International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Holistic Review of PCI Security Standards Framework for Customer Relationship Management (CRM) Software

Srinivas Chippagiri

Submitted:14/03/2024 **Revised**: 29/04/2024 **Accepted**: 06/05/2024

Abstract: Payment Card Industry Data Security Standard (PCI-DSS) a set of security standards developed as a cooperative effort among card issues. Customer Relationship Management (CRM) software must be PCI DSS complaint in order to properly address security of customer payment data. Given that more and more organizations have become victims of data breaches and cyberattacks, CRM systems that regularly process, store, and transfer payment card data must meet the standards set by the PCI DSS guidelines. This article provides a complex overview of the PCI security requirements, including their relevance to and fitness for CRM software. This work aims to explain the functions of different areas of the PCI DSS as well as data encryption, access control, network security, and the part of security audit on the compliance level. The paper also analyses the specific difficulties businesses experience when it comes to achieving PCI compliance in CRM systems: the listed problems include high costs of implementation, complicated legislation, and constant monitoring processes. It also gives recommendations on what can be done in practice, including using secure APIs, tokenization, or assigning risk assessments at the stages of creating and updating CRMs. The need to be PCI compliant with respect to the protection of sensitive data, avoiding fines, gaining customer trust and staying competitive is discussed. This comprehensive analysis reemphasizes the call for the incorporation of PCI DSS standards into CRM software solutions for the improvement of security, protection of customer information, and addressing compliance requirements in the rapidly growing e-business environment.

Keywords: *Overview of Payment card industry (PCI), PCI Requirement, CRM software, challenges.*

1. Introduction

Credit card companies Visa and MasterCard promote a set of rules called the PCI standard in an attempt to make the payment card services sector more secure. The PCI Data Security Requirements are applicable to all Members, merchants, and service providers who store, handle, or transport cardholder data, as stated in the Payment Card Industry Security Audit Procedure document[1]. The goal of both programs was to improve the security of credit card transactions processed by customers, businesses, and any other intermediaries covered by the applicable standard [2]. Best practice recommendations comparable to those of other industry-leading security standards were also made accessible by these endeavours. The differences in the "targeted" audiences that were addressed by Visa and MasterCard were a major distinction between the two programs[3]. Depending on the number of transactions handled, Visa compelled some organisations to conform. [4][5].

To make sure that credit card data is securely processed, stored, and sent, there is a complete set of criteria called the PCI Security Standards Framework. It is especially suitable for the Customer Relationship Management (CRM) software that is used to store customers' information and sometimes even their payment credentials. It is evident that CRM systems are fundamental in today's business processes; they consist of important data about customers and help control interactions with them[6], and therefore are attractive to hackers. To protect such information and avoid security breaches – which inflict significant monetary losses and a company's image – PCI DSS standards must be met. Figure 1 shows the customer relationship management software.

Fig. 1 Customer Relationship Management Software

The principles of PCI DSS act as measures to which CRM systems need to adhere when handling cardholder data. These consist of provisions on encryption, system access, testing and updates in security standards and Architecture for payment card information storage and transfer. By so doing, companies can protect consumer trust, meet legal requirements and reduce risks of experiencing a leakage of

[1] *Sr. Member of Technical Staff, Salesforce Inc, Seattle, USA*
Email: cvas22 [at] gmail [dot] com
ORCID ID: https://orcid.org/0009-0004-9456-3951

their data [7]. Integrating PCI DSS into CRM software may involve implementing security measures such as tokenization and secure authentication protocols, ensuring that all customer

offline.

The following paper are organized as: Section II and III. Overview of Customer Relationship Management (CRM) software in payment and Payments Card Industry Security Standard Frameworks, Section IV provide the Integration Of Payment Card Industry (PCI) in CRM Software, Section V give the Impacts of PCI DSS On CRM Software, Section VI discussed some challenges and solutions of PCI security for CRM, Section VII provide the literature review, Section VIII discussed conclusion of this paper.

2. Overview Of Customer Relationship Management (CRM) Software In Payment

Customer Relationship Management is abbreviated as CRM. The goal of CRM is to create a bond with consumers by learning about their wants, needs, and behaviors. Do research from a distance or methodically approach and engage with clients. CRM will handle client data, including contact details, needs, and transaction history data, to improve customer service management. CRM makes it simple for firms to evaluate and create a list of prospective and devoted clients. Furthermore, CRM manages client complaints and issues in order to establish a fair and sustainable customer service plan. A customer relationship management system is the simplest way to describe CRM. CRM allows for the systematic and normative implementation of a plan to ensure customer satisfaction. Electronic systems benefit from CRM since it aids in controlling, maintaining, and increasing customer satisfaction, which in turn helps to boost revenue. Marketing, sales, and customer service can all be better coordinated with this[8][[9]. In the Payment Card Industry (PCI), CRM software plays a critical role in managing customer data and interactions while ensuring secure payment processing. Due to the high level of compliance expected in the industry, these CRM systems will require suitable security features to respond to the payment information properly. Key Roles in PCI:

