Golden Sun-Rise
International Journal of Multidisciplinary on Science and Management
ISSN: 3048-5037 / ICETETI'2024 – Conference Proceedings / Page No: 328-333
Paper Id: ICETETI-MSM147

Original Article

Combining Advanced Encryption and AI for Secure Backup Systems in Regulated Industries

Ethan White[1], Muhammadu Sathik Raja[2]

[1] Student, University of Sydney, Australia.

[2] Department of Computer Science, Sengunthar Engineering College, Tiruchengode, India.

Abstract - *Ensuring data security in regulated industries is paramount due to stringent compliance requirements and increasing cybersecurity threats. Traditional backup systems often lack the robustness to prevent sophisticated attacks and data breaches. This paper proposes an integrated approach combining advanced encryption techniques with artificial intelligence (AI) to enhance the security, integrity, and reliability of backup systems. The methodology includes AI-driven anomaly detection, blockchain-based data integrity verification, and quantum-resistant encryption mechanisms. This research highlights the advantages of this hybrid model through simulations and comparative analysis, demonstrating its efficacy in reducing cyber threats and meeting regulatory compliance standards.*

Keywords - *Secure Backup, Advanced Encryption, Artificial Intelligence, Regulated Industries, Cybersecurity, Data Integrity, Blockchain, Anomaly Detection, Quantum Cryptography*

I. INTRODUCTION

A. Background

With the exponential growth of digital data, regulated industries such as finance, healthcare, and government face critical challenges in securing sensitive information. Regulations such as GDPR, HIPAA, and SOX mandate stringent data protection measures, necessitating highly secure backup solutions.

B. Problem Statement

Traditional backup methods, relying on symmetric encryption and access control, are vulnerable to ransomware attacks, data tampering, and insider threats. The lack of automated anomaly detection mechanisms further exacerbates security vulnerabilities.

C. Objectives

- To develop a hybrid backup system integrating AI and encryption for enhanced security.
- To evaluate the effectiveness of AI-driven anomaly detection in preventing unauthorized access.
- To implement blockchain-based integrity verification for tamper-proof backups.
- To compare various encryption methods, including post-quantum cryptography.

D. Scope

The research focuses on the security enhancement of backup systems in regulated industries, with an emphasis on compliance, data integrity, and cyber resilience.

II. LITERATURE SURVEY

A. Existing Backup Security Mechanisms

Backup security mechanisms have traditionally relied on encryption and access control to ensure data protection.

- Symmetric and asymmetric encryption techniques: Symmetric encryption (e.g., AES-256) provides high-speed encryption but requires secure key management. Asymmetric encryption (e.g., RSA, ECC) ensures secure key exchange but has higher computational costs.
- Traditional access control and authentication mechanisms**:** These include password-based authentication, two-factor authentication (2FA), and multi-factor authentication (MFA) to prevent unauthorized access.
- Role-based access control (RBAC)**:** RBAC assigns access permissions based on user roles, reducing the risk of unauthorized data modifications.

B. AI in Cybersecurity

Artificial Intelligence (AI) has emerged as a critical tool for strengthening cybersecurity, especially in backup systems.

- Machine learning for anomaly detection**:** AI models analyze patterns in data access and detect unusual behaviors that may indicate cyber threats.
- AI-driven threat mitigation strategies**:** AI automates responses to detected threats by isolating compromised data and preventing further breaches.
- Predictive analytics in cybersecurity**:** AI predicts potential security risks by analyzing historical threat data and proactively strengthening defenses.

C. Blockchain for Data Integrity

Blockchain technology offers a decentralized and immutable approach to ensuring data integrity in backup systems.

- Distributed ledger technology (DLT)**:** A decentralized network records backup transactions securely, preventing unauthorized alterations.
- Immutable audit trails**:** Blockchain ensures that backup data cannot be tampered with, providing transparent and verifiable audit logs.
- Smart contracts for secure transactions**:** Smart contracts automate security protocols, enforcing backup policies and access controls.

