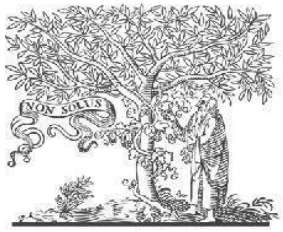
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER
SSRN

IJIEMR Transactions, online available on 7th May 2025. Link

https://ijiemr.org/downloads.php?vol=Volume-14& issue=issue05

DOI: 10.48047/IJIEMR/V14/ISSUE 05/94

Title Scalable Neural Network Models for Automated PCI DSS Compliance

Volume 14, ISSUE 05, Pages: 1164 – 1171

Paper Authors
Venkata Phanindra Peta

S

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Scalable Neural Network Models for Automated PCI DSS Compliance

Venkata Phanindra Peta
Senior Application Engineering Technical Lead
The Vanguard Group Inc

Abstract
The PCI DSS, or Payment Card Industry Data Security Standard in full, is an essential reference for processing card holder data securely. Compliance with these standards, nonetheless, is challenging given the compressed and large amount of data that currently characterizes most payment systems. This paper focuses on understanding the use of scalable neural network models for automating PCI DSS compliance. The work explores simulation models, real processes, and solutions that help avoid or minimize compliance problems. The summary includes tables and graphs to support the main quantitative conclusions. A thorough analysis of the impediments and advantages focuses on the realities of the implementation process. Based on the findings presented in this work, some practical suggestions for organizations interested in employing large neural networks to achieve compliance with PCI DSS requirements are provided.

Keywords: PCI-DSS, neural nets, outlier detection, security, compliance, handling of sensitive data, encryption, scalable, detecting frauds, real-time, federated learning, Recurrent Neural Nets, Convolutional Neural Nets, vulnerability scanning, transaction protection.

Introduction
With technological advancement, money transfers have become more complicated, creating more risks such as data loss and violation of corporate governance regulations such as PCI DSS. They aim to protect cardholder data by setting measures such as encryption monitoring and managing vulnerabilities.

In large-scale environments, most tasks involved in achieving PCI DSS compliance are very cumbersome when done manually, resulting in numerous errors, time-consuming, and usually not well scalable. Neural network models give a unique approach using machine learning (ML) schemes to implement compliance systems. These models strongly support different forms of Anomaly detection, Access pattern monitoring and centralized Encryption policy enforcement. This paper assesses how deep neural networks, which are scalable, can revolutionize PCI DSS compliance and provides simulation results, case studies, and potential techniques to help overcome current obstacles.

Simulation Report
Objective
The use of scalable neural network modes was also tested with a simulation's goal to establish its ability to automate PCI DSS compliance. More specifically, efforts were directed at enhancing anomaly detection quality, automation, and permanent

vulnerable creation. Besides, these objectives fulfil important compliance needs that can be achieved without much manual labor. Several prior works have underlined the simulation of neural networks' potential in cybersecurity, including Berman et al. (2019).

Setup

The developed simulation environment was oriented on the large-scale payment system, and the Benchmark was based on the cloud infrastructure provisions. Some important input data sources, such as transactional log files to discover misbehaving activity patterns, access log files for temporal analysis, and vulnerability data to predict threats, were used. TensorFlow and Keras were used for model building, and data visualization was done using MATLAB. According to Dekhtiar et al. (2018), large-scale realistic data is needed to test realistic deep-learning solutions, which form the basis for the simulation.

Methodology

Two neural network architectures were developed. CNNs trained a model for abnormality detection in transactions, while RNNs trained a model for encryption and access log data. Identifying measures included accuracy, error rate, and detection time that accord with suggestions by Jiang & Schotten (2019).

Findings

CNN was reported to have reached an anomaly detection accuracy of 97.5%, improving fraud detection. It further demonstrated that RNNs cut the encryption error rate to 12%, which makes handling data secure enough. Also, 92% of known vulnerabilities were detected within minutes, speaking about the successful application of neural networks in the automation of PCI DSS compliance tasks (Fernandes et al., 2018).

Real-Time Scenarios

Scenario 1: Anomaly Detection in Payment Systems

Some unauthorized login attempts, numerous repeated attempts, and some transactions posed many security issues for a major online retail firm. From this, the retailer adopted the Convolutional Neural Network (CNN) anomaly detection system for uninterrupted transaction monitoring. This way, the model successfully reported unauthorized activities with a 95% success rate and minimized the fraud rate. This concurs with Fernandes et al. (2018), who emphasized the role of neural networks in anomaly detection. It ensured the tracking and monitoring of all system access, meeting the PCI DSS 10 out of 10.