- **Data Centralization:** These are systems in PCI that centralize data relating to customers' payments and transactions history/ preferences and help in providing optimal service.
- **Integration with Payment Gateways:** They allow easy and safe payment to be made and this is enhanced by its compatibility with PCI compliant payment platforms.
- **Fraud Prevention and Risk Management:** Marketing communication technologies employed by CRM platforms make use of sophisticated analysis and surveillance mechanisms to provide protection against transaction fraud.
- **Regulatory Compliance:** These systems have to operate under the existing PCI DSS standard – that means that payment data has to be stored, processed, and transferred securely.

A. Role of CRM Software in Payment Processing

CRM also has great significance in today's payment processing as it is the core system used to store, process and organise customer relations, information and financial transactions. CRM systems [10] link with payment processors to ensure users have a favorable experience when entering relevant payments, thus improving the outcomes for such businesses while ensuring data integrity[11]. Key Functions in Payment Processing:

- **Data Management:** CRM software also has to deal with and file customers' personal and often confidential information such as account numbers, purchase records, and preferences necessary for tailored services.
- **Integration with Payment Systems:** Most of the CRM systems actually use external payment gateway so that the payment can be done right within the CRM system's interface.
- **Fraud Prevention:** The tools such as the transaction monitoring, the anomaly detection, the management of secure data ensure the detection of possible fraud risks in CRM.
- **Automation and Efficiency:** Many communications with customers are also handled through CRM, such as automated billing, invoicing, and processing recurrent payments, all of which cuts down on inefficiencies and mistakes.
- **Customer Experience:** By consolidating payment processing with customer management, CRM systems enable businesses to provide a unified and hassle-free experience, enhancing customer satisfaction and loyalty.

3. Overview Of Payments Card Industry Security Standard Frameworks

A functional system that enables merchants to receive payments from customers using payment cards and finish back-end transactions with banks has been created by the Payment Card Industry (PCI). Users, retailers, and financial institutions are the main actors in the ecosystem, and their interconnections are shown in Figure 2. Bank accounts held by the buyer and seller could be different. The issuing bank handles the user's credit or debit card accounts and provides the user with payment cards (step 1). The payment card is

used by users at different kinds of retailers (steps 2, 5, and 7). The merchant receives and routes the transaction information (steps 4, 6, and 8) via an account that is managed by the acquirer bank. After the transaction is finished via the payment network, the acquirer bank makes sure that money is sent to the merchant's account (steps 9 and 10). The payment network, also referred to as the card brands (Visa, MasterCard, etc.), serves as a conduit between the banks that issue the cards and the buyers[12].

Various kinds of traders exist. Merchants that operate an e-commerce service, meaning that all transactions are conducted online, often communicate with the acquirer bank via a payment gateway, such as Square or Stripe, which facilitates payment processing and integration (3). Point-of-sale (POS) devices, also known as payment terminals, are used by retailers with physical shopfronts to gather and send user card data to the acquirer bank. They have the option of using their own POS (5) or the acquirer bank's POS (7). The primary distinction is that acquirer POS does not save the card information inside the retailer; instead, it sends it straight to the bank. However, the card information could be stored in the merchant POS [13].

Mspaint

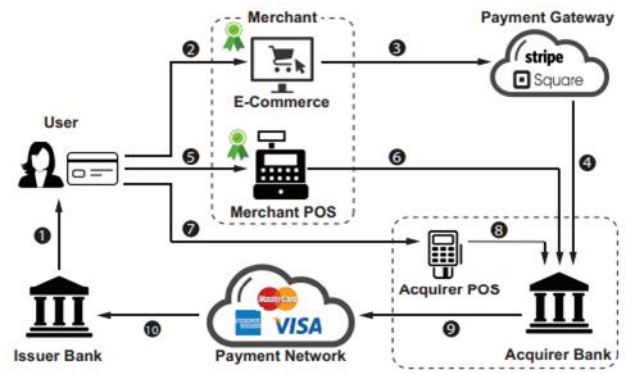

Fig 2. Main actors in the ecosystem

E-commerce websites and merchant POS systems must retain card information, thus merchants must demonstrate to the bank that they are capable of handling information processing securely. To continue having accounts with the acquiring bank, these merchants must get PCI security certificates [15]. The procedure for security certification is then outlined.

