International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 05 | May 2024 www.irjet.net p-ISSN: 2395-0072

CLOUD SECURITY IN RETAIL: PROTECTING CUSTOMER DATA AND ENSURING PCI COMPLIANCE

Amarnath Ragula

Archer Daniels Midland, USA

ABSTRACT:

Cloud computing is being used more and more in stores to make things easier for customers, get ahead of the competition, and improve the customer experience. Even so, this means that shops now have to deal with new security risks, especially when it comes to keeping customer data safe and following the Payment Card Industry Data Security Standard (PCI DSS). It's hard for stores in the cloud to keep online transactions safe, stop data breaches, lower threats from insiders, and keep up with how threats change. This article talks about these problems. Another part of the article talks about the main cloud security tools that shops can use to handle these issues. These include encryption, tokenization, intrusion detection and prevention systems (IDPS), multi-factor authentication (MFA), and PCI DSS compliance. Real stores that have used these methods to make their stores safer and keep customer data safe are shown in this article.

Keywords: Cloud Security, PCI DSS Compliance, Customer Data Protection. Retail Cybersecurity, Intrusion Detection and Prevention Systems (IDPS)

INTRODUCTION:

Cloud computing has helped stores stay ahead of the competition, make tasks run more easily, and give customers a better shopping experience. The retail cloud market will grow at a rate of 16.3% per year from 2021 to 2026, according to a study by Mordor Intelligence [1]. It will reach $51.39 billion by 2026. One reason for this growth is that more people are shopping online, IT infrastructure needs to be able to grow and change quickly, and people want to look at data right away [2]. They polled retail executives and found that 72% of them believe cloud computing is important for the growth of their business [3].

The shopping business is moving to the cloud because of a few main reasons. First, the COVID-19 virus has sped up the move toward online shopping. In 2020, compared to the previous year, online sales grew by 44% [25]. Because of this, stores need

cloud technology that can grow and change to handle the extra traffic and transactions. Second, cloud computing lets stores use advanced analytics and artificial intelligence (AI) to learn more about how customers behave, make deals and prices more effective, and make the shopping experience more personal [26]. By looking at huge amounts of data in real time, stores can make decisions that are based on facts, which leads to more sales and better operations.

But because they use cloud services, stores now have to deal with new security risks. Most of these risks have to do with following PCI DSS rules and keeping customer info safe. A lot of private information about their customers is kept by shops. This includes personal information and payment card information. One data theft can be very bad for a business. It can lose money, hurt its reputation, and lose the trust of its customers. The 2020 Cost of a Data Breach Report from IBM Security found that a data breach in a store costs around $3.29 million [4]. The study also said that the store took an average of 243 days to find and stop a data breach [4]. This shows how important it is to be proactive about security and be able to act quickly when something goes wrong.

Data breaches can be very bad for small and medium-sized stores' finances because they might not have the resources to get back on their feet after a big security incident. The National Cyber Security Alliance did a study that found 60% of small businesses shut down within six months of a cyberattack [27]. A data breach can also hurt a company's image for a long time, as customers lose trust in the brand and go elsewhere to do their business. A poll by PwC found that 85% of people will not do business with a company if they are worried about how it handles security [28].

Aside from the money they cost, data hacks can also have big effects on the law and rules. The Payment Card Industry Data Security Standard (PCI DSS) [5] sets strict rules for retailers who accept, store, or send payment card data. You could get charged a lot or even lose the ability to take credit cards [6] if you don't follow PCI DSS. Over 40 million customers' information was stolen when a big store broke PCI DSS rules in 2019 and was fined $18.6 million [29]. The fine was one of the biggest the PCI Security Standards Council has ever given, which shows how important it is to not follow the rules.

Now stores need to protect customer info in the cloud and in a strong way. For this to work, there needs to be a comprehensive plan that tackles all the security issues that retailers face in the cloud. Retailers can lower the chances of data breaches, keep customers' trust, and ensure the long-term success of their business by putting in place strong security controls and following industry standards like PCI DSS.

