systems and by randomised assignment of nudges across employee groups. The key tests are the sign of the training–workload interaction and the additivity of the nudge effect; both can be estimated with a few thousand employee-campaign observations. Longitudinal data would additionally reveal the decay of training effects and habituation to nudges, which the simulation does not model.

Limitations

The harness encodes the hypothesised behavioural process with design parameters; it demonstrates the framework's logic and the interaction's consequences rather than testing them. Click behaviour is a single binary outcome, whereas human risk spans many behaviours. Habituation to nudges, decay of training effects and social influences are not modelled. All reported values are simulation outputs.

Conclusion

Employee security behaviour is a manageable organisational risk with three controllable drivers: knowledge, workload and point-of-decision cues. In simulation, training reduced unsafe behaviour substantially but less so under high workload, nudges reduced it independently, and a sizeable residual remained. Organisations should manage awareness, workload and nudges together, measure behaviour rather than completion, and quantify residual human risk so that it is contained by technical controls or explicitly accepted.

References

1. 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.
2. 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
3. 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
4. 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
5. 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
6. 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
7. 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
8. Jain, J., & Jain, A. (2022). Securing e-Healthcare Images Using an Efficient Image Encryption Model. Scientific Programming, 2022(1), 6438331.
9. 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
10. 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
11. 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
12. Kumar, S., Jain, A., & Moparthi, N. R. (2022). Enhanced method of object tracing using extended Kalman filter via binary search algorithm.
13. 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
14. 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
15. 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
16. 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
17. 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.
18. 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
19. 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
20. 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
21. 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
22. 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
23. 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
24. 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
25. 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
26. 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
27. 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.
28. 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
29. 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
30. 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
31. 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
32. 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
33. Jain, Arpit, Adesh Kumar, and Sanjeev Sharma. "Comparative design and analysis of mesh, torus and ring NoC." Procedia Computer Science 48 (2015): 330–337.
34. 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
35. 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.
36. 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
37. 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.
38. 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
39. 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
40. 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
41. 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
42. 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.
43. 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
44. 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.

45. 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
46. 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
47. 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
48. 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.
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, 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.
51. 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
52. 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.
53. 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