A. PCI Council and Data Security Standard

A variety of standards are overseen by the Payment Card Industry Security Standards Council to guarantee data security inside the exceedingly intricate payment environment. Of all the requirements, the only ones that are necessary are the Data Security Standard (DSS) and the Card Production and Provisioning (CPP). Regulation of card issuers and manufacturers is the primary goal of CPP. All systems that accept payments must comply with the Data Security Standard (DSS), which is the most significant specification for issuer banks, acquirer banks, e-commerce sites, and merchants of all kinds. Ensuring compliance with DSS is our main emphasis.

To ensure the safety of customers' credit card information, businesses must adhere to 12 guidelines laid forth in the PCI Data Security Standard specifications. These specifications address a number of topics, including testing, vulnerability management, access control, data protection policies, network security, and people management. The 12 high-level needs include 79 more specific components in total. The levels of potential compliance that are similar to the majority of payment brands are shown in Table I.

TABLE1. PCI Compliance levels and their evaluation criteria.

Level	**Transaction Per Year**	**Compliance Requirements**		
		Self-report with SAQ	***Sec Scans by ASV***	***Sec Audits by QSA***
Level 1	Over 6M	Quarterly	Quarterly	Required
Level 2	1M – 6M	Quarterly	Quarterly	Required/Optional
Level 3	20K – 1M	Quarterly	Quarterly	Not Required
Level 4	Less than 20K	Quarterly	Quarterly	Not Required

All participants in the ecosystem, including issuer/acquirer banks and merchants, are subject to DSS. In order to create a business account with the acquirer bank, merchants must first verify their compliance. The first step is that the PCI security standard council supplies the requirements and the SAQs[16]. Businesses evaluate their own DSS compliance and include the surveys with their reports. The second requirement is that the vendor has to be approved by third-party security organizations like ASVs and QSAs[17].

B. Components of Payment Card Industry

- **PCI Data Security Standard–** Anyone who handles, processes, or transmits information that identifies a cardholder is subject to the PCI DSS. Included or linked to cardholder data are technical and operational system components that are covered. Compliance with the PCI DSS is mandatory for every firm that processes or accepts payment cards.
- **PIN Entry Device Security Requirements–** Payment card industry security standard PCI PED

pertains to companies who design and build terminals that accept PINs for financial transactions.

- **Payment Application Data Security Standard:** Application developers and integrators that handle cardholder data in any way—storage, processing, or transmission—for authorization or settlement purposes are the target audience of the PA-DSS. It also regulates the sale, distribution, or licensing of these apps to other parties[18].
- **PCI Data Security Standard–** Anyone who handles, processes, or transmits information that identifies a cardholder is subject to the PCI DSS. Included or linked to cardholder data are technical and operational system components that are covered. Compliance with the PCI DSS is mandatory for every firm that processes or accepts payment cards[19].
- **PIN Entry Device Security Requirements–** Payment card industry security standard PCI PED pertains to companies who design and build terminals that accept PINs for financial transactions.
- **Payment Application Data Security Standard:** Application developers and integrators that handle cardholder data in any way—storage, processing, or transmission—for authorization or settlement purposes are the target audience of the PA-DSS. It also regulates the sale, distribution, or licensing of these apps to other parties[20].

Figure 3 depicts the Payment Card Industry (PCI) Software Security Framework, a set of guidelines and tools for the safe creation of financial applications. A vital component of the payment transaction flow, payment software security is necessary to enable accurate and dependable payment transactions. The SSF updates the PA-DSS with new criteria that are compatible with more kinds of payment software, as well as different technologies and ways of making software. Developers are given additional leeway to implement payment application security via agile development approaches and rapid update cycles by the SSF's outcome-focused standards[22]. Without sacrificing security, the SSF expedites the delivery of businesses' payment application customization and functionality. Additionally, it enhances the validation assurance for acquirers, merchants, and service providers who oversee the usage of payment solutions by improving transparency and consistency in testing payment applications.

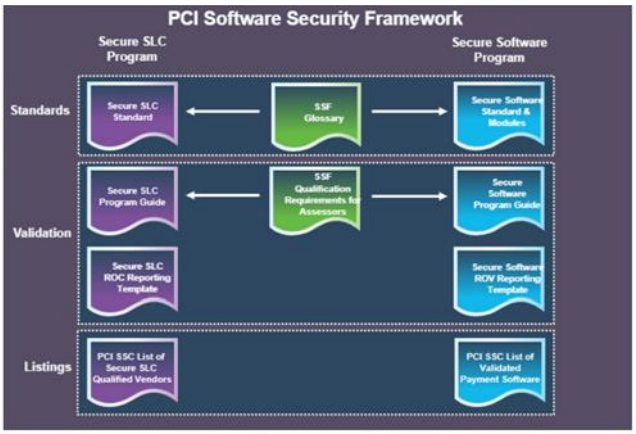

Fig 3. PCI security framework

Introduces a novel method for checking the safety of all types of payment software, including current and future versions. Encourages security-focused training for developers on how to incorporate it into software development processes [20].