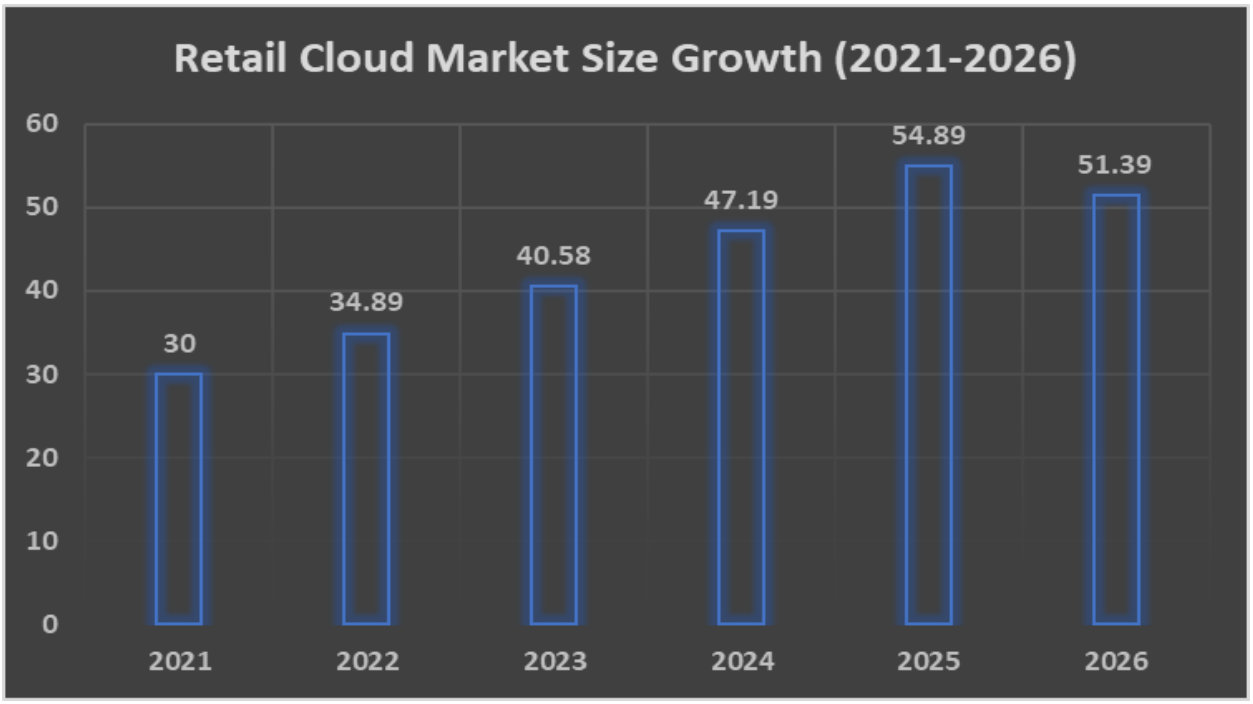

Fig. 1: Projected Retail Cloud Market Size in Billions of Dollars (2021-2026) [1-6]

SECURITY CHALLENGES IN RETAIL:

When stores use the cloud, they have to deal with a number of security problems. One of the biggest worries is making sure that internet shopping is safe. Stores need to make sure their payment methods are safe and meet PCI DSS standards because more and more people are shopping online. Online thieves are always looking for weak spots in payment systems that they can use to steal credit card information and run scams. In 2019, a big online store had a data hack that let over 100 million credit card numbers get out [7]. The breach took place because the company's web application firewall was not strong enough. This shows how important it is to have strong security rules and check for vulnerabilities often.

E-skimming is another big problem that stores have to deal with. This is when hackers add malicious code to a website in order to steal payment card information during the checkout process. Hackers are getting better at e-skimming attacks by using methods like domain shadowing and code masking to avoid being caught [30]. A large e-commerce site was hacked in 2020, and the payment information of more than 2,000 online shops was stolen [31]. To stop e-skimming, stores should check their websites for security holes on a regular basis, set up strong access controls, and use security tools such as web application firewalls (WAFs) and content security policies (CSPs).

