**Module Tutor Name: Faizan Ahmad**

**Module Number: LD7152**

**Student Name: Shabina**

**Student ID: W21060994**



|  |
| --- |
| Close-up image showing the leaf-sides of two oversized books side-by-side on a bookshelf, with additional books in soft focus background |
| **Module Title: Engineering and Environment Advanced Practice London Campus Research Project Assignment Title: Ensuring PCI DSS Compliance in Cloud Environments: Challenges and Best Practices**  **Course of Study: AP Research Project – Report & Poster Presentation** **Module** |
| |  |  |  | | --- | --- | --- | |  |  |  | |

Table of Contents

[Research Topic: Ensuring PCI DSS Compliance in Cloud Environments: Challenges and Best Practices 5](#_Toc135141833)

[Abstract: 5](#_Toc135141834)

[Introduction: 5](#_Toc135141835)

[**Part A: Reflective Report** 6](#_Toc135141836)

[1. Finding a research topic: Ensuring PCI DSS Compliance in Cloud Environments: Challenges and Best Practices 6](#_Toc135141837)

[Exploring the Why and How of My Research Topic: Motivations and Rationale Behind the Choice of Inquiry 6](#_Toc135141838)

[Mastering Information Retrieval: Effective Techniques and Library Search Tools for Finding Relevant Information: 7](#_Toc135141839)

[Exploring Information Retrieval: Navigating Disciplinary Boundaries and Beyond: 7](#_Toc135141840)

[Aims and Objectives: 7](#_Toc135141841)

[Supervisor Collaborations in Research: Discussions and Recommendations for Success: 8](#_Toc135141842)

[2. Professional Activities: 8](#_Toc135141843)

[2.1 Research development tasks: 8](#_Toc135141844)

[Schedule and Record of Research Development Tasks: 8](#_Toc135141845)

[By conducting a literature review 8](#_Toc135141846)

[Conducting a PCI DSS compliance assessment: 8](#_Toc135141847)

[Creating a strategy to address identified risks and gaps: 8](#_Toc135141848)

[Creating an online survey using Google Forms: 8](#_Toc135141849)

[2.1.1 Gantt chart: 9](#_Toc135141850)

[2.2 Function of Independent Researcher: 10](#_Toc135141851)

[1. Ensuring compliance across multiple regions 10](#_Toc135141852)

[2. Managing shared responsibility: 10](#_Toc135141853)

[3. Keeping up to date with changing regulations: 10](#_Toc135141854)

[2.3 Problems Overcome and Solutions: 10](#_Toc135141855)

[2.4 Communication Experiences with My Supervisor: 11](#_Toc135141856)

[3.Literature Review 12](#_Toc135141857)

[3.1 Mind Map: 12](#_Toc135141858)

[3.1.2 Tools and resources used to develop the mind map were: 13](#_Toc135141859)

[3.3 Introduction 13](#_Toc135141860)

[3.4 Understanding Regulations and Standards for PCI DSS Compliance in Cloud Environments: A Comprehensive Overview: 14](#_Toc135141861)

[3.4.1 Cloud Computing Guidelines: 14](#_Toc135141862)

[3.4.2 Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR): 14](#_Toc135141863)

[3.4.4 National Institute of Standards and Technology (NIST) Cybersecurity Framework: 15](#_Toc135141864)

[3.3 Challenges for PCI DSS Compliance in Cloud Environments: 15](#_Toc135141865)

[Shared Responsibility Mode 15](#_Toc135141866)

[Lack of Visibility and Control 16](#_Toc135141867)

[Data Location and Storage 16](#_Toc135141868)

[3.5 Best Practices for PCI DSS Compliance in Cloud Environments: 16](#_Toc135141869)

[Understand the Shared Responsibility Model 16](#_Toc135141870)

[Implement Strong Access Controls 17](#_Toc135141871)

[Firewall: 17](#_Toc135141872)

[Avoid Vendor-Supplied Defaults: 17](#_Toc135141873)

[Protect Stored Cardholder Data: 17](#_Toc135141874)

[Encrypt Data in Transit and at Rest: 18](#_Toc135141875)

[Antivirus: 18](#_Toc135141876)

[Monitor Access to Network and Data: 18](#_Toc135141877)

[Regular Security Testing and File Integrity Monitoring (FIM): 18](#_Toc135141878)

[3.6 Case Studies of Successful PCI DSS Compliance in Cloud Environments: 18](#_Toc135141879)

[3.7 Exploring the Future of Payment Card Security: Emerging Trends in Cloud Computing and PCI DSS Compliance: 18](#_Toc135141880)

[Conclusion: 19](#_Toc135141881)

[4. Reflection of Research Project 19](#_Toc135141882)

[4.1 How I Contributed to My Assignment: A Personal Reflection 19](#_Toc135141883)

[4.1.1 Survey on Ensuring PCI DSS Compliance in Cloud Environments: Practices and Challenges 19](#_Toc135141884)

[4.1.2 Survey Response Statistics: 19](#_Toc135141885)

[4.2 Challenges and Recommendations 26](#_Toc135141886)

[4.2.1 Cloud Access Security Brokers (CASBs): 26](#_Toc135141887)

[4.2.2 Container Security: 27](#_Toc135141888)

[4.2.3 Cloud-native Security Tools: 28](#_Toc135141889)

[4.2.4 Secure DevOps: 29](#_Toc135141890)

[4.2.5 Identity and Access Management (IAM): 31](#_Toc135141891)

[4.3 SWOT ANALYSIS: 31](#_Toc135141892)

[4.4 Research Reflection: Career Relevance: 32](#_Toc135141893)

[4.5 Recommendations 32](#_Toc135141894)

[**Part B: Poster Presentation –** 33](#_Toc135141895)

[Conclusion: 35](#_Toc135141896)

[References 36](#_Toc135141897)

Table of Figures

[Fig 1: What is PCI DSS? (Fugue , n.d.) 5](#_Toc134971963)

[Fig 2: PCI DSS IS A CONTINUOUS PROCESS ( PCI Security Standards Council, 2022) 6](#_Toc134971964)

[Fig. 3 – Gantt Chart (created by author) (Please refer table to understand the Phases) 9](#_Toc134971965)

[Fig. 4: PCI Data Security Standard ( PCI Security Standards Council, 2022) 11](#_Toc134971966)

[Fig.5: Sample cardholder dataflow diagram (Payment Card Industry Data , 2020) 13](#_Toc134971967)

[Fig. 6: CSA STAR to integrate your security systems (CSA, 2020) 14](#_Toc134971968)

[Fig 7: NIST Cybersecurity Framework (Aseem Rastogi , 2019) 15](#_Toc134971969)

[Fig 8: Shared Responsibility Model (Payment Card Industry Data, 2020) 16](#_Toc134971970)

[Fig 9: Key PCI Compliance Requirements in the Cloud (Atlantic.Net Blog, 2021) 17](#_Toc134971971)

[Fig. 10: Employee Role In The Organization 19](#_Toc134971972)

[Fig.11: Pie Chart Of Cloud Service Provider 20](#_Toc134971973)

[Fig.12: PCI DSS challenges in Cloud Environment 20](#_Toc134971974)

[Fig.13: Best Practice to ensure PCI DSS compliance in cloud environment. 21](#_Toc134971975)

[Fig.14: Challenges face by Organization in Ensuring PCI DSS compliance in Cloud Environment 21](#_Toc134971976)

[Fig.15: PCI DSS assessments conducted by Organization 22](#_Toc134971977)

[Fig.16: Additional Resource need Organization to ensure PCI DSS Compliance in Cloud Environments 22](#_Toc134971978)

[Fig.17: Specific Measure taken by an organization to Address Challenges on PCI DSS Compliance in Cloud Environment 23](#_Toc134971979)

[Fig.18: Use of 3rd party compliance 23](#_Toc134971980)

[Fig.19: Best Practice for maintaining PCI DSS compliance in a cloud environment 24](#_Toc134971981)

[Fig.20: Additional Resource organization needs 24](#_Toc134971982)

[Fig.21: Recommendation for improving PCI DSS Compliance process in Cloud Environment 25](#_Toc134971983)

[Fig.22: Step taken to encounter issues 25](#_Toc134971984)

[Fig.23: Purpose of Implementing Security Controls 26](#_Toc134971985)

[Fig.24: Implementing Security controls in cloud Environment 26](#_Toc134971986)

[Fig. 25: Pillars of CASB (SV-Networks, 2022) 27](#_Toc134971987)

[Fig 26: Container Security Pillars (Matteo Bisi, 2023) 28](#_Toc134971988)

[Fig 27: The 4c’s Pillars of cloud native security (Snyk, n.d.) 29](#_Toc134971989)

[Fig 28: The five key pillars of DevSecOps (gmgchow, 2020) 30](#_Toc134971990)

[Fig 29: SWOT Analysis 31](#_Toc134971991)

[Fig.30: Poster Presentation on Ensuring PCI DSS Compliance in Cloud Environments: Challenges and Best Practices 34](#_Toc134971992)

List of Tables

[Table 1 – Different tasks/phases of research (created by author) ---------------------------------------------------------9](#_Toc134972064)

# Research Topic: Ensuring PCI DSS Compliance in Cloud Environments: Challenges and Best Practices

Abstract:Any company that handles, stores, or sends credit card data must adhere to the Payment Card Industry Data Security Standard (PCI DSS) set of security requirements. Ensuring PCI DSS compliance in cloud environments has grown more crucial and difficult as more businesses shift their activities to the cloud (George Mateaki, n.d.). The difficulties and ideal procedures for maintaining PCI DSS compliance in cloud systems are examined in this assignment.