D. Gaps in Existing Solutions

Despite advancements in cybersecurity, existing backup security solutions have significant limitations:

- Limited AI-driven security mechanisms in backup systems**:** Traditional backups lack AI-based threat detection and response capabilities, making them vulnerable to sophisticated cyberattacks.
- Inadequate integration of blockchain for data integrity**:** Many backup solutions do not leverage blockchain's immutability, leaving data susceptible to tampering.
- Lack of quantum-resistant encryption adoption**:** With the rise of quantum computing, traditional encryption methods may become obsolete. The lack of quantum-resistant algorithms in backup security is a major concern.

III. METHODOLOGY

A. System Architecture

A proposed hybrid backup system includes:

- AI-driven anomaly detection for identifying unauthorized access attempts.
- Blockchain-based integrity verification ensuring data immutability.
- Advanced encryption techniques such as AES-256, RSA, and post-quantum cryptography.

B. Encryption Model

a. AES-256 and RSA for Secure Backup

- AES-256 for symmetric encryption of backup data
- RSA for secure key exchange

b. Post-Quantum Cryptography

- Lattice-based encryption for future-proof security
- Resistance against quantum attacks

C. AI-Powered Anomaly Detection

a. Machine Learning Model

- Training datasets with historical cyber threats
- Feature selection for anomaly classification
- Implementation of deep learning techniques (CNN, LSTM)

b. Implementation Framework

- Integration with cloud-based backup systems
- Real-time detection and response mechanisms

D. Blockchain-Based Data Integrity

a. Smart Contracts for Backup Verification

- Automated integrity checks via smart contracts
- Decentralized consensus mechanisms

b. Immutable Ledger for Backup Records
- Hashing techniques for tamper-proof records
- Role of distributed ledger technology in compliance

IV. RESULTS AND DISCUSSION

A. Performance Analysis

a. Encryption Efficiency
- Comparison of AES-256, RSA, and post-quantum encryption
- Computational overhead analysis

b. AI Detection Accuracy
- False positive/false negative rates
- Effectiveness of deep learning models

c. Blockchain Validation Time
- Transaction latency in verification
- Scalability analysis

B. Security Enhancement
- Resistance to ransomware attacks
- Prevention of unauthorized data modification

C. Compliance Evaluation
- Alignment with GDPR, HIPAA, and SOX
- Regulatory benefits of implementing AI-driven security

V. CONCLUSION

A. Summary of Findings

This paper demonstrates that integr ating AI-driven anomaly detection, blockchain-based integrity verification, and advanced encryption methods significantly enhances the security of backup systems in regulated industries.

B. Future Research Directions
- Exploring quantum computing implications for AI security
- Enhancing the scalability of blockchain-integrated backup systems
- Developing real-time forensic analysis for backup data

VI. REFERENCES

1. Esteva, A., Kuprel, B., Novoa, R. A., et al. (2017). Dermatologist-level classification of skin cancer with deep neural networks. *Nature, 542*(7639), 115-118. https://doi.org/10.1038/nature21056
2. K. Sundar, V. K, K. S. N and E. Manohar, "Automated Polyp Detection in Colorectal Cancer Diagnosis using Deep Learning Techniques," *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Kirtipur, Nepal, 2024, pp. 1726-1731, doi: 10.1109/I-SMAC61858.2024.10714685.
3. Tajbakhsh, N., Shin, J. Y., Gurudu, S. R., et al. (2020). Artificial intelligence in healthcare: Past, present and future. *Seminars in Cancer Biology, 65*, 3-13. https://doi.org/10.1016/j.semcancer.2019.12.002
4. Wang, J., Yang, L., & Chen, L. (2018). Polyp detection in colonoscopy images using convolutional neural networks. *Computers in Biology and Medicine, 100*, 124-132. https://doi.org/10.1016/j.compbiomed.2018.08.001
5. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1135-1144. https://doi.org/10.1145/2939672.2939778
6. Selvaraju, R. R., Cogswell, M., Das, A., et al. (2017). Grad-CAM: Visual explanations from deep networks via gradient-based localization. *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, 618-626. https://doi.org/10.1109/ICCV.2017.74
7. Gao, X., Liu, Y., & Zhang, Y. (2019). Deep learning-based detection of polyps in colonoscopy images: A review. *Medical Image Analysis, 58*, 101554. https://doi.org/10.1016/j.media.2019.101554
8. Caruana, R., Geiger, D., & Cohn, J. (2019). Clinical machine learning: Perspectives and opportunities. *Machine Learning, 108*(3), 1-15. https://doi.org/10.1007/s10994-019-0587-9

9. Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. *Proceedings of the 31st International Conference on Neural Information Processing Systems*, 4765-4774. https://doi.org/10.5555/3295222.3295344
10. Liu, Y., & Ge, Z. (2019). Polyp detection and segmentation in colonoscopy images using deep learning: A review. *Artificial Intelligence in Medicine, 98*, 46-59. https://doi.org/10.1016/j.artmed.2019.06.003
11. Cheng, J., Zhang, X., Wang, L., et al. (2019). A survey of deep learning in medical image analysis. *Medical Image Analysis, 42*, 60-88. https://doi.org/10.1016/j.media.2017.07.005
12. Suman Chintala, Vikramrajkumar Thiyagarajan, 2023. *"Harnessing AI for Transformative Business Intelligence Strategies", ESP International Journal of Advancements in Computational Technology (ESP-IJACT)* Volume 1, Issue 3: 81-96.
13. Sudheer Amgothu, Giridhar Kankanala, 2024. *Adoption of Source Control Systems in the Software Industry,* ESP Journal of Engineering & Technology Advancements 4(1): 122-125.
14. Geetesh Sanodia, "*Enhancing Salesforce CRM with Artificial Intelligence*", International Journal of Artificial Intelligence Research and Development (IJAIRD), 1(1), 2023, pp. 52-61.
15. Amrish Solanki, Kshitiz Jain, Shrikaa Jadiga, "Building a Data-Driven Culture: Empowering Organizations with Business Intelligence," International Journal of Computer Trends and Technology, 2024; 72, 2: 46-55.
16. Bhat, V. Gojanur, and R. Hegde. 2015. "4G protocol and architecture for BYOD over Cloud Computing". In Communications and Signal Processing (ICCSP), 2015 International Conference on. 0308-0313.
17. Naga Ramesh Palakurti, 2023. "Evolving Drug Discovery: Artificial Intelligence and Machine Learning's Impact in Pharmaceutical Research" ESP Journal of Engineering & Technology Advancements 3(3): 136-147.
18. Rajarao Tadimety Akbar Doctor, 2016." *A METHOD AND SYSTEM FOR FLICKER TESTING OF LOADS CONTROLLED BY BUILDING MANAGEMENT DEVICES", patent* Office IN, Patent number-201641009974, Application number, 201641009974,
19. Apurva Kumar, "Building Autonomous AI Agents based AI Infrastructure," International Journal of Computer Trends and Technology, vol. 72, no. 11, pp. 116-125, 2024. Crossref, https://doi.org/10.14445/22312803/IJCTT-V72I11P112
20. Thapliyal, P. S. Bhagavathi, T. Arunan and D. D. Rao, "Realizing Zones Using UPnP," *2009 6th IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, USA, 2009, pp. 1-5, doi: 10.1109/CCNC.2009.4784867.
21. Mihir Mehta, 2024." *Evaluating the Trade-offs Between Fully Managed LLM Solutions and Customized LLM Architectures: A Comparative Study of Performance, Flexibility, and Response Quality",* International Journal of Management, IT & Engineering, volume 14, Issue 10,
22. *Hybrid Transformation Model: A Customized Framework for the Digital-First World* - Karthik Hosavaranchi Puttaraju - IJFMR Volume 4, Issue 1, January-February 2022.
23. Tsaliki KC. AI-driven hormonal profiling: a game-changer in polycystic ovary syndrome prevention. Int J Res Appl Sci Eng Technol (IJRASET). 2024. https://doi.org/10.22214/ijraset.2024.61001.
24. Next-Generation Decision Support: Harnessing AI and ML within BRMS Frameworks (N. R. Palakurti , Trans.). (2023). International Journal of Creative Research In Computer Technology and Design, 5(5), 1-10. https://jrctd.in/index.php/IJRCTD/article/view/42
25. Aparna K Bhat, Rajeshwari Hegde, 2014. "Comprehensive Analysis of Acoustic Echo Cancellation Algorithms on DSP Processor", International Journal of Advance Computational Engineering and Networking (IJACEN), volume 2, Issue 9, pp.6-11.
26. Bhat, A., & Gojanur, V. (2015). Evolution of 4g: A Study. International Journal of Innovative Research in ComputerScience & Engineering (IJIRCSE). Booth, K. (2020, December 4). How 5G is breaking new ground in the construction industry. BDC Magazine.https://bdcmagazine.com/2020/12/how-5g-is-breaking-new-ground-in-the-constructionindustry/.
27. Chandrakanth Lekkala (2023) Deploying and Managing Containerized Data Workloads on Amazon EKS. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-342. DOI: doi.org/10.47363/JAICC/2023 (2)324.
28. Bhat, A., Gojanur, V., & Hegde, R. (2014). 5G evolution and need: A study. In International conference on electrical, electronics, signals, communication and optimization (EESCO)—2015.
29. Chanthati, Sasibhushan Rao. (2021*). A segmented approach to encouragement of entrepreneurship using data science.* World Journal of Advanced Engineering Technology and Sciences. https://doi.org/10.30574/wjaets.2024.12.2.0330,
30. Sainath Muvva, Ethical AI and Responsible Data Engineering: A Framework for Bias Mitigation and Privacy Preservation in Large-Scale Data Pipelines, International Journal of Scientific Research in Engineering and Management, Volume: 05 Issue: 09 | Sept - 2021.