4. Integration Of Payment Card Industry(PCI) In CRM Software

The integration of PCI DSS into CRM systems ensures that customer relationship management platforms handle payment card data securely and in compliance with industry standards. CRM systems often store and process sensitive customer information, including payment details, making them a critical point for implementing PCI DSS requirements. Integration includes use of secure encryption for storage and transfer of information, strict authentication measures and a good security management environment for the network.

A. Integrating PCI Compliance with CRM

Data encryption, access control, and security checks are a few of the basic practices that organizations must take in order to obtain PCI requirements in the CRM..

1. Data Encryption

Importance of data preservation as it is transmitted and stored is underlined in modern reading. It is advised that CRM systems use robust encryption methods, such as AES-256. Data encryption is vital because it prevents content obfuscation in the event that data interception or unauthorized access occurs.]. Data encrypted during this procedure includes information sent across networks, such as that which occurs when CRM systems talk to external servers, as well as data kept in databases and backup systems.

2. Access Control

Security methods for access control must be straightforward to implement and provide high levels of protection. This includes measures like implementing multifactor authentication to further strengthen security and limiting

access to sensitive information to authorized personnel [21]. It is recommended to utilize RBAC when granting permissions. This method restricts access based on user roles and helps prevent unauthorized access. It is also important to keep an eye on the process for verifying and changing workers' access privileges. When employees move up the corporate ladder or when the demands of a certain organization change, their access privileges sometimes alter as well. It is crucial to maintain and routinely review the access logs in order to promptly address any suspicious actions.

3. *Security Audits*

The following may be among the time-consuming and methodical security checks: An examination of security measures and potential threats is known as a security audit. A security consultant or other impartial third party should conduct these audits. An audit is defined by the PCI DSS as a review of the controls, processes, and policies of an organization to ensure they are up to code. The CRM system and its underlying architecture must be scanned periodically by the IT department in order to detect vulnerabilities. Such measures ensure that compliance with the PCI standard remains uninterrupted among other things, identification of a security weakness and its remediation as well as safeguarding of cardholder data [22].

B. Ensuring PCI DSS Compliance in CRM Software

Adherence to PCI DSS standards is crucial for CRM software because the application processes payment data that should not be breached and accessed without the user's permission. Therefore[22], the CRM solutions must include security elements such as data encryption and tokenization and industrial security audits in order to meet compliance standards and maintain customer loyalty.

- **Encryption:** CRM software must encrypt payment data both during storage and transmission. This means that any information that may be intercepted will still not be read by someone else than the intended recipient. Both AES-256 and TLS 1.2/1.3 are widely used sophisticated methods to enhance the security of data transfer successfully..
- **Tokenization:** Tokenization involves substituting delicate payment information with token equivalents which are non-delicate hence reducing exposure to breaches.. In addition to minimizing the volume of data considered to be sensitive, tokenization also lessens the specific area of PCI DSS compliance for CRM.
- **Authentication:** Rest assured that only authorized workers will have access to critical payment data due to role-based access restrictions. In multi-factor authentication (MFA), the second factor prevents the system from breaking should someone hack into the login information..
- **Regular Security Assessments:** Even with all the risks involved, it is possible to detect and rectify CRM system vulnerabilities through a process of vulnerability scans, as well as periodic penetration tests. Monitoring activities and audit trails help to identify problems to avoid or fix issues that are unusual.
- **Data Minimization and Secure Storage:** For a long time, risk exposures are minimized if considerable data is stored for only a short while. Application of sealed up and encrypted databases, secure servers adds onto it to ensure that only authorized personnel gains entry.
- **Compliance Training:** Despite this, employees are vulnerable sources of breaches and should undergo continual training in the PCI DSS measures to avoid violated actions. Third party auditors are treated as independent scrutinizers to guaranty the CRM software is compliant with the rules.

