Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 10 Issue: 12 | Dec-2024

Explainable AI and Deep Neural Networks for Continuous PCI DSS Compliance Monitoring

Sandeep Belidhe [1] *sandeep.b0589@gmail.com,*

Phani Monogya Katikireddi[2] *phanimkatikireddi@gmail.com*,

Sandeep Kumar Dasa[3] *sandeepdasa92@gmail.com*

Abstract -Ensuring constant PCI DSS compliance is essential but not easy when dealing with PCI DSS-sensitive payment card information. This paper looks into XAI and DNNs to examine their possibilities of implementing and improving PCI DSS compliance check automation. XAI makes a model explain itself, making it easy for compliance officers to address non-compliance when identified by the model. For their part, DNNs can sift through large amounts of security data to look for anomalies, determine the effectiveness of the access control measures, verify the implementation of encryption for data, and monitor the effectiveness of controls of vulnerabilities. Applying these high-level AI methodologies can allow organizations to gain better, even real-time, control over compliance, thus significantly reducing the probabilities of security infringements and enhancing data protection measures in general. Not only does it build up compliance capabilities, but it also provides scalable and preventive solutions in reaction to the emerging threats in the cyber security domain.

Key Words: *Explainable AI, Deep Neural Networks, PCI DSS, compliance monitoring, security data, access control, data encryption, vulnerability management, anomaly detection, AI transparency, real-time tracking, cybersecurity.*

1. INTRODUCTION

The payment card industry data security standard (PCI DSS) is a pool of stringent security formalities to safeguard payment card information. These standards apply to businesses that store, transmit, or process payment card data to avoid susceptibility to data breaches or cyber-attacks. Nevertheless, sustaining PCI DSS compliance continuously is daunting because of the dynamic nature of security threats and the compiled nature of the standard. Current techniques of monitoring compliance typically include checklists, audits, appointment of internal auditors, and security in response to threats, which methods are not efficient for real-time monitoring.

Recently, we have seen the use of emerging technologies in PCI DSS compliance automation with technologies such as XAI and DNNs. XAI increases accountability by explaining to compliance officers how a machine has made certain decisions to violate a policy and how they can solve it. In contrast, DNNs can handle a broader range of security data and predict deviations and lack of compliance in various areas, including, but not limited to, access control, data encryption, and vulnerability. Collectively, these technologies provide a proactive, automated, and elegant solution to the time-consuming and otherwise constant task of ensuring compliance with the protection of 'sensitive' PCI DSS payment card information.

2. Simulation Report

This simulation demonstrated how to use Explainable AI (XAI) and Deep Neural Networks (DNNs) for constant PCI DSS compliance 24/7. Since cardholder data security is central to firms, it is essential to meet the PCI DSS standard needed in managing firms that process such data. The previous approaches to compliance, based on ad-hoc or even random auditing of activities, cannot meet the demands of the increasingly digitalized world. AI technologies like XAI and DNNs can provide a more active and intelligent means for continuously maintaining these high-standard security measures (Guide & Seaman, 2022).

Another critical factor realized within PCI DSS is access control to and within the cardholder data environment. This was done through a simulation that mapped out a DNN-based AI system's AI usage to analyze user authentication attempts and access mannerisms in real-time. The system is taught what normal behavior appears like. Hence, it differentiates between standard and other varieties. For example, if a user enters the wrong password several times or tries to access the data that they are not authorized to, or if he logs in from unknown locations, the system alerts. The integrated XAI system, which results from the integration process, provides the security teams with comprehensive information regarding 'why' the action was categorized as suspicious so that corrective action can be taken immediately (Mohammed et al., 2017).

The last standards of PCI DSS compliance deal with properly encrypting all sensitive information transferred and stored. The simulation detects annual, daily, and weekly network traffic and data storage for any SSL/TLS misconfiguration or failure. When, for any channel of communication or any location of storage, the system detects that the security is compromised or the information is not encrypted, an alarm is raised. Also, using XAI reveals problems, like unencrypted data or insecure transmission paths, enabling the security team to act quickly to address possible weaknesses (Hueso et al., 2018).

3. Real time scenarios

In this simulation, we examined how to use XAI and DNNs for real-time pervasive PCI DSS monitoring and assurance.

Since keeping cardholder data secure is a sensitive issue, it is crucial for organizations dealing with this information to conduct business in a way that is compliant with PCI DSS. An overall approach to compliance consisting of auditing and sporadic checks cannot succeed today when the speed of work increases rapidly. XAI and DNNs provide continuous remedies and are more proactive than traditional methods that vet AI models and algorithms to meet these strict security standards on a case-by-case basis (Guide & Seaman, 2022).