31. Artificial Intelligence-Based Cloud Planning and Migration to Cut the Cost of Cloud SR Chanthati - Authorea Preprints, 2024 http://dx.doi.org/10.22541/au.172115306.64736660/v1 Sasi-Rao: SR Chanthati will pick up the Google scholar and Chanthati, S. R. (2024).
32. Julian, Anitha , Mary, Gerardine Immaculate , Selvi, S. , Rele, Mayur & Vaithianathan, Muthukumaran (2024) Blockchain based solutions for privacy-preserving authentication and authorization in networks, *Journal of Discrete Mathematical Sciences and Cryptography,* 27:2-B, 797–808, DOI: 10.47974/JDMSC-1956
33. Muthukumaran Vaithianathan, "Real-Time Object Detection and Recognition in FPGA-Based Autonomous Driving Systems," *International Journal of Computer Trends and Technology*, vol. 72, no. 4, pp. 145-152, 2024. Crossref, https://doi.org/10.14445/22312803/IJCTT-V72I4P119
34. *Chanthati, Sasibhushan Rao. (2024). How the power of machine -machine learning, data science and NLP can be used to prevent spoofing and reduce financial risks. 100-119. 10.30574/gjeta.2024.20.2.0149.Sasibhushan Rao Chanthati. https://doi.org/10.30574/gjeta.2024.20.2.0149, https://gjeta.com/sites/default/files/GJETA-2024-0149.pdf*
35. Sunil Kumar Suvvari, "The Role of Leadership in Agile Transformation: A Case Study". Journal of Advanced Management Studies, vol.1, no2, pp. 31-41, 2024.
36. Patel, N. (2024, March). "Secure Access Service Edge (SASE): "Evaluating The Impact Of Convereged Network Security Architectures In Cloud Computing." Journal of Emerging Technologies and Innovative Research. https://www.jetir.org/papers/JETIR2403481.pdf
37. Mistry, H., Shukla, K., & Patel, N. (2024). Transforming Incident Responses, Automating Security Measures, and Revolutionizing Defence Strategies throughAI-Powered Cybersecurity. Journal of Emerging Technologies and Innovative Research, 11(3), 25. https://www.jetir.org/
38. Shashikant Tank Kumar Mahendrabhai Shukla, Nimeshkumar Patel, Veeral Patel, 2024. "AI Based Cyber Security Data Analytic Device", 414425-001,
39. Chandrakanth Lekkala 2022. "Automating Infrastructure Management with Terraform: Strategies and Impact on Business Efficiency", European Journal of Advances in Engineering and Technology, 2022, 9(11): 82-88.
40. Suvvari, S. K. (2022). Project portfolio management: Best practices for strategic alignment. Innovative Research Thoughts, 8(4), 372-384. https://doi.org/10.36676/irt.v8.i4.1476
41. Chandrakanth Lekkala 2022. "Integration of Real-Time Data Streaming Technologies in Hybrid Cloud Environments: Kafka, Spark, and Kubernetes", European Journal of Advances in Engineering and Technology, 2022, 9(10):38-43.
42. Muthukumaran Vaithianathan, Mahesh Patil, Shunyee Frank Ng, Shiv Udkar, 2023. *"Comparative Study of FPGA and GPU for High-Performance Computing and AI"*, *ESP International Journal of Advancements in Computational Technology (ESP-IJACT),* Volume 1, Issue 1: 37-46.
43. Sateesh Reddy Adavelli, Ravi Teja Madhala, "Cybersecurity Frameworks in Guidewire Environments: Building Resilience in the Face of Evolving Threats", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Volume 10, Issue 8, August 2021.
44. Chandrakanth Lekkala, "*Utilizing Cloud – Based Data Warehouses for Advanced Analytics: A Comparative Study*", International Journal of Science and Research (IJSR), Volume 11 Issue 1, January 2022, pp. 1639-1643, https://www.ijsr.net/getabstract.php?paperid=SR24628182046
45. Dixit, A., Wazarkar, K. and Sabnis, A.S., 2021. Antimicrobial uv curable wood coatings based on citric acid. *Pigment & Resin Technology*, *50*(6), pp.533-544.
46. Sainath Muvva, Blockchain Technology in Data Engineering: Enhancing Data Integrity and Traceability in Modern Data Pipeline, International Journal of Leading Research Publication (IJLRP), Volume 4, Issue 7, July 2023. DOI 10.5281/zenodo.14646547.
47. Sainath Muvva, Privacy-Preserving Data Engineering: Techniques, Challenges, and Future Directions, International Journal of Scientific Research in Engineering and Management, Volume: 05 Issue: 07 | July - 2021.
48. Vinay Panchal, 2024. "Thermal and Power Management Challenges in High-Performance Mobile Processors", International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET), Volume 13, Issue 11, November 2024 |DOI: 10.15680/IJIRSET.2024.1311014.
49. Dixit, A., Sabnis, A. and Shetty, A., 2022. Antimicrobial edible films and coatings based on N, O-carboxymethyl chitosan incorporated with ferula asafoetida (Hing) and adhatoda vasica (Adulsa) extract. *Advances in Materials and Processing Technologies*, *8*(3), pp.2699-2715.