Introduction: The Payment Card Industry Data Security Standard (PCI DSS) is a thorough set of security requirements designed to safeguard credit card information and guarantee that it is handled and stored securely. All businesses, services, and financial institutions that accept credit card payments must comply with PCI DSS. Organisations now confront additional difficulties in maintaining PCI DSS compliance in cloud systems as a result of the rising use of cloud computing.

A picture containing text, font, screenshot, circle

Description automatically generated

Fig 1: What is PCI DSS? (Fugue , n.d.)

Data loss and leakage, account or service traffic hijacking, and unsecured interfaces and APIs are among the top security risks for cloud computing, according to the Cloud Security Alliance's (CSA, 2022)assessment on the dangers to the industry. To ensure PCI DSS compliance in cloud environments, these security concerns may provide tough hurdles. Regarding this, this assignment will examine the difficulties and best practises for ensuring PCI DSS compliance in cloud environments and offer helpful advice for businesses on how to secure their cloud environments and keep PCI DSS compliance.

# **Part A: Reflective Report**

## Finding a research topic: Ensuring PCI DSS Compliance in Cloud Environments: Challenges and Best Practices

### Exploring the Why and How of My Research Topic: Motivations and Rationale Behind the Choice of Inquiry

A key set of rules called the Payment Card Industry Data Security Standard (PCI DSS) was created to guarantee the security of credit card transactions. Maintaining PCI DSS compliance has grown more difficult, though, as cloud computing has become more widely used. The shared responsibility paradigm of cloud computing, which raises questions about accountability and responsibility, is one of the major obstacles. To achieve PCI DSS compliance in cloud environments, organisations must take a risk-based approach, identifying the risks related to cloud usage and putting in place the necessary security controls to reduce those risks (PCI Security Standards Council, 2019).

More than just payment account data are protected by PCI DSS. In spite of being especially designed with environments containing payment card account data in mind, PCI DSS can be utilised to protect and secure various elements of the payment ecosystem ( PCI Security Standards Council, 2022).

A picture containing text, screenshot, font, line

Description automatically generated

Fig 2: PCI DSS IS A CONTINUOUS PROCESS ( PCI Security Standards Council, 2022)

A thorough analysis of the difficulties and ideal procedures for achieving PCI DSS compliance in cloud systems is given by Shaw and Katzan (2017). They advise taking a risk-based approach and keeping up a thorough knowledge of the cloud environment (Shaw, E., & Katzan, H., 2017).

Moving operations to the cloud introduces new challenges for maintaining PCI DSS compliance, including the shared responsibility model of cloud computing, the need to secure data across multiple cloud environments, and the potential for compliance gaps. These challenges require organizations to adopt a risk-based approach and implement appropriate security controls to mitigate the risks associated with cloud usage (Gartner, 2020).

### Mastering Information Retrieval: Effective Techniques and Library Search Tools for Finding Relevant Information:

I started my study by utilising a variety of methods and approaches to locate pertinent data on the subject. I began by running a quick search using all-encompassing terms like "cloud security," "PCI DSS standards," and "cloud service providers" that were connected to PCI DSS compliance in cloud environments. I then focused my search by using more precise terms relevant to each of the areas that the issue may cover, such as "strategies for managing risks in cloud environments" and "technologies for monitoring credit card data in the cloud". ACM Digital Library, IEEE Xplore, and Google Scholar are just a few of the search engines and databases I used. I also made use of the library resources I had at my disposal. I specifically used the JSTOR, Scopus, and ProQuest online databases that my university's library makes available. I also searched for pertinent books, journal articles, and conference papers using the library's search capabilities.

### Exploring Information Retrieval: Navigating Disciplinary Boundaries and Beyond:

Due to its novelty, I found that there aren't many studies that specifically address PCI DSS compliance in cloud environments. I looked outside the realm of computer science and cybersecurity to find enough information. I read papers in the finance, compliance, and audit industries to better understand PCI DSS requirements and credit card data standards. Academic publications, conferences, and resources like the PCI Security Standards Council and cloud service providers all provided insightful information. Relevant papers from organisations like ICINS and CCEM highlight the problem's interdisciplinary aspect and call for investigation outside of one's core expertise.

### Aims and Objectives:

In order to give best practises for protecting cloud-based payment card data, my research aims to pinpoint the primary obstacles to establishing and maintaining PCI DSS compliance in cloud environments. My research's objectives are:

1. To comprehend the specific security problems offered by the cloud and the PCI DSS requirements in cloud contexts.
2. To list the main dangers of using cloud-based credit card data together with the prevention measures.
3. To review the technology and techniques available for monitoring and safeguarding credit card information in the cloud.
4. Consider how cloud service providers contribute to and uphold PCI DSS compliance.
5. Examine case studies on the effective implementation of PCI DSS compliance in cloud environments.
6. To examine potential changes in cloud security and how they may affect PCI DSS compliance (Shaw, E., & Katzan, H., 2017).

### Supervisor Collaborations in Research: Discussions and Recommendations for Success:

My study topic and objectives were discussed in depth with my supervisor. His advice was quite helpful when it came to my research plan. We stressed the need of concentrating on particular difficulties and proposed solutions for achieving and maintaining PCI DSS compliance in the cloud rather than providing a broad picture. My boss suggested reading recent publications and taking into account successful implementation case studies to acquire insightful information.

## Professional Activities:

2.1 Research development tasks: In order to learn more about the subject and create a strategy for tackling compliance risks and gaps, I undertook a number of research development assignments as part of my study, Ensuring PCI DSS Compliance in Cloud Environments: Challenges and Best Practises. Some of the area where I've worked on include:

Schedule and Record of Research Development Tasks: To give my research assignment a methodical framework, I created a Gantt chart. The Gantt chart provided a visual representation of the duration, dependencies, and deadlines of the research projects. Due to my ability to prioritise my work and maintain focus, I will be able to complete the assignment by the deadline.

By conducting a literature review: I was able to gain a thorough understanding of the subject, as well as the difficulties in ensuring PCI DSS compliance in cloud environments, best practices, and legal requirements. I looked in academic databases like IEEE Xplore, ACM Digital Library, and Google Scholar for related articles, conference proceedings, and reports. I was able to determine the most important areas that needed to be addressed to ensure compliance through this approach and gain insightful information from subject matter experts in the area.

Conducting a PCI DSS compliance assessment: I assessed the cloud environment's PCI DSS compliance in collaboration with my professor. To assure compliance, this required assessing the configuration of the cloud environment and identifying any risks or gaps that needed to be resolved. I conducted the assessment using the PCI DSS Self-Assessment Questionnaire (SAQ).

Creating a strategy to address identified risks and gaps: Based on the outcomes of the assessment, I came up with a plan to deal with the risks and gaps that were found. The plan outlines a timeline for conducting regular audits and reviews to ensure ongoing compliance and for implementing the required security measures in the cloud environment.

Creating an online survey using Google Forms: I made a Google Forms-based online survey to get opinions from experts on PCI DSS compliance. The poll was created by me to learn more about the difficulties professionals encounter when trying to ensure compliance in cloud systems, as well as the strategies they use to get around these difficulties.

2.1.1 Gantt chart: I also developed a Gantt chart to schedule and monitor the development of research activities based on the below tasks (Phases).

Table

Description automatically generated  
  
 Table 1 – Different tasks/phases of research (created by author)

Fig. 3 – Gantt Chart (created by author) (Please refer table to understand the Phases)

My supervisor gave me direction and criticism throughout this process and offered insightful comments and suggestions for enhancing the research development activities. Through our cooperation, I was able to create a more thorough and practical plan for addressing the difficulties and dangers related to ensuring PCI DSS compliance in cloud environments.