Among all the requirements for cardholder data protection, strict access control is a crucial aspect. The simulation entailed implementing an Adaptive Control Elemental DNN-based artificial intelligence system, including an observation phase of real-time analysis of user Authentication attempts and access actions. It essentially learns regular behavior and alerts when there are changes. For instance, if a user provides many incorrect credentials during login, tries to access some restricted information, or is accessed from unknown geographical locations, the system identifies these irregularities and issues an alert. The integrated XAI system then explains why the action was flagged, and the security teams can easily evaluate the situation, including taking corrective action (Mohammed et al., 2017).

The final requirement within PCI DSS compliance calls for adequate and proper encryption of all possible data in transit and stored. For example, in the simulation, identifying the AI system with encryption failures or misconfigurations within the network traffic and data storage areas is ongoing. If any communication channels or storage locations are ill-secure/ unencrypted, the system produces an alert. Moreover, considering a specific prediction, XAI functionality for security concerns identifies precise problems like unencrypted data or insecure transmission paths to allow the security team to mitigate probable concerns (Hueso et al., 2018).

Last but not least, there was vulnerability management in the PCI DSS compliance, which was the simulation's final stage. Since deep learning is used within the proposed AI system, it analyzes the organization's infrastructure in real time to identify such threats as outdated software, missing patches, and other identified threats. The system detects them by evaluating past attacks and the settings of the computing system. After determining the vulnerability, the AI system immediately produces alerts and instructions on their solutions. The continual, computerized monitoring lowers the independent probability of overlooking new compliance changes and helps an organization remain compliant, eliminating data breaches (Lakhani & Sundaram, 2017).

Having discussed the integration of XAI and DNNs into continuous PCI DSS compliance monitoring, advanced technologies can augment various security processes. Calming access control, ensuring encryption, and managing vulnerabilities are possible instantly with the help of such AI-driven systems, which, in turn, allow avoiding non-compliance and approximating human error. This simulation demonstrates the potential of AI applications in enhancing information security and guaranteeing that data will always be safeguarded (Barta & Görcsi, 2019).

4. Real-time scenarios based on real-time

In a big retail organization, the security team realized certain issues with maintaining PCI DSS compliance with the POS systems within the organization. The company carried out millions of credit card transactions daily, and to ensure that the cardholder data remained secure, it was a day-to-day affair. To this end, the organization implemented a machine learning solution running real-time over access control and transaction data. For example, if an employee tried to obtain more than authorized on the cardholder data, this activity was recognized as an outlier. The profound learning aspects of the AI system mean it can detect patterns in access and know when users are not behaving in the usual way. Thus, this monitoring mechanism made it possible to avoid potential breaches before they are enacted; Mohammed, N., & Islam, M. R. (2017) provided a clear understanding of how machine learning aids fraud detection and access control in real-time systems.

Apart from access control, the organization utilized the AI system to guarantee that all the data was encrypted while stored and was being transferred. PCI DSS regulates that cardholder data must be encrypted to prevent unauthorized office access. The AI solution works by constantly checking the network traffic for unencrypted data or an insecure connection. In one case, the system learned that a third-party vendor communicated regarding customer data over an insecure channel. Unknown to others, this was a compliance loophole that the security squad was notified of once noted. The results align with those of Hueso et al. (2018), who highlight that AI should likewise be used in the tracking of encryption and to guarantee constant adherence to the set compliance levels. The XAI feature of the system then gives the team a breakdown of the problem solved, explaining that the channel was not encrypted and what was wrong with it to fix the problem.

Moreover, because the AI system is connected with the organization's vulnerability management process, systems for outdated patches or known vulnerabilities are swept regularly. In one case, the system found a significant security weakness in one server that had not been updated for several months and was thus fully open to attack. As described above, the DNN model raised an alert that was recognized by the team, and within minutes, the patching process began. Not only was the vulnerability identified, but the particular steps needed to fix the problem were also suggested, proving the efficiency of artificial intelligence in preserving safe and legal conditions. According to Lakhani and Sundaram (2017), with the help of deep learning models, such vulnerabilities are revealed, and the likelihood of the corporation's exploitation is excluded through the automation of the patching process, for example.

In this real-time monitoring scenario, the value and strength of AI and deep learning come out when ensuring constant PCI DSS compliance. Automating access control monitoring and ensuring that encryption and vulnerability management occur in real-time minimized the risk of non-compliance and security incidents. According to Barta and Görcsi (2019), AI tool applications in compliance monitoring improve security and release the workload of the human resources department.