C. Importance of PCI Compliance in CRM Software

PCI compliance should be a priority for CRM software because it processes card data together with personal data of customers. Implementing Compliance with the PCI DSS safeguards cardholder information loss as well as helps to decrease the possibility of financial crimes and build consumer trust. Failure has consequences including higher fines, negative brand image, and surrender of the payment processing rights. For businesses, a PCI-compliant CRM cannot only increase data security but also the following business benefits. It is some importance point of PCI compliance in CRM software are as follow:

- **Protection of Sensitive Data:** This information can include customer's personal information as well as details such as payment cards. Ensuring that delicate information is processed, stored and transmitted safely, PCI compliance minimizes vulnerability to attacks.
- **Prevention of Financial Loss:** Failure to conform with the PCI DSS is dire since it results in penalties, fines and in some cases, put the company to litigation when a data breach incident occurs. However, compliance minimizes organizations from exposing themselves to such financial risks.
- **Building Customer Trust:** This means that the companies that have the focus of ensuring that their customers' mode of payment is secure will always get their trust. PCI compliant CRM systems help an organization to improve its image and credibility on the market.
- **Regulatory Requirement:** PCI DSS compliance is a

mandatory standard for businesses that engage in processing the payment card data which are determined by the payment card networks. CRM software cannot violate these standards or it incurs legal and operational consequences.

- **Mitigation of Cybersecurity Threats:** There is a tendency that targeted attacks on payment card data are becoming much more complicated. These threats are well countered by PCI compliance which in turn shields the businesses and their clientele.
- **Competitive Advantage:** Companies that have PCI-compliant CRM systems in place hold an advantage over competitors in world markets, including within attempts to secure customers who value data protection.
- **Simplified Audits and Reporting:** The use of PCI compliant CRM software helps to ease the undertaking of compliance during the auditing exercise thus easing the burden on the businesses.
- **Support for Long-Term Growth:** When the size of a company's commerce operation grows, so too does the number of payment cards that are processed. PCI compliance helps their CRM systems to be ready for this growth both securely and effectively.

5. Impacts Of PCI DSS On CRM Software

The Payment card industry data security standard significantly influences the development of Customer Relationship Management (CRM) software, especially when such systems handle sensitive payment card data. Developers of CRM are to implement the security measures to ensure compliance with the PCI DSS requirements of which affects several aspects of application development, infrastructure and management[23].

A. Security First Development Approach:

PCI DSS mandates security measures, compelling CRM developer to prioritize security at every stage of the software development lifecycle.

- **Secure coding practice:** Developer should ensure that he or she adheres to different secure coding Principles such as avoiding code vulnerabilities such as the SQL injection.
- **Risk assessment:** Regular threat modeling a disk assessment are required to identify potential vulnerabilities in the CRM system.

B. Data storage and Encryption:

PCI DSS emphasize protecting stored cardholder data, which directly impacts CRM data management.

- **Data Minimization:** CRMs must minimize data regarding cardholder identification or account information as much as is reasonable.
- **Data Encryption:** Data encrypted during this procedure includes information sent across networks, such as that which occurs when CRM systems talk to external servers, as well as data kept in databases and backup systems.
- **Tokenization:** Substitute cardholder data with tokens because CRM systems eliminate associated risks.
- **Authentication and Access Controls:** The PCI DSS recognizes the importance of the concept of access control and makes strict access control mechanisms and parameters mandatory for access to cardholder data.

C. Network Security and Integration:

They usually communicate with other networks like those for payment gateways. PCI DSS plays a role as to how these integrations are secured.

- **Secure APIs:** Developers of CRM must make sure that all API used for communication with payment processors are safe from hackers and encrypted.
- **Firewall and Intrusion Detection:** Firewalls and intrusion detection system must be integrated into the CRM systems to detect and prevent the traffic on the networks. include relevant information. Do not combine references. There must be only one reference with each number. If there is a URL included with the print reference, it can be included at the end of the reference.

D. Regular Testing and Monitoring:

PCI DSS requires ongoing testing and monitoring to ensure the CRM system remains secure.

- **Vulnerability Scanning:** Incidences of vulnerability in the CRM software have to be addressed and this has to be done by incorporating automated scanning to check for vulnerabilities.
- **Penetration Testing:** Regular penetration testing is conducted to simulate attacks and identify potential vulnerabilities.
- **Security Audits:** An examination of security measures and potential threats is known as a security audit. Audits are defined by the PCI DSS as looking at The CRM system and its underlying architecture must be scanned periodically by the IT department in order to detect vulnerabilities.
- **Simulation Reports:** The effectiveness of the CRM systems may be evaluated by assessing the degree of PCI compliance using these simulated reports. Additionally, they assist an organization in

taking steps to stop these dangerous places before criminals take use of them..

6. Challenges and Solutions of PCI Security For CRM

It some cchallenges and Solutions of PCI security for CRM are as follow:

A. High Implementation Costs

There are expenses associated with complying with the PCI DSS standards; some of these fees are reasonable, while others are rather high, especially for SMEs. Investments in new or upgraded infrastructure, trained security guards, and regulatory fees may add up quickly. There are a number of approaches to managing compliance that take into account both financial and security considerations. One approach is to prioritize the most pressing compliance issues while simultaneously looking for ways to invest in cost-effective security measures. Local infrastructure investment needs may be reduced by using services that comply with the payment card industry.