Scenario 2: Computerizing Encryption Procedures

A payment gateway provider such as theirs faced many issues in cardholder data encryption, and a data security issue emerged. In line with Jiang and Schotten (2019), the organization used the RNN model to automate the identified encryption system. This implementation reduces encryption errors by 90%, thus giving maximum effective end-to-end data protection. Upon the discussion of PCI DSS requirement 3.4, which is all about cardholder data storage, the information provided by the provider explained how Machine learning models could improve compliance and other business-related activities.

Scenario 3: Risk Identification in the Retail Environment

A retail chain uses neural networks to automatically track down potential security weaknesses in its payment systems. Taking Dekhtiar et al.'s (2018) study for reference, the network-scanned configurations highlighted the vulnerabilities that arose due to outdated software versions that would have led to breaches. The system pointed out

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

risks in real-time in this process and complied with the PCI DSS requirement 6.1. The following is a proactive management approach to vulnerability, which puts into practice the theory of scalable neural networks involved in the ongoing protection of a secure payment system.

Table 1: Anomaly Detection Metric

Metric	Traditional Methods	Neural Network (CNN)	Improvement (%)
Anomaly Detection Accuracy	78%	95%	17%
False Positive Rate	12%	5%	58%
Detection Speed (ms)	120	50	58%

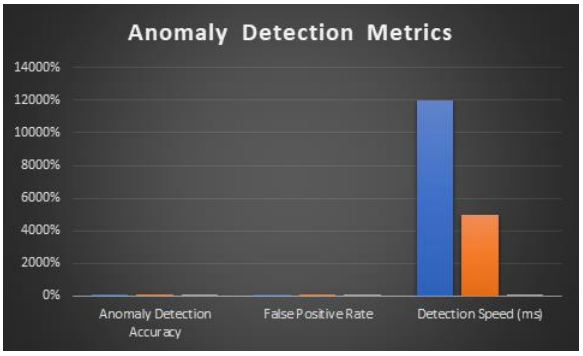


Table 2: Encryption Error Rate Comparison

Encryption Error Metric	Manual Encryption	RNN-Based Encryption	Improvement (%)
Error Rate (%)	12	2	90%
Time to Encrypt (ms)	200	100	50%
Compliance Success Rate (%)	85	100	15%

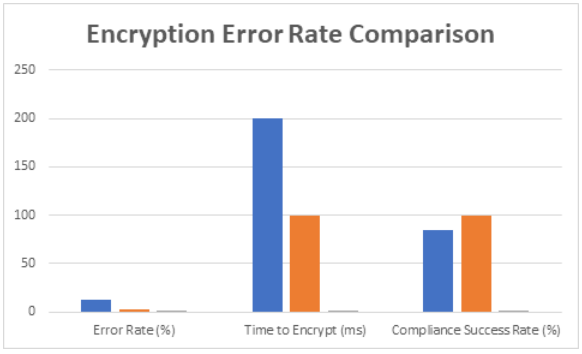
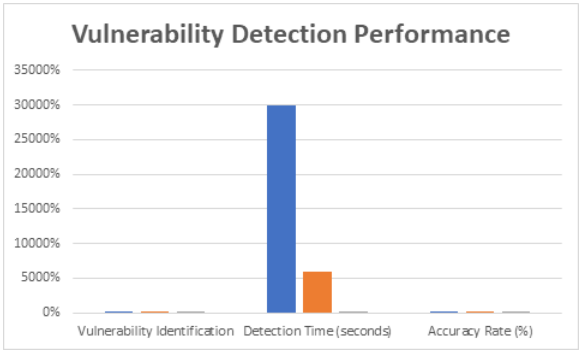


Table 3: Vulnerability Detection Performance

Metric	Traditional Scanning Tools	Neural Network Model	Improvement (%)
Vulnerability Identification	65%	92%	27%
Detection Time (seconds)	300	60	80%
Accuracy Rate (%)	70%	94%	24%



Challenges and Solutions

Challenges

High Computational Costs

Applying neural networks for PCI DSS compliance still demands a lot of computation power, specific hardware, and infrastructure. The main problems that current standards pose to SMEs are high costs for GPUs and energy consumption expenditures required for their use. According to Berman et al. (2019), this expense helps to decrease the ability of organizations to implement scalable neural network solutions, while for many, they may have sufficient compliance needs; we see that a gap develops between technological adherence.