## 2.2 Function of Independent Researcher:

As an independent researcher, it would be my responsibility to collect data, analyse it, and share the findings with interested parties. To succeed as an independent researcher, I would need to possess in-depth understanding of PCI DSS compliance and cloud computing. This would require keeping up with industry standards and the latest research, as well as having a thorough grasp of the technical and legal aspects of the field.

Amazon Web Services (AWS) is a real-world example of a business that is focusing on PCI DSS compliance. Due to the fact that it offers cloud computing services to companies and organisations all over the world, AWS is required to comply with PCI DSS.

The following are some of the difficulties AWS encounters in achieving PCI DSS compliance in cloud environments:

1. Ensuring compliance across multiple regions**:** AWS operates in a number of international locations, each of which has its own particular compliance standards. It may be difficult to guarantee that every region complies fully with PCI DSS standards as a result.
2. Managing shared responsibility: According to the shared responsibility model used by AWS, while customers oversee protecting their own applications and data, AWS is in charge of maintaining the security of the cloud infrastructure. Due to this, ensuring that all parties adhere to PCI DSS rules in full may be difficult.
3. Keeping up to date with changing regulations: It can be difficult for AWS to keep up with the most recent criteria and guarantee that all services and systems are fully compliant because PCI DSS regulations are continually changing (AWS, 2021).

AWS would need to be flexible, inventive, and collaborative to overcome these obstacles. In order to develop and execute effective security measures that satisfy regulatory standards and guarantee the flexibility and scalability of the cloud environment, it may be necessary to collaborate closely with customers, regulators, and industry experts. To automate and streamline compliance activities, it can also entail making investments in new technologies and procedures, such as solutions based on artificial intelligence and machine learning.

## 2.3 Problems Overcome and Solutions:

During my research and development work on ensuring PCI DSS compliance in cloud environments, I ran into a number of problems and difficulties. I was able to solve these issues, though, by combining critical thinking, research skills, and creativity.

Due to their technical nature, it proved difficult for people without IT security credentials to comprehend the complex PCI DSS compliance standards. Overcoming this challenge required reading pertinent papers, reviewing requirements, and engaging experts in the field. My understanding of the needs and how they are applied in cloud systems has improved as a result of these efforts (Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. , 2009).

The rapid advancement of technology made it difficult to identify and put into practise the best procedures for preserving PCI DSS compliance in the cloud. To get around this, I reviewed a lot of literature, looked at research papers and industry publications, and spoke with specialists in-person. This made sure that my suggestions were supported by the most recent research and industry best practises (Payment Card Industry Security Standards Council, 2019).

I had trouble getting data and information from PCI DSS compliance professionals. I used Google Forms to develop an online survey that I disseminated to pertinent people and organisations in order to get beyond this challenge. My research benefited greatly from their insightful opinions and useful thoughts. Despite the difficulties, I was able to complete my research and development on preserving PCI DSS compliance in the cloud. I obtained a thorough understanding of the topic and offered helpful assistance in my study by utilising my research abilities and interacting with business people.  
  
A picture containing diagram

Description automatically generated

Fig. 4: PCI Data Security Standard ( PCI Security Standards Council, 2022)

The employment of encryption technologies is one potential answer to this problem. Sensitive data can be protected in the cloud using encryption both at rest and during transmission. Depending on the particular requirements of the organisation, encryption can be implemented at a variety of levels, including the application level and the database level. Companies may drastically lower the risk of data breaches and maintain PCI DSS compliance by deploying encryption solutions.

The obligation to stay current with the most recent PCI DSS rules and best practises presents another challenge for businesses. Companies must make sure they stay current with the most recent updates to PCI DSS requirements in order to maintain compliance. Working with a third-party PCI DSS compliance provider is one potential answer to this problem. These service providers can give specialised knowledge and skills, enabling businesses to stay current with the most recent standards and best practises.

In conclusion, maintaining PCI DSS compliance in cloud settings can be difficult, but businesses can overcome these difficulties and safeguard sensitive data by putting in place the right security measures, like using encryption technology. To maintain continuing compliance, it is crucial to stay current with the most recent requirements and best practises.

## 2.4 Communication Experiences with My Supervisor:

Communication with my supervisor on a frequent basis was crucial during the entire research project. We talked about my work, the findings of the study, and clarified any issues. Helpful advise helped me clarify my research topics, pinpoint knowledge gaps, and raise the standard of my work. My contribution to cybersecurity has been tremendously aided by this ongoing contact. Professional development initiatives like workshops, webinars, certificates, and cybersecurity conferences improved networking, research methodology, and awareness of innovations. These activities were crucial to the success of my research endeavour and to my development as a professional. Creating a Gantt chart, doing in-depth literature reviews, time management, and regular communication with my supervisor were all part of my overall development. Through these efforts, I gained valuable research skills, overcame challenges, and successfully completed my study objectives.

## 3.Literature Review

In the current digital era, cloud computing has emerged as a well-liked option for businesses of all kinds to store and analyse data. However, achieving compliance with the Payment Card Industry Data Security Standard (PCI DSS) presents special difficulties in cloud contexts. In order to ensure PCI DSS compliance in cloud systems, this literature study will examine difficulties and best practises.

## Mind Map:

A mind map is a visual tool for brainstorming, planning, and problem-solving that groups information around a key idea (Graham Burnett, n.d.).

A screenshot of a computer

Description automatically generated with low confidence

Fig 5: Mind Map on Ensuring PCI DSS Compliance in Cloud Environment (by author)

**Click to access Mind map🡪 **

### 3.1.2 Tools and resources used to develop the mind map were:

* I had to create a mind map about "Ensuring PCI DSS Compliance in Cloud Environments" as a student
* I used Coggle.it software to organize the branches and added text and images for each sub-topic
* I consulted various resources like online articles, white papers, official documents from PCI SSC, industry experts, and webinars to ensure that the information was accurate and up to date
* The branches were categorized by topic, and the main topic was at the centre of the map
* Under "PCI DSS Requirements," "Challenges in Cloud Environments," and "Best Practices," I created branches with more detailed subtopics
* "PCI DSS Requirements" had sub-branches for "Network Security," "Access Control," "Data Encryption," and "Security Monitoring"
* "Challenges in Cloud Environments" had sub-branches for "Shared Responsibility Model," "Data Privacy and Security," "Data Residency," and "Vendor Management"
* "Best Practices" had sub-branches for "Cloud Security Controls," "Compliance Automation," "Security Awareness Training," and "Regular Auditing"
* The use of mind mapping software and a range of resources helped me create a comprehensive and informative map on the topic

## 3.3 Introduction

The PCI DSS is a set of security rules designed to ensure that all firms that receive, handle, store, or transmit credit card information do so in a safe environment. A key element of a company's security posture is achieving and maintaining PCI DSS compliance.

A screenshot of a computer

Description automatically generated with medium confidence

Fig.6: Sample cardholder dataflow diagram (Payment Card Industry Data , 2020)

Cloud computing has completely changed how businesses manage their data since it offers flexibility, scalability, and cost efficiency. However, organisations have particular difficulties in maintaining PCI DSS compliance as they progressively shift their data and apps to the cloud. (PCI SSC, 2018).

## 3.4 Understanding Regulations and Standards for PCI DSS Compliance in Cloud Environments: A Comprehensive Overview:

Regulations and standards related to PCI DSS compliance in cloud environments are designed to ensure the protection of sensitive payment card data. The General Data Protection Regulation (GDPR) is a regulation established by the European Union that outlines data protection and privacy for individuals within the EU. Organizations that handle payment card data of individuals residing in the EU must comply with GDPR to protect their data (Europian Union, 2016).

3.4.1 Cloud Computing Guidelines: In 2013, the PCI SSC released cloud computing guidelines that offer advice for maintaining PCI DSS compliance when utilising cloud services (Payment Card Industry Data , 2020).

3.4.2 Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR): A publicly accessible registry called the CSA STAR offers details on cloud service providers' security and compliance. Through doing so, businesses may evaluate the security of their cloud service providers and make sure they adhere to PCI DSS rules (CSA, 2023).

A picture containing text, circle, font, logo

Description automatically generated

Fig. 7: CSA STAR to integrate your security systems (CSA, 2020)

3.4.4 National Institute of Standards and Technology (NIST) Cybersecurity Framework: A set of principles and best practises for enhancing cybersecurity risk management are provided by the NIST Cybersecurity Framework. Although it is not specifically related to PCI DSS compliance, it can be utilised as a foundation for creating an all-encompassing cybersecurity programme that covers cloud environments (Barrett, M., 2018).

A picture containing text, screenshot, design

Description automatically generated

Fig 8: NIST Cybersecurity Framework (Aseem Rastogi , 2019)

Overall, organisations can make use of these frameworks and recommendations to assist maintain PCI DSS compliance in cloud environments and successfully manage the risks related to processing credit card information in the cloud.