B. Complexity of Compliance

Consequently, the PCI DSS is the one that might put a strain on an organization's capacity to handle challenges. This implies that without expert guidance, a company faces a mountain of technical and administrative requirements. For greater PCI standard compliance, organizations could use QSAs for services or speak with compliance experts. The use of compliance management software, however, facilitates the administration and accurate tracking of all such activities. When everything is done correctly and compliance management software is much simpler, the same can be said for the previously specified factors.

C. Maintaining Ongoing Compliance

Achieving early compliance is one thing, but maintaining it is quite another. As a result, it is crucial to regularly update the policy, audit the business, and make sure that staff members are properly educated to handle evolving security threats. There must be a dedicated compliance department whose primary responsibility is to keep an eye on system performance, do audits, and ensure compliance. It is essential to implement updates and other programming tools that enable continuous compliance monitoring and the rapid localization of identified issues. The organization's personnel must be kept alert and not break the regulations, thus it is crucial that them have ongoing professional-level feeling sessions on security compliance.

D. Human error and insider threats

There aren't many opponents when it comes to PCI compliance, but insiders and mistakes are two of them. This may occur when employees, either intentionally or unintentionally, pose a risk to the company's security. Avoiding such a danger may be possible with the use of updated technology, such as stringent access control mechanisms and comprehensive security training for all staff. As a rapid reaction tool, ongoing auditing of all accesses and subsequent recording of cardholder data may help detect potential unauthorized individuals.

7. Literature Review

This section provides a literature review on A holistic Review PCI security standard Framework for customer relationship management (CRM) software, summary shows in Table II.

This study, Zohora et al. (2024) aims at examining how the consumer data such as the demographic data, the purchasing behaviour and the security measures they adopt can help improve fraud prevention measures. This study is based on survey data of 200 participants from US credit card users, supported by data on recent frauds. Other variables considered were age, income, number of online transactions, password creation and protection and two-factor authentication. Results indicate that it is possible to improve the security of credit cards in the US financial sector by implementing individual anti-fraud measures considering the behavioural and demographic characteristics of consumers. Consumer behavioural data enables institutions to adopt dynamic approaches that involve real-time transaction notification and behaviour-driven analytics to enhance the accuracy of fraud identification and reduce false alarms[24].

Bhutta et al. (2022), article is a first step in getting researchers to focus on making future PCI DSS versions compatible for the IoT, which will secure the new payment methods that are based on the IoT. The features of the IoT, like the resource-constrained nature of devices and the need to update the software/firmware of a large number of physical devices, make the present version of PCI DSS unsuitable for payment systems focused on the IoT. In addition, there is an immediate need to adopt PCI DSS evaluations and regulations to ensure the security of all parties involved in the payment process that handle user credentials. In order to propose changes to the PCI DSS that are appropriate for IoT, the article has examined both the conventional payment procedure and factors related to payment systems that are based on the IoT[25].

L. Nunnagupala et al. (2022), focusses on how CRM systems are currently assessed for PCI DSS compliance. An in-depth strategy for implementing PCI compliance into CRM systems is presented in this article by an analysis of simulation results and real-time case and problem observation pertaining to the pertinent solutions. Regardless of how difficult it may be, any business that handles cardholder data must implement PCI compliance with CRM systems. While DSS's operations are designed to be fully compliant with PCI standards, one of its goals is to

safeguard data and stop its leaking. However, there are a few drawbacks to be aware of, including the relatively high costs of implementation, the relative complexity, and the need for constant monitoring and updates, which can be a drain on resources. The use of cloud services, consulting with compliance experts, implementing automated compliance solutions, and raising organizational members' understanding of compliance issues are all steps that may be taken to lessen the impact of these risks[27].

According to the results of this study, SaMS-PSP may improve customer retention and loyalty by incorporating sentiment analysis' emotional polarity score into a value-added customer orientation tool [25].

G. Wanganga et al. (2020), recommends a model for consumer sentiment analysis that uses deep learning and an associated algorithm for sentiment analysis inside SaMS-PSP. Compared to traditional machine learning techniques, our model outperforms them experimentally and is better equipped to deal with "big data" applications like consumer sentiment research[26].

S. Rahaman et al (2019), improve the situation where the PCI DSS certification process for Internet shops is assessed quantitatively using an evaluation method. With our e-commerce web application testbed, Buggy Cart, they may add or delete 35 vulnerabilities relevant to PCI DSS as needed. Next, they used the testbed to investigate the complexity of the certification procedure as well as the capabilities and constraints of PCI scanners. Based on the findings, 86% of the websites had at least one PCI DSS violation, which should have made them ineligible for non-compliance. The results produced by PciCheckerLite are more accurate than those of w3af, according to our comprehensive accuracy study. For the purpose of bettering enforcement in practice, they contacted the PCI Security Council to relay the findings of our study[14].