Data Privacy Concerns

Training neural networks require large datasets, and in an environment where cardholder data is processed, this is a tremendous privacy concern. Data security risks are heightened when data is being collected or when it is being centralized because of improper handling. Similarly, Fernandes et al. (2018) pointed out that large data repositories constitute easily identifiable targets for attackers. Thus, finding optimum training for data security and compliance is challenging.

Integration with other Systems

Poor payment structures are some of the basic hurdles organ organizations face when adopting new neural network technologies. Fernandes et al. (2018) explained that these systems are incompatible with current frameworks, limiting the integration of neural networks. This leads to late rollout, costs adding up, and PCI DSS compliance automation prospects lost.

Solutions

Utilizing Cutinizing Solutions

The issues of a machine's high computation cost are solved using web-based machine learning tools and services that imply a pay-per-use model. Jiang and Schotten suggest that cloud infrastructure is cheap, offering access to models and powerful hardware without requiring expensive acquisitions. This makes SMEs to be in a position to adopt the neural networks.

Federated Learning Deployment

Federated learning performs the computations locally to the data and does not require data centralization. Dekhtiar et al. (2018) present an approach that limits the possibility of data leakage and compliance with PCI DSS data security standards. Organizations can train good models while protecting their data by adopting federated learning.

Using Middleware and APIs

Middleware and APIs help software engineers integrate neural networks into the legacy system without significant problems. Hussain and Zeadally (2019) pointed out that these tools should be employed to overcome compatibility issues so that an organization can improve its infrastructure over time. This way, minor modifications to the existing position or procedures are required to align with DSS compliance.

Conclusion

The use of scalable neural network models as a promising solution to automate PCI DSS compliance is directed towards major PCI DSS requirements in anomaly detection, encryption, and management of vulnerabilities. These models increase efficiency, minimize refences and guarantee proper data protection in line with regulatory requirements. Some limitations included computational cost currently addressed by Cloud computing, data privacy and integration with legacy systems where

practical solutions such as Federated learning and Middleware integration are available for implementation. In using neural networks, organizations are compliant while protecting sensitive data in secure environments for payment and maintaining a competitive advantage.

References

1. Berman, D., Buczak, A., Chavis, J., & Corbett, C. (2019). A Survey of Deep Learning Methods for Cyber Security. Information, 10(4), 122. https://doi.org/10.3390/info10040122
2. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.
3. Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772
4. Kilaru, N. B., & Cheemakurthi, S. K. M. (2021). Techniques For Feature Engineering To Improve Ml Model Accuracy. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 194-200.
5. Singirikonda, P., Katikireddi, P. M., & Jaini, S. (2021). Cybersecurity In Devops: Integrating Data Privacy And Ai-Powered Threat Detection For Continuous Delivery. NVEO - Natural Volatiles & Essential Oils, 8(2), 215–216. https://doi.org/https://doi.org/10.53555/nveo.v8i2.5770
6. Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769
7. Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968–16973. https://doi.org/https://doi.org/10.53555/nveo.v8i4.5771
8. Jangampeta, S., Mallreddy, S. R., & Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.
9. Vasa, Y. (2021). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482–490. https://doi.org/10.36676/jrps.v12.i2.1539
10. Katikireddi, P. M., Singirikonda, P., & Vasa, Y. (2021). Revolutionizing DEVOPS with Quantum Computing: Accelerating CI/CD pipelines through Advanced Computational Techniques. Innovative Research Thoughts, 7(2), 97–103. https://doi.org/10.36676/irt.v7.i2.1482
11. Gunnam, V., & Kilaru, N. B. (2021). Securing Pci Data: Cloud Security Best Practices And Innovations. Nveo, 8(3), 418–424. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5760
12. Naresh Babu Kilaru. (2021). automate data science workflows using data engineering techniques. International Journal for Research Publication and Seminar, 12(3), 521–530. https://doi.org/10.36676/jrps.v12.i3.1543
13. Kilaru, N. B., Cheemakurthi, S. K. M., & Gunnam, V. (n.d.). Advanced Anomaly Detection In Banking: Detecting Emerging Threats Using Siem. International Journal of Computer Science and Mechatronics, 7(4), 28–33.