## 3.3 Challenges for PCI DSS Compliance in Cloud Environments:

### Shared Responsibility Mode

One of the key challenges of sustaining PCI DSS compliance in cloud systems is the shared responsibility concept. Customers are in charge of guaranteeing the security of their data and applications on the cloud, while cloud service providers are in charge of managing the security of the cloud infrastructure.

The parties accountable for particular security safeguards may not be clear-cut under this shared responsibility paradigm. For instance, a cloud provider may be in charge of protecting the network and physical infrastructure, while the client is in charge of setting up firewalls, putting in place access controls, and encrypting data (Payment Card Industry Data, 2020).

A picture containing text, screenshot, font, businesscard

Description automatically generated

Fig 9: Shared Responsibility Model (Payment Card Industry Data, 2020)

### Lack of Visibility and Control

The absence of visibility and control in cloud systems presents another difficulty for maintaining PCI DSS compliance. Being highly dynamic, cloud systems allow for the instant creation, modification, and deletion of instances. Due to this, it may be challenging to keep an accurate asset inventory and guarantee that all security procedures are applied consistently.

Customers may also have little knowledge of the security measures that their cloud provider has put in place. Due to this, it may be challenging to verify that the supplier is complying with PCI DSS rules and that all security controls are operating as intended (Payment Card Industry Data, 2020).

### Data Location and Storage

Another difficulty for PCI DSS compliance in cloud systems is the location and storage of data. The location of the data and the type of storage medium employed might significantly affect the necessary compliance measures. For instance, there can be additional legal and regulatory criteria to be met if data is held in a different nation. Furthermore, cloud companies could make use of shared storage infrastructure, which can make it challenging to guarantee that data isn't mixed up with that of other clients. This raises the possibility of data leakage and makes it more challenging to meet PCI DSS requirements.

## 3.5 Best Practices for PCI DSS Compliance in Cloud Environments:

### Understand the Shared Responsibility Model

Understanding the shared responsibility paradigm is essential for achieving PCI DSS compliance in cloud environments. The cloud provider must demonstrate that the necessary security controls have been deployed for their infrastructure, while the customer is in charge of putting security controls in place that are compliant with PCI DSS. The key is making sure everyone is aware of their responsibilities. (Payment Card Industry Data , 2020).

### Implement Strong Access Controls

For cloud systems to be in compliance with PCI DSS, rigorous access controls are essential. Access should be restricted to authorised individuals using multi-factor authentication. All access should be monitored and documented so that any attempts at unauthorised access can be quickly identified and dealt with. (PCI SSC, 2018)



Fig 10: Key PCI Compliance Requirements in the Cloud (Atlantic.Net Blog, 2021)

### Firewall:

A firewall is required by PCI to safeguard cardholder data. This can be accomplished locally by installing firewall devices on each network. Utilise the features offered by the cloud provider when using the cloud. Make sure auditors can see the security settings because it must be recorded (Atlantic.Net Blog, 2021).

### Avoid Vendor-Supplied Defaults:

Any IT system in a secure setting needs to update the default password and security settings to be in compliance with PCI. It would take too long to manually verify each cloud resource for default settings; therefore, it is advised to use automated technology like CSPM to find security flaws and cloud misconfigurations (Atlantic.Net Blog, 2021).

### Protect Stored Cardholder Data:

Cardholder data can be protected with the help of PCI-compliant hosting companies, some of which also provide fully managed security. However, it is the user's obligation to set up the security tools properly. It's crucial to assess both current and potential suppliers to ensure the right tools. handled hosting businesses must make sure that DEK and KEK are safely handled in accordance with PCI regulations. Key management is a crucial factor.

### Encrypt Data in Transit and at Rest:

To ensure the security of cardholder data in cloud environments, it is essential to encrypt data in transit and at rest. All data transmitted over public networks should be encrypted using strong encryption protocols, while data at rest should be encrypted using industry-standard encryption algorithms (Atlantic.Net Blog, 2021).

### Antivirus:

The typical strategy in a local setting is to install an antivirus or endpoint protection agent on each computer. The same rule applies to the cloud: you must install an antivirus agent on each cloud resource to guard against malware infection. Deployment on cloud resources is supported by contemporary endpoint protection technologies (Atlantic.Net Blog, 2021).

### Monitor Access to Network and Data:

Tracking and monitoring cardholder data access on-premises is accomplished by "sniffing" network traffic and keeping track of network records. Check relevant event streams and resource logs in the cloud using the cloud provider's monitoring platform or tools from outside sources (Atlantic.Net Blog, 2021).

### Re**gular Security Testing and File Integrity Monitoring (FIM):**

Vulnerability scanning technologies, which frequently incorporate a FIM agent, can meet this criterion in a local context. Examine the security testing tools that the cloud provider makes available, and if they are inadequate, deploy a third-party solution that supports the necessary cloud services (Atlantic.Net Blog, 2021).

## 3.6 Case Studies of Successful PCI DSS Compliance in Cloud Environments:

Many companies have successfully achieved PCI DSS compliance on the cloud, including Global Payments and Verifone (Global Payments Integrated, 2020) (Verifone, 2021). These businesses were able to guarantee the security of cloud payment processing by putting security controls including encryption, access restriction, and regular security assessments into place. To ensure adherence to security standards, they also developed solid relationships with their cloud service providers. These case studies demonstrate that employing different security measures and collaborating closely with cloud service providers are necessary for achieving PCI DSS compliance in the cloud. To guarantee the security of credit card data in the cloud, organisations must also take into account problems like retaining data control and adhering to local data protection rules.

## 3.7 Exploring the Future of Payment Card Security: Emerging Trends in Cloud Computing and PCI DSS Compliance:

Adapting security measures is necessary given how cloud computing and credit card transactions are developing. Today, edge computing lowers latency and improves security while real-time transaction monitoring and threat detection are handled by artificial intelligence (AI). Real-time monitoring, automatic threat identification, and quick incident response are all features of cloud-native security products. To maintain PCI DSS compliance and guarantee safe credit card transactions in the cloud, it's essential to keep up with current trends. To properly protect their operations, organisations should implement best practises and keep up with new technological developments (Peter Mell and Tim Grance, 2011).

## Conclusion:

The important takeaways, hazards, and best practises revealed in the investigation should be summarised in the literature review's conclusion on PCI DSS compliance in cloud environments. Implementing risk management plans, adhering to laws and guidelines like the GDPR, CSA STAR, and NIST Cybersecurity Framework, and conducting regular security audits are all recommendations for organisations. To ensure compliance and protect payment card data in the cloud, regular security audits, vulnerability assessments, and monitoring are crucial. Organisations can fulfil industry best practises and regulatory requirements for protecting credit card data in the cloud by adhering to these standards and laws.

## 4. Reflection of Research Project

## 4.1 How I Contributed to My Assignment: A Personal Reflection

My contribution to this assignment was centred around understanding the current challenges that the industry is facing with regard to PCI DSS compliance in cloud environments, and identifying the latest technology being used to address these challenges. To achieve this, I conducted an online survey using Google Forms and utilized various platforms to gather responses from industry professionals.

### 4.1.1 Survey on Ensuring PCI DSS Compliance in Cloud Environments: Practices and Challenges

[**Link To Survey Questionnaire**](https://forms.gle/t7Zfs1DpNUYuqvBd8)

4.1.2 Survey Response Statistics:Below are thestatistics on the responses for each question.



Fig. 11: Employee Role In The Organization

Forms response chart. Question title: 2.Which cloud service provider does your organization use?
. Number of responses: 20 responses.

Fig.12: Pie Chart Of Cloud Service Provider

Forms response chart. Question title: 3.Which of the following PCI DSS requirements pose the greatest challenge in cloud environments? (Select all that apply)
. Number of responses: 20 responses.

Fig.13: PCI DSS challenges in Cloud Environment

Forms response chart. Question title: 4.Which of the following best practices does your organization follow to ensure PCI DSS compliance in cloud environments? (Select all that apply)
. Number of responses: 20 responses.

Fig.14: Best Practice to ensure PCI DSS compliance in cloud environment.

Forms response chart. Question title: 5.What are the main challenges that your organization faces in ensuring PCI DSS compliance in cloud environments? (Select all that apply)
. Number of responses: 20 responses.

Fig.15: Challenges face by Organization in Ensuring PCI DSS compliance in Cloud Environment

Forms response chart. Question title: 6.How often does your organization conduct PCI DSS compliance assessments in cloud environments?
. Number of responses: 19 responses.

Fig.16: PCI DSS assessments conducted by Organization

Forms response chart. Question title: 7.What additional resources or support do you need to ensure PCI DSS compliance in cloud environments? (Select all that apply)
. Number of responses: 20 responses.