Table II can be used as a checklist to establish how the literature can be beneficial in the aspects of enhancing PCI DSS compliance for CRM systems, for tools, analysis, strength, weaknesses and recommendations.

Table II. summary of literature review of PCI security standard of customer relationship management (CRM)

Reference	Area	Tools/Techniques	Analysis	Advantage	Disadvantage	Recommendation
Zohora et al. (2024)	Fraud Prevention and Security	Survey data analysis, behavioral analytics, real-time transaction notification	Examines how consumer behavior and demographics can improve fraud prevention.	Enables dynamic fraud prevention; Real-time notifications reduce false alarms.	May require extensive data collection and advanced analytics capabilities.	Integrate behavior-driven analytics into CRM systems for tailored fraud prevention measures.
Bhutta et al. (2022)	IoT-based Payment Security	Review of PCI DSS for IoT, recommendations for standards modification	Highlights the unsuitability of current PCI DSS for IoT payment systems due to resource constraints.	Brings focus on IoT security; Highlights need for updates in security frameworks.	High implementation complexity; Challenges in updating multiple devices.	Extend PCI DSS to include IoT-specific measures for secure payment systems.
L. Nunnagupala et al. (2022)	PCI DSS Compliance in CRM	Simulation reports, real-time observation, cloud solutions, automated compliance tools	Discusses adopting PCI DSS compliance within CRM systems and associated challenges.	Promotes better data security in CRM systems; Recommends automation and cloud services.	High costs and resource consumption; Complexity in implementation.	Automate compliance tasks and foster awareness among organizational members to ensure effective PCI compliance in CRM systems.
G. Wanganga et al. (2020)	Sentiment Analysis for CRM in the Payment Industry	Deep learning-based sentiment analysis model, SaMS-PSP algorithm	Demonstrates sentiment analysis for customer retention and	Superior performance over conventional methods; Handles large-scale	Complexity of deep learning models; Requires substantial computational resources.	Integrate sentiment analysis into CRM for improved customer orientation and loyalty in the Payment Industry.

			loyalty using deep learning.	customer sentiment data.		
S. Rahaman et al. (2019)	PCI DSS Certification Process	BuggyCart testbed for PCI DSS vulnerabilities evaluation; Tools: PciCheckerLite, w3af	Measures effectiveness of PCI DSS certification processes for e-commerce websites.	Reveals gaps in compliance processes; Highlights need for improvement in certification rigor.	Significant compliance gaps in existing systems.	Enhance rigor of PCI DSS certification for CRM systems by implementing stricter evaluation methods and improving scanner tools.

8. Conclusion

PCI DSS compliance remains critical in realizing secure processing of payment card data in CRM software to reduce business and customer risks. Therefore, PCI DSS compliance for the CRM system is mandatory to protect the customer's payment details and the credibility of the business. In addition to protecting against data loss and cyber threats, adherence to the practices advanced by PCI DSS ensures organizations meet legal obligations and maintain customer confidence as they avert penalties. By the same token, while compliance entails certain expenses such as high implementation costs and constant monitoring, business can overcome these challenges stick to such methods as encryption, tokenization, and secure APIs. Finally, the PCI DSS norms have to be incorporated into the CRM software to protect payment data and retain market position in a highly competitive market.

References

[1] N. Abid, "Improving Accuracy and Efficiency of Online Payment Fraud Detection and Prevention with Machine Learning Models," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 12, pp. 711–723, 2024.

[2] S. Arora, "Security Vulnerabilities in Edge Computing : A Comprehensive Review," *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 936–941, 2022.

[3] H. Sinha, "An examination of machine learning-based credit card fraud detection systems," *Int. J. Sci. Res. Arch.*, vol. 12, no. 01, pp. 2282–2294, 2024, doi: https://doi.org/10.30574/ijsra.2024.12.2.1456.

[4] M. Gorge, "The PCI standard and its implications for the security industry," *Comput. Fraud Secur.*, 2006, doi: 10.1016/S1361-3723(06)70307-4.

[5] S. Yulianto, C. Lim, and B. Soewito, "Information security maturity model: A best practice driven approach to PCI DSS compliance," *Proc. - 2016 IEEE Reg. 10 Symp. TENSYMP 2016*, pp. 65–70, 2016, doi: 10.1109/TENCONSpring.2016.7519379.

[6] R. Arora, "Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications," *8th Int. Conf. "Computing Sustain. Glob. Dev.*, no. March, pp. 458–463, 2021.