50. M. Rele and D. Patil, "Revolutionizing Liver Disease Diagnosis: AI-Powered Detection and Diagnosis", *International Journal of Science and Research (IJSR)*, 2023.https://doi.org/10.21275/SR231105021910
51. Sateesh Reddy Adavelli, "AI and Cloud Synergy in Insurance: AWS, Snowflake, and Guidewire's Role in DataDriven Transformation", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Volume 12, Issue 6, June 2023.
52. Sunil Kumar Suvvari, 2024. "Ensuring Security and Compliance in Agile Cloud Infrastructure Projects," International Journal of Computing and Engineering, CARI Journals Limited, vol. 6(4), pages 54-73.
53. Vinay Panchal, 2025. "Designing for Longer Battery Life: Power Optimization Strategies in Modern Mobile SOCS", International Journal of Electrical Engineering and Technology (IJEET) Volume 16, Issue 1, January-February 2025, pp. 1-17, Article ID: IJEET_16_01_001 Available online at https://iaeme.com/Home/issue/IJEET?Volume=16&Issue=1
54. Sateesh Reddy Adavelli, Nivedita Rahul, "*Personalized P&C Policies: Leveraging Big Data and Machine Learning to Tailor Insurance Coverage for Individual Risk Profiles*", International Journal of Innovative Research in Computer and Communication Engineering, Volume 11, Issue 3, March 2023.