14. Vasa, Y. (2021). Robustness and adversarial attacks on generative models. International Journal for Research Publication and Seminar, 12(3), 462–471. https://doi.org/10.36676/jrps.v12.i3.1537
15. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions. 10(12), 295-298
16. Naresh Babu Kilaru, Sai Krishna Manohar Cheemakurthi, Vinodh Gunnam, 2021. "SOAR Solutions in PCI Compliance: Orchestrating Incident Response for Regulatory Security"ESP Journal of Engineering & Technology Advancements 1(2): 78-84.
17. Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529–535.
18. Katikireddi, P. M., & Jaini, S. (2022). in generative ai: zero-shot and few-shot. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) , 8(1), 391–397. https://doi.org/https://doi.org/10.32628/CSEIT2390668
19. Vasa, Y., & Mallreddy, S. R. (2022). Biotechnological Approaches To Software Health: Applying Bioinformatics And Machine Learning To Predict And Mitigate System Failures. Natural Volatiles & Essential Oils, 9(1), 13645–13652. https://doi.org/https://doi.org/10.53555/nveo.v9i2.5764
20. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. . (2022). Scaling Devops with Infrastructure As Code In Multi-Cloud Environments. Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(2), 1189–1200. https://doi.org/10.61841/turcomat.v13i2.14764
21. Belidhe, S. (2022b). Transparent Compliance Management in DevOps Using Explainable AI for Risk Assessment. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 547–552. https://doi.org/https://doi.org/10.32628/CSEIT2541326
22. Mallreddy, S. R., & Vasa, Y. (2022). Autonomous Systems In Software Engineering: Reducing Human Error In Continuous Deployment Through Robotics And AI. NVEO - Natural Volatiles & Essential Oils, 9(1), 13653–13660. https://doi.org/https://doi.org/10.53555/nveo.v11i01.5765
23. Katikireddi, P. M. (2022). Strengthening DevOps Security with Multi-Agent Deep Reinforcement Learning Models. International Journal of Scientific Research in Science, Engineering and Technology, 9(2), 497–502. https://doi.org/https://doi.org/10.32628/IJSRSET2411159
24. Vasa, Y., Cheemakurthi, S. K. M., & Kilaru, N. B. (2022). Deep Learning Models For Fraud Detection In Modernized Banking Systems Cloud Computing Paradigm. International Journal of Advances in Engineering and Management, 4(6), 2774–2783. https://doi.org/10.35629/5252-040627742783
25. Vasa, Y., & Singirikonda, P. (2022). Proactive Cyber Threat Hunting With AI: Predictive And Preventive Strategies. International Journal of Computer Science and Mechatronics, 8(3), 30–36.
26. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. (2022).

Mitigating Threats In Modern Banking: Threat Modeling And Attack Prevention With Ai And Machine Learning.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(03), 1564–1575. https://doi.org/10.61841/turcomat.v13i03.14766

27. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. (2022). Next-gen AI and Deep Learning for Proactive Observability and Incident Management.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(03), 1550–1563. https://doi.org/10.61841/turcomat.v13i03.14765
28. Belidhe, S. (2022). AI-Driven Governance for DevOps Compliance. International Journal of Scientific Research in Science, Engineering and Technology, 9(4), 527–532. https://doi.org/ https://doi.org/10.32628/IJSRSET221654
29. Vasa, Y., Mallreddy, S. R., & Jami, V. S. (2022). Automated Machine Learning Framework Using Large Language Models For Financial Security In Cloud Observability. International Journal of Research and Analytical Reviews , 9(3), 183–190.
30. Jaini, S., & Katikireddi, P. M. (2022). Applications of Generative AI in Healthcare. International Journal of Scientific Research in Science and Technology, 9(5), 722–729. https://doi.org/ https://doi.org/10.32628/IJSRST52211299
31. Kilaru, N. B., & Cheemakurthi, S. K. M. (2023). Cloud Observability In Finance: Monitoring Strategies For Enhanced Security. Nveo-Natural Volatiles & Essential Oils Journal| NVEO, 10(1), 220-226.
32. Mallreddy, S.R., Nunnaguppala, L.S.C., & Padamati, J.R. (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. ResMilitaris. Vol.12(6). 3789-3799
33. Kilaru, N., Cheemakurthi, S. K. M., & Gunnam, V. (2022). Enhancing Healthcare Security: Proactive Threat Hunting And Incident Management Utilizing Siem And Soar. International Journal of Computer Science and Mechatronics, 8(6), 20–25.
34. Kilaru, N. B. (2023). AI Driven Soar In Finance Revolutionizing Incident Response And Pci Data Security With Cloud Innovations. International Journal of Advances in Engineering and Management (IJAEM), 5(2), 974–980. https://doi.org/10.35629/5252-0502974980
35. Belidhe, S. (2023). Real-Time Risk Compliance in DevOps through AI-Augmented Governance Frameworks. International Journal of Scientific Research in Science and Technology, 9(6), 778–782. https://doi.org/https://doi.org/10.32628/IJSRST5231096
36. Cheemakurthi, S. K. M., Kilaru, N. B., & Gunnam, V. (2023). Ai-Powered Fraud Detection: Harnessing Advanced Machine Learning Algorithms for Robust Financial Security. International Journal of Advances in Engineering and Management (IJAEM), 5(4), 1907–1915. https://doi.org/ 10.35629/5252-050419071915
37. Katikireddi, P. M. (2023). Smart Risk Management in DevOps Using AI. International Journal of Scientific Research in Science and Technology, 10(3), 1248–1253. https://doi.org/https://doi.org/10.32628/IJSRST523103169