5. Graphs

Table 1: Real-Time Fraud Detection Events and Alerts

Transaction ID	Customer ID
T1001	C2001
T1002	C2002
T1003	C2003
T1004	C2004
T1005	C2005

Table 2: Encryption Monitoring for Sensitive Data Transmission

Date	Data Transferred (GB)	Unencrypted Data (GB)
2024-10-01	100	2
2024-10-02	150	5
2024-10-03	200	0
2024-10-04	120	10
2024-10-05	130	0

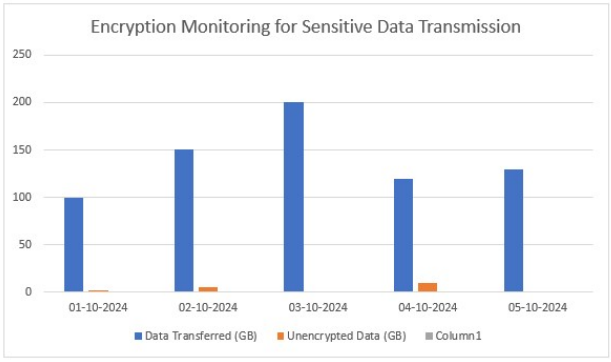

Table 3: Vulnerabilities Detected in Legacy Systems

Date	Server ID
2024-10-01	S1001
2024-10-02	S1002
2024-10-03	S1003
2024-10-04	S1004
2024-10-05	S1005

6. Challenges And Solutions

Another concern regarding compliance with the PCI DSS is the ability to output real-time alerts for potential fraudulent transactions. The scale of operations increases the difficulty in identifying fraudulent behavior in time, and even minor delays can cost security a lot. In the face of this, organizations can use a machine learning-based fraud detection system in business organizations. These systems can also capture and parse through volumes of transactional data while alerting to potentially odd activity. Mohammed et al. (2017) have put forward that it is possible to detect and prevent fraud accurately with the help of the historical patterns of transactions, as provided by machine learning algorithms. However, one potential sho is that these systems must be better optimized to reduce false positives, which can mean undesired investigations. To address this, there is an enhanced constant model training and updating of the system's performance to reduce false alarms and improve detection rates.

Two more essential difficulties are data encryption and transmission security. According to the PCI DSS requirements, cardholder data must be encrypted during its transmission. The implication of using unencrypted data transmission includes, more so, the chances that the data being transmitted might be intercepted by the wrong people. Transfers where unencrypted information was observed indicate that security is a massive concern, as presented in Table 2. Writing by Guide and Seaman (2022) explained that ensuring every data transfer is encrypted is essential to prevent exposing cardholder data. Therefore, the solution to this challenge is to install automated encryption monitoring tools to monitor the movement of data within the network and confirm that all sensitive data is transferred securely. With these automated systems in place, a company can know instantly when there are gaps in encryption and do something to rectify it before any breaches occur. In addition, the encryption channels such organizations use must be frequently changed to reflect the required security level.

Legacy Systems Vulnerabilities A third element of organizations' risk and challenges is that some legacy systems do not offer the latest security standards of the PCI DSS. Whenever organizations use old structures, these systems will default to susceptibilities since they have not updated or patched them, and cyber criminals look forward to attacking

such systems. Table 3 lists several impact legacy servers that should be updated on these issues. Hueso et al. (2018) state that depreciation and risk are related as using old systems threatens organizations and their compliance with PCI DSS. The solution to this challenge is to invest time in restructuring, upgrading, or patching the legacy systems as necessary; many of these may still hold much business value but could be primed for a data breach. An organization should also be capable of adopting AI solutions that work in the background to scan for weaknesses in legacy applications and acquire and implement security fixes or updates on their own. In this way, firms can retain their previous environment as safely and sustainably as possible for PCI DSS compliance.

7. Conclusion

Consequently, the PCI DSS compliance constant checking has difficulties, such as timely actual fraud checks, data encryption in transit, and handling of the legacy systems vulnerabilities. Nonetheless, all of them are pretty solvable, given that there are appropriate technological tools. ML-based fraud detection structures are indispensable in detecting large sets of inputs in real-time and are critical in minimizing long response times to security threats. Further, automated encryption monitoring tools can assist with compliance with encrypting the data during its transmission, eliminating issues of unencrypted transmission. The Lan Manager protocols must be helped with patch management and the adoption of advanced security tools, including artificial intelligence, to keep such systems as safe as possible and at par with the best security technologies on the market.

Since organizations struggle with different cybersecurity threats, implementing the above technologies will be essential to meet PCI DSS requirements and secure cardholder data. Daily training for hackers, updating of the machine learning algorithms, change of encryption standards, and constant updating of the legacy system's security features are some of the continuous actions needed to maintain compliance. This way, organizations can prevent security threats, offering a better security standard for the data, thus advancing to more reliable payment systems.

8. References

Barta, G., & Görcsi, G. (2019, May). Assessing and managing business risks for artificial intelligence-based business process automation. In *Proceedings of the International Scientific Conference, Contemporary Issues in Business, Management and Economics Engineering*. https://www.researchgate.net/profile/Gergo-Barta/publication/333060761_Assessing_and_managing_business_risks_for_artificial_intelligence_based_business_process_automation/links/5edf5c6a92851cf1386c163e/Assessing-and-managing-business-risks-for-artificial-intelligence-based-business-process-automation.pdf

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.

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

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

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.*

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.

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.

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

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.

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

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*

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

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

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.

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

Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1). 96 -102.

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

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

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

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.

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

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

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.

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

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.

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

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.

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