Fig.17: Additional Resource need Organization to ensure PCI DSS Compliance in Cloud Environments

Forms response chart. Question title: 8.What specific measures have you taken to address these challenges and ensure PCI DSS compliance in your cloud environment? (Select all that apply)
. Number of responses: 20 responses.

Fig.18: Specific Measure taken by an organization to Address Challenges on PCI DSS Compliance in Cloud Environment

Forms response chart. Question title: 9.What is your opinion on the use of third-party compliance auditors for PCI DSS compliance in cloud environments?
. Number of responses: 20 responses.

Fig.19: Use of 3rd party compliance

Forms response chart. Question title: 10. Which of the following is a best practice for maintaining PCI DSS compliance in a cloud environment?
. Number of responses: 19 responses.

Fig.20: Best Practice for maintaining PCI DSS compliance in a cloud environment

Forms response chart. Question title: 11.What additional resources or support do you believe would be most helpful for companies trying to ensure PCI DSS compliance in cloud environments? (Select all that apply)
. Number of responses: 20 responses.

Fig.21: Additional Resource organization needs

Forms response chart. Question title: 12. Which of the following is a recommendation for improving the PCI DSS compliance process in cloud environments?
. Number of responses: 19 responses.

Fig.22: Recommendation for improving PCI DSS Compliance process in Cloud Environment