[7] R. Arora, S. Gera, and M. Saxena, "Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2021, pp. 458–463.

[8] V. Tien Dat *et al.*, "The process of CRM system implementation at Dien May Xanh in Vietnam," *Int. J. Multidiscip. Res. Growth Eval.*, 2021.

[9] H. A. Al-homery, H. Asharai, and A. Ahmad, "The Core Components and Types of CRM I . Introduction," *Pakistan J. Humanit. Soc. Sci.*, vol. 7, no. 1, pp. 121–145, 2019.

[10] R. Bishukarma, "Scalable Zero-Trust Architectures for Enhancing Security in Multi-Cloud SaaS Platforms," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1308–1319, 2023, doi: 10.48175/IJARSCT-14000S.

[11] B. Boddu, "SOC Audit and Encryption Customer Data and Privacy at Database Security," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 2, no. 1, p. 5, 2024.

[12] P. S. S. Council, "Payment Card Industry (PCI) Data Security Standard," *May*, 2018.

[13] P. S. S. Council, "Payment Card Industry (PCI) Payment Application Data Security Standard Requirements and Security Assessment Procedures," *PCI DSS Requir. Secur. Assess. Proced.*, 2010,[Online].Available: https://otm.finance.harvard.edu/files/otm/files/pci_security_standards.pdf

[14] S. Rahaman, G. Wang, and D. Yao, "Security certification in payment card industry: Testbeds, measurements, and recommendations," in *Proceedings of the ACM Conference on Computer*

and Communications Security, 2019. doi: 10.1145/3319535.3363195.

[15] K. Razikin and A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance," *CommIT J.*, 2021, doi: 10.21512/commit.v15i2.6931.

[16] S. HANCOCK, "THE PCI SELF-ASSESSMENT QUESTIONNAIRE (SAQ)," in *PCI DSS Version 4.0*, IT Governance Publishing, 2024, pp. 54–58. doi: 10.2307/jj.12011252.15.

[17] A. A. Chuvakin and B. R. Williams, "Why Is PCI Here?," in *PCI Compliance*, 2010. doi: 10.1016/b978-1-59749-499-1.00008-8.

[18] PCI Security Standards and Council, "Payment Card Industry Security Standards," *PCI Secur. Stand. Counc. LLC*, 2010, [Online].Available: https://listings.pcisecuritystandards.org/documents/PCI_SSC_Overview.pdf

[19] C. PCI Security Standards, "PCI Software Security Framework Provides a Modern Approach to Payment Software Security," pcisecuritystandards. [Online]. Available: https://listings.pcisecuritystandards.org/documents/SSF_At-a-Glance.pdfftware Security

[20] D. Ortiz-Yepes, "A critical review of the EMV payment tokenisation specification," *Comput. Fraud Secur.*, 2014, doi: 10.1016/S1361-3723(14)70539-1.F. Benefits, F. Requirements, and P. Software, "PCI Software Security Framework Provides a Modern Approach to Payment Software Security Options Support Broader Range of," 2019.

[21] H. Omotunde and M. Ahmed, "A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond," *Mesopotamian Journal of CyberSecurity*. 2023. doi: 10.58496/MJCS/2023/016.

[22] V. M. Michail, "Dissertation « Payment Card Industry Data Security Standard-Readiness Project»," no. December, 2015.

[23] A. and P. Khare, "Cloud Security Challenges : Implementing Best Practices for Secure SaaS Application Development," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 669–676, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.11.

[24] F. Zohora, R. Parveen, A. Nishan, M. Haque, and S. Rahman, "OPTIMIZING CREDIT CARD SECURITY USING CONSUMER BEHAVIOR DATA: A BIG DATA AND MACHINE LEARNING APPROACH TO FRAUD DETECTION," *Front. Mark. Manag. Econ. J.*, vol. 04, pp. 26–60, 2024, doi: 10.37547/marketing-fmmej-04-12-04.

[25] M. N. M. Bhutta *et al.*, "Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS)," *Wirel. Commun. Mob. Comput.*, 2022, doi: 10.1155/2022/9942270.

[26] G. Wanganga and Y. Qu, "A Deep Learning based Customer Sentiment Analysis Model to Enhance Customer Retention and Loyalty in the Payment Industry," in *Proceedings - 2020 International Conference on Computational Science and Computational Intelligence, CSCI 2020*, 2020. doi: 10.1109/CSCI51800.2020.00086

[27] L. S. C. Nunnagupala, S. R. Mallreddy, and J. R. Padamati, "Achieving PCI Compliance with CRM Systems," *Turkish J. Comput. Math. Educ.*, vol. 13, no. 1, pp. 529–535, 2022, doi: 10.61841/turcomat.v13i1.14689