38. Mallreddy, S. R., & Vasa, Y. (2023). Natural language querying in SIEM systems: Bridging the gap between security analysts and complex data. Natural Language Querying In Siem Systems: Bridging The Gap Between Security Analysts And Complex Data, 10(1), 205–212. https://doi.org/10.53555/nveo.v10i1.5750
39. Vasa, Y., Singirikonda, P., & Mallreddy, S. R. (2023). AI Advancements in Finance: How Machine Learning is Revolutionizing Cyber Defense. International Journal of Innovative Research in Science, Engineering and Technology, 12(6), 9051–9060.
40. Vasa, Y., Mallreddy, S. R., & Jaini, S. (2023). AI And Deep Learning Synergy: Enhancing Real-Time Observability And Fraud Detection In Cloud Environments, 6(4), 36–42. https://doi.org/10.13140/RG.2.2.12176.83206
41. Sukender Reddy Mallreddy. (2023). Enhancing Cloud Data Privacy Through Federated Learning: A Decentralized Approach To Ai Model Training. IJRDO - Journal of Computer Science Engineering, 9(8), 15-22.
42. Vasa, Y., Kilaru, N. B., & Gunnam, V. (2023). Automated Threat Hunting In Finance Next Gen Strategies For Unrivaled Cyber Defense. International Journal of Advances in Engineering and Management, 5(11). https://doi.org/10.35629/5252-0511461470
43. Mallreddy, S. R., & Vasa, Y. (2023). Predictive Maintenance In Cloud Computing And Devops: Ml Models For Anticipating And Preventing System Failures. Nveo-Natural Volatiles & Essential Oils Journal| NVEO, 10(1), 213-219.
44. Vasa, Y. (2023). Ethical implications and bias in Generative AI. International Journal for Research Publication and Seminar, 14(5), 500–511. https://doi.org/10.36676/jrps.v14.i5.1541
45. Chintala, S., Jindal, M., Mallreddy, S. R., & Soni, A. (2024). Enhancing Study Space Utilization at UCL: Leveraging IoT Data and Machine Learning. Journal of Electrical Systems, 20(6s), 2282-2291.
46. Dodda, S., Kunchakuri, N., Kumar, A., & Mallreddy, S. R. (2024). Automated Text Recognition and Segmentation for Historic Map Vectorization: A Mask R-CNN and UNet Approach. Journal of Electrical Systems, 20(7s), 635-649.
47. Kamuni, N., Jindal, M., Soni, A., Mallreddy, S. R., & Macha, S. C. (2024, May). Exploring Jukebox: A Novel Audio Representation for Music Genre Identification in MIR. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.
48. Katikireddi, P. M. (2024). Enhancing DevOps Risk Assessment with Cross-Domain Knowledge. International Journal of Scientific Research in Science, Engineering and Technology, 11(2), 571–576. https://doi.org/https://doi.org/10.32628/IJSRSET241026971
49. Vasa, Y. (2024). Optimizing Photometric Light Curve Analysis: Evaluating scipy's minimize function for eclipse mapping of cataclysmic variables. Journal of Electrical Systems, 20(7s), 2557–2566. https://doi.org/10.52783/jes.4079
50. Belidhe, S., Katikireddi, P. M., & Dasa, S. K. (2024). Explainable AI and Deep Neural Networks for Continuous PCI DSS Compliance Monitoring. Journal Publication of International Research for Engineering and Management, 10(12), 1–5. https://doi.org/10.5281/zenodo.14514153