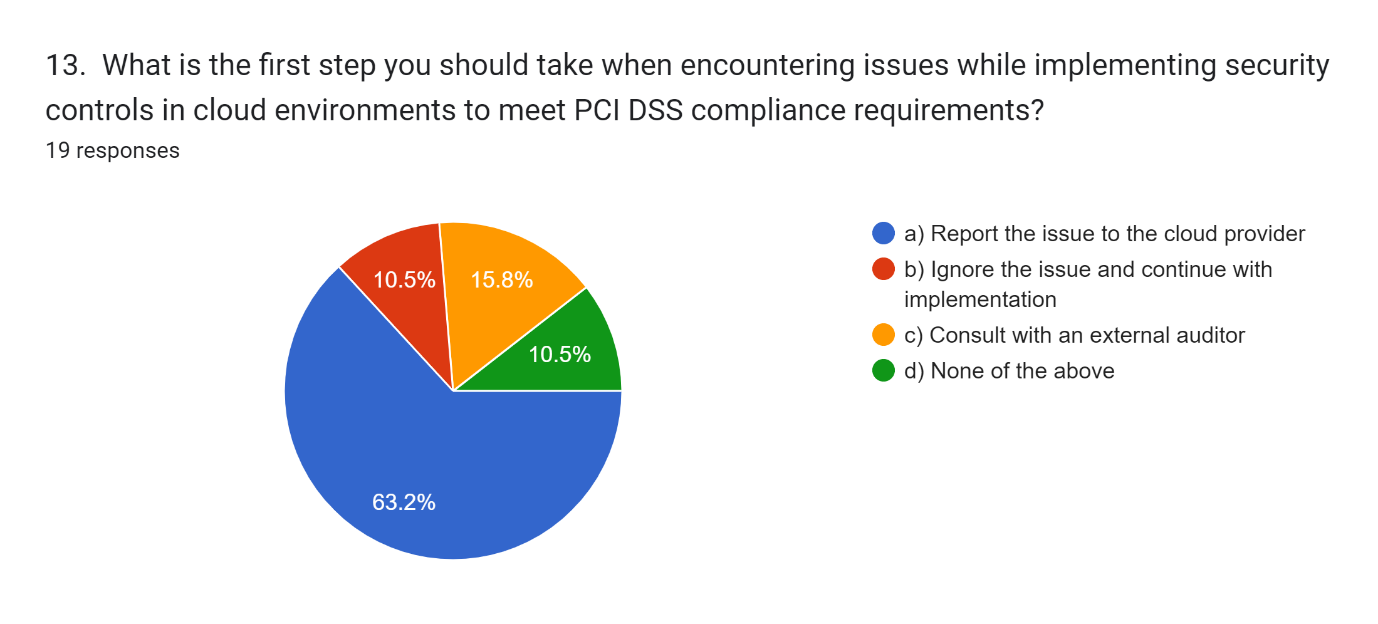


Fig.23: Step taken to encounter issues

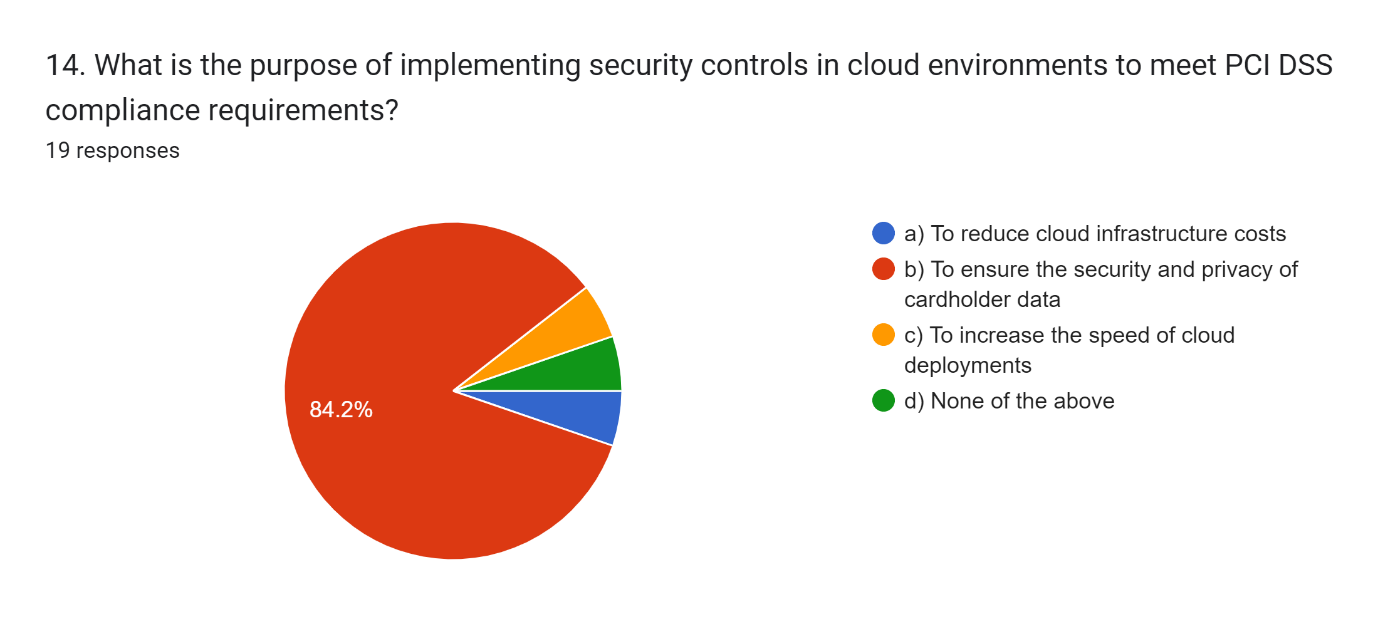


Fig.24: Purpose of Implementing Security Controls

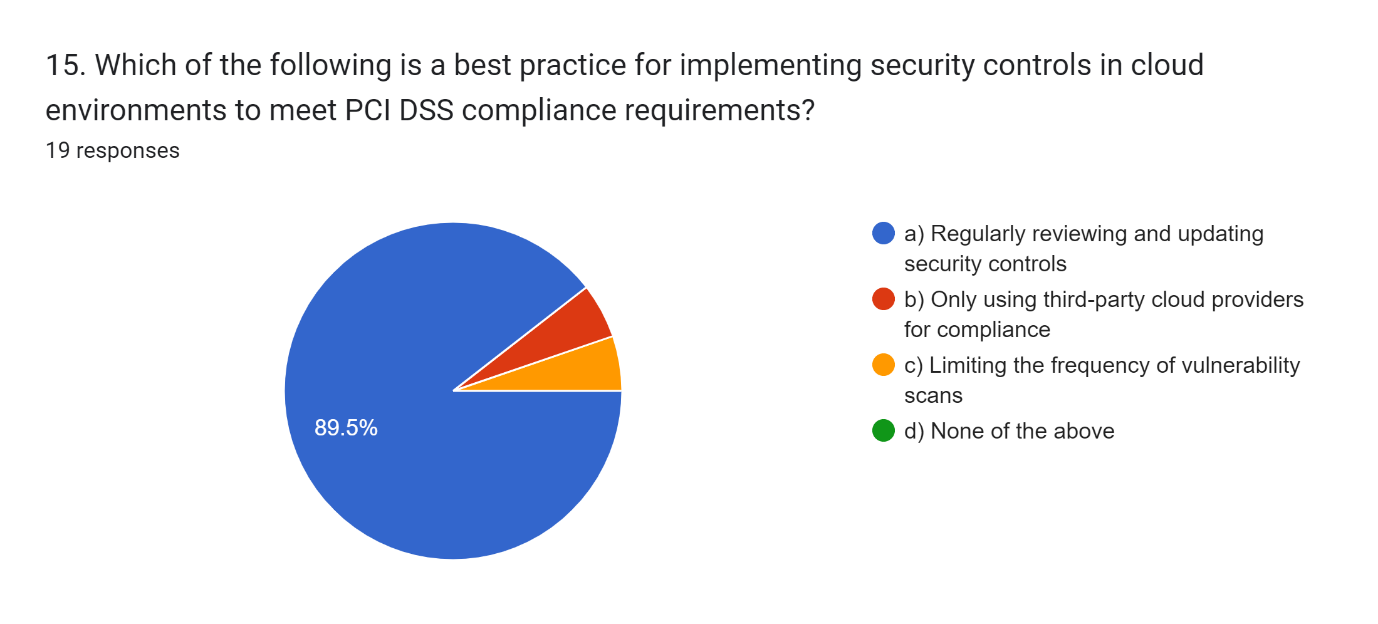


Fig.25: Implementing Security controls in cloud Environment

The poll and the responses provided insightful information about lowering fraud risk and weaknesses in PCI DSS compliance on the cloud. In order to help organisations, maintain compliance, emerging tech solutions are being researched.

## 4.2 Challenges and Recommendations

Organisations utilise a range of technologies to help assure compliance in cloud settings, and the technological landscape for PCI DSS compliance is continuously changing. Here are a few instances of the most recent technologies being used by business to ensure PCI DSS compliance and their challenges and how to resolve that issue:

4.2.1 Cloud Access Security Brokers (CASBs): For credit card data, businesses adopting cloud solutions must assure data security and PCI DSS compliance. CASBs can be useful, however they pose compliance difficulties. Solutions and suggestions are covered in this article (cybersecurity-insiders, 2021).

A picture containing text, screenshot, font, logo

Description automatically generated

Fig. 26: Pillars of CASB (SV-Networks, 2022)

**Challenges Faced by CASB on PCI DSS Compliance:**

1. Visibility and Control
2. Data Encryption
3. Access Control
4. Compliance Monitoring

**Resolutions to Solve the Challenges:**

1. Implementing a CASB Solution
2. Data Classification and Encryption
3. Multi-Factor Authentication

Businesses can employ MFA for users of cloud-based resources to comply with PCI DSS and prevent unauthorised access to payment card data (cybersecurity-insiders, 2021).

By evaluating the resource coverage and security of the CASB solution, updating the policies and authentication, and carrying out annual reviews and monitoring, you may ensure PCI DSS compliance (cybersecurity-insiders, 2021).

4.2.2 Container Security: Containerization introduces new security risks that need to be addressed to ensure the security and compliance of payment card data. Container security is crucial for PCI DSS compliance because a data breach in a containerized environment can lead to significant financial loss and damage to a company's reputation (Matteo Bisi, 2023).

Although containers are a more and more common way to deploy applications in the cloud, they also present new security risks that businesses must deal with. To guarantee that containers are correctly configured, secured, and monitored and to stop unauthorised access or data breaches, container security solutions offer tools (Gartner, 2022).

A diagram of a container security pillars

Description automatically generated with low confidence

Fig 27: Container Security Pillars (Matteo Bisi, 2023)

**Challenges in Container Security on PCI DSS Compliance**

1. Lack of Visibility
2. Vulnerability Management
3. Access Control
4. Compliance Monitoring
5. Data Protection
6. Network Security
7. Third-Party Integrations
8. Human Error

**Resolutions to Container Security Challenges on PCI DSS Compliance**

1. Implement a Comprehensive Security Strategy
2. Use Vulnerability Scanners
3. Enforce Access Control
4. Conduct Regular Compliance Audit
5. Encrypt Data at Rest and in Transit (Matteo Bisi, 2023).

4.2.3 Cloud-native Security Tools: In order to assist organisations in maintaining compliance in the cloud, cloud providers are increasingly providing native security tools and services. To improve security and compliance in cloud environments, these technologies may have automated compliance monitoring, threat detection, and access management functions ( Dr. Shue-Jane Thompson,Shamla Naidoo, Shawn DSouza, 2020).

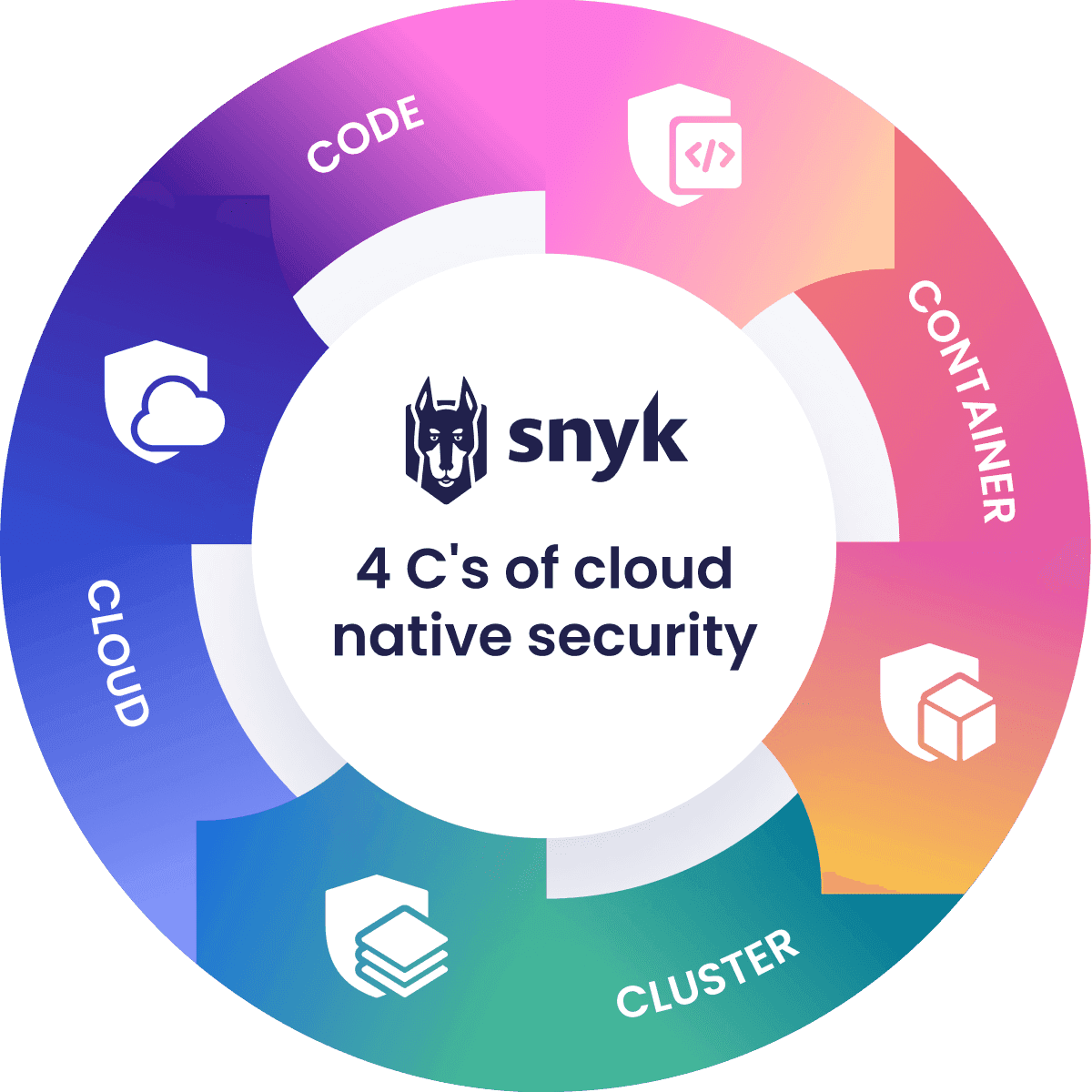


Fig 28: The 4c’s Pillars of cloud native security (Snyk, n.d.)

**Some of the challenges faced by cloud-native security tools in PCI DSS compliance include:**

1. Lack of visibility
2. Complex configurations
3. Compliance automation (Chen, S., Huang, M., & Tsai, W., 2021)

**To address these challenges, organizations can take several steps, such as:**

**Implementing cloud-native security tools that** are specifically designed to address the unique challenges of cloud environments, such as container security platforms.

**Leveraging automation** to increase visibility and decrease the amount of human work needed for compliance assessments.

To guarantee that security is embedded into the cloud-native environment from the outset, it is important to include **DevOps teams** in the compliance process as well as all other key stakeholders (Gragido, W., 2020).

Organisations can successfully use cloud-native security products to achieve and maintain PCI DSS compliance by following these steps.

4.2.4 Secure DevOps: In cloud environments, DevOps approaches are more common, and Secure DevOps practises are emerging as a way to include security into the DevOps process. Organisations may make sure that security is taken into account at every stage of the process, from planning to deployment, by integrating security into the software development lifecycle (NIST, n.d.).

A picture containing text, screenshot, diagram, font

Description automatically generated

Fig 29: The five key pillars of DevSecOps (gmgchow, 2020)

Secure DevOps is a methodology that combines the principles of agile development with security best practices. While Secure DevOps can help organizations develop and deploy secure applications, it can also present challenges when it comes to achieving and maintaining compliance with the Payment Card Industry Data Security Standard (PCI DSS).

**Some of the challenges faced by Secure DevOps in PCI DSS compliance include:**

1. Lack of security expertise
2. Rapid development cycles
3. Collaboration (Hsu, M. H., Chiu, C. Y., Wu, T. H., & Lee, W. , 2021)

**To address these challenges, organizations can take several steps, such as:**

1. Security-Focused Development
2. Early Vulnerability Detection
3. Collaborative Compliance Planning (Singh, S., & Rana, P., 2019)

By taking these steps, organizations can effectively leverage Secure DevOps to achieve and maintain PCI DSS compliance.

4.2.5 Identity and Access Management (IAM): In order to comply with PCI DSS, Identity and Access Management (IAM) is essential since it makes sure that only individuals with permission may access sensitive information. But in order to use IAM for PCI DSS compliance efficiently, a number of issues must be resolved (AWS, 2021).

**Some of the challenges faced by IAM in PCI DSS compliance include:**

1. Complexity
2. User management
3. Managing access for third-party vendors and service providers (Herath, T., Abawajy, J., & Lee, H., 2020)

**To address these challenges, organizations can take several steps, such as:**

1. Centralized IAM Integration
2. Automated User Provisioning
3. Robust Access Controls (Vignesh, S., & Selvam, S, 2019)

Cloud PCI DSS compliance is enabled by new technology. The optimal plan is a comprehensive approach, however it relies on the requirements of each organisation.

### 4.3 SWOT ANALYSIS:



Fig 30: SWOT Analysis

4.4 Research Reflection: Career Relevance: In order to ensure PCI DSS compliance in the cloud, one must be knowledgeable of current technology and legal requirements. My research exposed problems that organisations encounter, such as constant monitoring, access management, and security. These problems can be solved using best practises including multi-factor authentication, automation, and continuous monitoring. There is potential for development in my decision-making and communication, but my strengths in teamwork, technical skills, and problem-solving have been acknowledged. My research is pertinent to both my programme in cybersecurity and my professional goals. Companies may protect themselves against fraud threats and cloud vulnerabilities by staying up to date with technology and procedures.

4.5 Recommendations: Enhancing PCI DSS compliance in cloud contexts requires the use of cutting-edge machine learning methods.

* Automatic credit card transaction analysis made possible by machine learning makes it possible to identify potential security breaches in real time
* The risk of data breaches is reduced thanks to this proactive approach's strengthening of security measures and ability to quickly respond to attacks
* Data collection, pre-processing, feature engineering, model training, real-time monitoring, anomaly detection, warning creation, reaction and remediation, and model updates are a few of the tasks involved in putting machine learning into practise
* Organisations can use machine learning to maintain PCI DSS compliance, improve security, and safeguard sensitive data in the cloud by adhering to this algorithm (Meenu, Swati Gupta, Sanjay Patel, Surender Kumar, Goldi Chauhan, 2020)

# **Part B: Poster Presentation –**

The identification of critical obstacles and recommended practises for upholding compliance is the most important conclusion from my study project on ensuring PCI DSS compliance in cloud environments.

Using graphs, charts, and photos to graphically present my findings would be an excellent way to convey difficult ideas and facts.

I may complement my poster during my lightning session by delivering succinct and compelling information including significant findings, useful advice, and underlining the significance of PCI DSS compliance in the cloud.

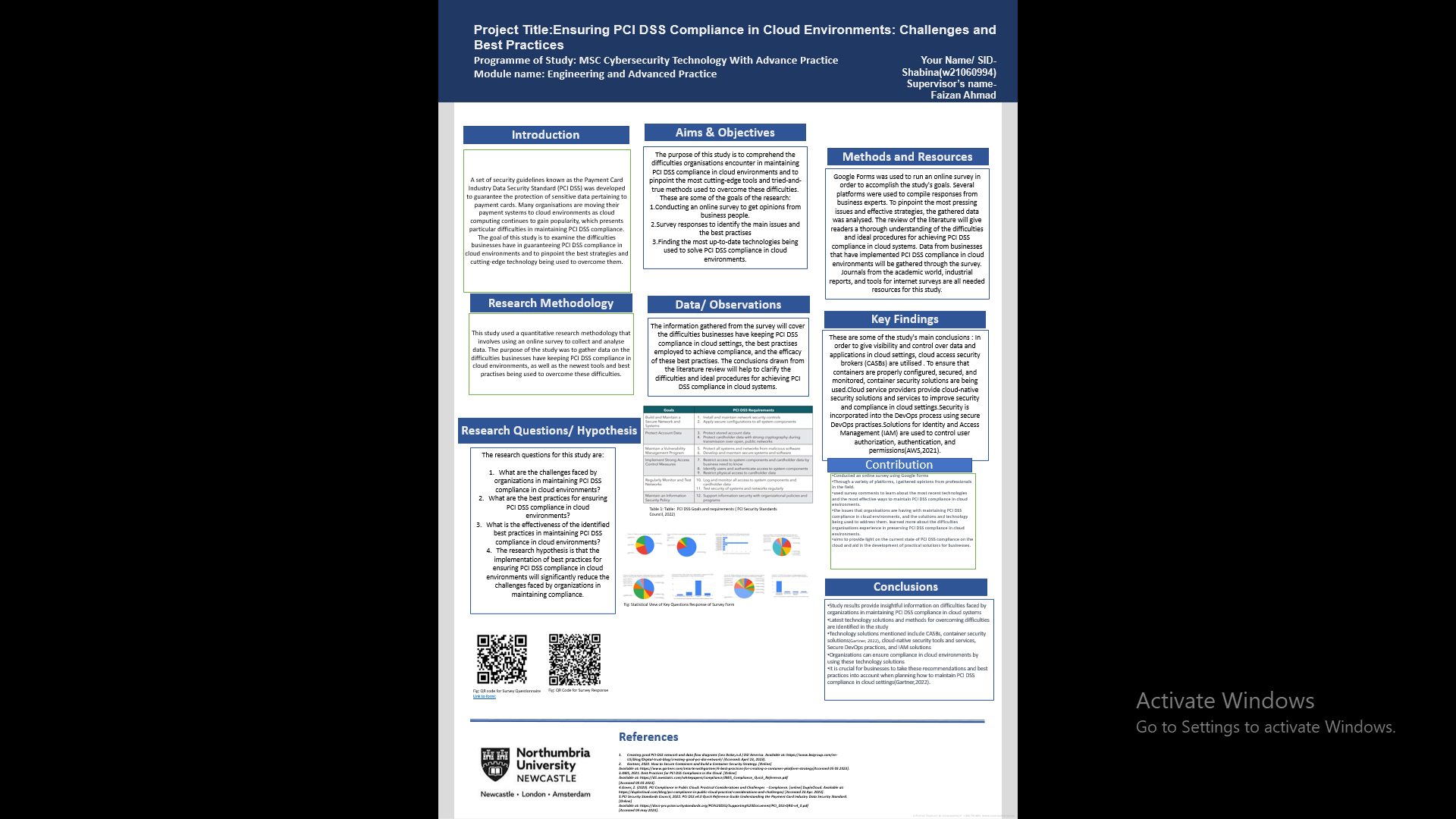


Fig.31: Poster Presentation on Ensuring PCI DSS Compliance in Cloud Environments: Challenges and Best Practices

**Click to access poster presentation 🡪**

Conclusion: The increasing importance of cloud computing in credit card data processing is the subject of my research, Ensuring PCI DSS Compliance in Cloud Environments. To obtain pertinent information, I used a variety of techniques, including an interdisciplinary literature review. My research intends to help firms achieve and maintain PCI DSS compliance in the cloud by highlighting obstacles and best practises. I am excited to add to the body of knowledge on credit card data compliance and cloud security, offering organisations handling payment card data in cloud environments helpful insights and recommendations.

# References

1. Dr. Shue-Jane Thompson,Shamla Naidoo, Shawn DSouza, 2020. *The new era of Cloud Security.* [Online]   
   Available at: https://www.ibm.com/downloads/cas/J6N8WRGG  
   [Accessed 05 05 2023].
2. PCI Security Standards Council, 2022. *PCI DSS v4.0 Quick Reference Guide Understanding the Payment Card Industry Data Security Standard.* [Online]   
   Available at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI\_DSS-QRG-v4\_0.pdf  
   [Accessed 04 05 2023].
3. PCI Security Standards Council, 2022. *What is the PCI Data Security Standard?.* [Online]   
   Available at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/General%20Guidance/PCI-DSS-v4-0-At-A-Glance.pdf  
   [Accessed 13 4 2023].
4. Aseem Rastogi , 2019. *Applying NIST Cybersecurity Framework to Cloud.* [Online]   
   Available at: https://www.cloudoptics.io/applying-nist-cybersecurity-framework-to-cloud/  
   [Accessed 10 5 2023].
5. Atlantic.Net Blog, 2021. *PCI Compliance in the Cloud: Challenges and Key Requirements.* [Online]   
   Available at: https://www.atlantic.net/pci-compliant-hosting/pci-compliance-in-the-cloud-challenges-and-key-requirements/  
   [Accessed 10 5 2023].
6. AWS, 2021. *AWS PCI DSS compliance..* [Online]   
   Available at: https://aws.amazon.com/compliance/pci-dss-faqs/  
   [Accessed 14 04 2023].
7. AWS, 2021. *Best Practices for PCI DSS Compliance in the Cloud.* [Online]   
   Available at: https://d1.awsstatic.com/whitepapers/compliance/AWS\_Compliance\_Quick\_Reference.pdf  
   [Accessed 05 05 2023].
8. Barrett, M., 2018. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework.* [Online]   
   Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf  
   [Accessed 10 05 2023].
9. Chen, S., Huang, M., & Tsai, W., 2021. *Cloud-Native Security Solutions for PCI DSS Compliance. In Proceedings of the 2021 International Conference on Cyber Security and Protection of Digital Services (pp. 1-7)..* s.l., IEEE.
10. CSA, 2020. *Using CSA STAR to Improve Cloud Governance and Compliance.* [Online]   
    Available at: https://cloudsecurityalliance.org/blog/2020/12/19/using-csa-star-to-improve-cloud-governance-and-compliance/  
    [Accessed 10 5 2023].
11. CSA, 2022. *Top Threats to Cloud Computing Pandemic Eleven.* [Online]   
    Available at: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/  
    [Accessed 03 05 2023].
12. CSA, 2023. *Security, Trust, Assurance and Risk (STAR).* [Online]   
    Available at: https://cloudsecurityalliance.org/star/  
    [Accessed 10 05 2023].
13. cybersecurity-insiders, 2021. *Challenges Faced by CASB on PCI DSS Compliance and Their Resolutions.* [Online]   
    Available at: https://www.cybersecurity-insiders.com/challenges-faced-by-casb-on-pci-dss-compliance-and-their-resolutions/  
    [Accessed 10 05 2023].
14. Europian Union, 2016. *General Data Protection Regulation.* [Online]   
    Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj  
    [Accessed 11 5 2023].
15. Fugue , n.d. *Achieving PCI DSS Compliance for Cloud Infrastructure.* [Online]   
    Available at: https://www.fugue.co/pci-cloud-compliance  
    [Accessed 10 05 2023].
16. Gartner, 2020. *Gartner Magic Quadrant for Cloud Access Security Brokers.* [Online]   
    Available at: https://www.gartner.com/en/documents/3992205  
    [Accessed 12 03 2023].
17. Gartner, 2022. *How to Secure Containers and Build a Container Security Strategy.* [Online]   
    Available at: https://www.gartner.com/smarterwithgartner/6-best-practices-for-creating-a-container-platform-strategy  
    [Accessed 05 05 2023].
18. George Mateaki, n.d. *PCI Compliance in the Cloud.* [Online]   
    Available at: https://www.securitymetrics.com/blog/PCI-compliance-cloud  
    [Accessed 04 05 2023].
19. Global Payments Integrated, 2020. *Global Payments Successfully Transitions to the Cloud with PCI DSS Compliance.* [Online]   
    Available at: https://www.globalpaymentsintegrated.com/en-us/resources/pci-compliance  
    [Accessed 10 5 2023].
20. gmgchow, 2020. *DevSecOps: What Is It and Why Is It Gaining Momentum in the Industry?.* [Online]   
    Available at: https://engineering.mercari.com/en/blog/entry/20201214-devsecops-what-is-it-and-why-is-it-gaining-momentum-in-the-industry/  
    [Accessed 13 5 2023].
21. Gragido, W., 2020. *PCI DSS Compliance in a Cloud Native World. Retrieved from.* [Online]   
    Available at: https://www.tripwire.com/state-of-security/security-data-protection/cloud/pci-dss-compliance-in-a-cloud-native-world/.  
    [Accessed 12 5 2023].
22. Graham Burnett, n.d. *How to use mind maps to revolutionise your note-taking.* [Online]   
    Available at: https://www.emeraldgrouppublishing.com/how-to/study-skills/mind-map  
    [Accessed 15 5 2023].
23. Herath, T., Abawajy, J., & Lee, H., 2020. An Identity and Access Management System for PCI DSS Compliance. *Journal of Network and Computer Applications,,* Volume 102710, p. 165.
24. Hsu, M. H., Chiu, C. Y., Wu, T. H., & Lee, W. , 2021. A Secure DevOps Methodology for Achieving PCI DSS Compliance.. *Journal of Information Security,* pp. 12(1),1-16..
25. Matteo Bisi, 2023. *Container Security 101: A Guide to Safe and Efficient Operations.* [Online]   
    Available at: https://thenewstack.io/container-security-101-a-guide-to-safe-and-efficient-operations/  
    [Accessed 12 5 2023].
26. Meenu, Swati Gupta, Sanjay Patel, Surender Kumar, Goldi Chauhan, 2020. Anomaly Detection in Credit Transactions using Machine Learning. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST),* 5, 8(3), pp. 2347-5552.
27. NIST, n.d. *DevSecOps.* [Online]   
    Available at: https://csrc.nist.gov/Projects/devsecops  
    [Accessed 05 05 2023].
28. Payment Card Industry Data , 2020. *Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 on AWS.* [Online]   
    Available at: https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf  
    [Accessed 08 05 2023].
29. Payment Card Industry Data, 2020. *Payment Card Industry Data Security Standard (PCI DSS).* [Online]   
    Available at: https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf  
    [Accessed 10 5 2023].
30. Payment Card Industry Security Standards Council, 2019. *PCI DSS Quick Reference Guide.* [Online]   
    Available at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI\_DSS-QRG-v4\_0.pdf  
    [Accessed 20 04 2023].
31. PCI Security Standards Council, 2019. *Cloud computing guidelines.* [Online]   
    Available at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4\_0.pdf  
    [Accessed 10 3 2023].
32. PCI SSC, 2018. *PCI SSC Cloud Computing.* [Online]   
    Available at: https://listings.pcisecuritystandards.org/pdfs/PCI\_SSC\_Cloud\_Guidelines\_v3.pdf  
    [Accessed 8 may 2023].
33. Peter Mell and Tim Grance, 2011. *The NIST Definition of Cloud Computing.* [Online]   
    Available at: https://www.nist.gov/system/files/documents/itl/cloud/cloud-def-v15.pdf  
    [Accessed 9 5 2023].
34. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. , 2009. *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds.* s.l., Association for Computing Machinery, p. 199–212.
35. Shaw, E., & Katzan, H., 2017. Ensuring PCI DSS compliance in cloud environments: Challenges and best practices. *Journal of Information Systems Applied Research,* Issue 10(3), pp. 41-51..
36. Singh, S., & Rana, P., 2019. *Implementing Secure DevOps for PCI DSS compliance. In 2019 11th International Conference on Computational Intelligence and Communication Networks (CICN).* s.l., IEEE..
37. Snyk, n.d. *Cloud Security - Essential to Your Cybersecurity.* [Online]   
    Available at: https://snyk.io/series/cloud-security/  
    [Accessed 10 5 2023].
38. SV-Networks, 2022. *What is CASB? Cloud Access Security Broker Overview.* [Online]   
    Available at: https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-casb  
    [Accessed 10 5 2023].
39. Verifone, 2021. *PCI.* [Online]   
    Available at: https://verifone.cloud/docs/uk-gateway/payments\_pci  
    [Accessed 10 5 2023].

40. Vignesh, S., & Selvam, S, 2019. Designing IAM for PCI-DSS Compliant Applications in the Cloud. *International Journal of Recent Technology and Engineering,* Volume 471-476, p. 8(1).