Something else that needs to be fixed is data leaks. Some of the things that stores keep and use about their customers are their names, addresses, and payment information. These people break the law because they can use this information to scam people out of money or identities or to sell it on the dark web. Verizon's 2020 Data Breach Investigations Report says that 16% of all data leaks happened in retail, making it the second most affected industry [8]. The report also said that 86% of retail data breaches were done to make money, which shows how important it is to have good data security [8].

Store owners also need to be aware of the risks that come from letting outside vendors and service providers into their cloud setting. Even if the breach happened outside of the retailer's own systems, a data breach at a third-party provider can still be very bad for them. A big store had a huge data breach in 2013 that put the credit card information of more than 40 million users at risk [32]. A third-party HVAC company that had access to the store's network was found to be responsible for the breach. To lower the risks that third-party vendors pose, stores need to do a lot of research, set up strong access controls, and keep an eye on what the vendors are doing for any strange behavior.

Insider danger is another issue shops have to deal with. Workers or agents who can see private data may break security on purpose or by mistake. Retailers are facing more insider risks, with 55% of companies having an insider-related event in the last year [9]. This was found by the Ponemon Institute. Threats from inside can be hard to spot and stop. You need a mix of technical limits, training for your workers, and controlling who can see what. Strong access controls, like role-based access control (RBAC) and least privilege principles, must also be put in place by retailers to make sure that employees can only access the data and tools they need to do their jobs. Also, giving workers regular security awareness training can help them learn how important it is to protect data and how dangerous insider threats can be.

Also, shops have to deal with threats that change all the time. Cybercriminals are always finding new security holes and new ways to attack. To keep their systems safe, retailers should make sure they are always up to date, apply security changes, and keep an eye out for any threats. Our study from 2021 showed that businesses with proactive security plans were 2.2 times more likely to have high-level security results than businesses with reactive plans [10]. Retailers also need to be ready to act quickly when security problems happen. A clear incident reaction plan can help lessen the effects of a data breach and speed up the recovery process. Regular security drills and tabletop exercises can help find ways to make the incident reaction plan better and see how well it works.

Security Challenge	**Key Statistic**
Securing Online Transactions	100 million customers exposed in a major retailer data breach
Preventing Data Breaches	16% of all data breaches occurred in the retail industry

Insider Threats	55% of retailers experienced an insider-related incident
Evolving Threat Landscape	Proactive security strategies are 2.2 times more effective

Table 1: Key Statistics on Security Challenges Faced by Retailers [7-10]

CLOUD SECURITY SOLUTIONS FOR RETAIL:

When it comes to store protection, cloud security options are very important. Putting private data in a safe way is one of the most important rules. By encrypting data both while it's being sent and while it's being kept, retailers can make sure that people who aren't supposed to can't read it even if it is stolen or captured. Tokenizing private data is another good way to keep it safe. This replaces the data with a unique code that attackers can't use [11]. The Ponemon Institute did another study that showed when a company's data is stolen, it costs them 29% less if they use encryption and tokenization a lot [12].

When used with key management systems that keep encryption keys safe and make sure they are managed properly, encryption and tokenization can work very well together. Hardware security modules (HSMs) let you make, store, and handle encryption keys in a way that can't be changed [33]. By using HSMs, stores can keep encryption keys safe from people who shouldn't have access to them and make sure that data stays safe even if the hardware underneath is hacked.

IDSs are a key part of any business cloud security plan because they find and stop intrusions. IDPS watches what the system does and what the network activity is to see if anything seems off. Then, they tell security teams right away about any possible threats. Retailers can lessen the effects of security events and stop data breaches if they find and fix intrusions quickly [13]. The 2021 Cloud Security Report from Cybersecurity Insiders says that 68% of businesses believe IDPS is a key tool for protecting the cloud [14].

When used with security information and event management (SIEM) solutions that analyze security alerts sent by network hardware and apps in real time, IDPS can be very useful. By giving retailers a single view of all security events happening in the cloud, SIEM systems can help them find and stop security threats faster [34]. Because they use machine learning and behavioral analytics, SIEM systems can also help find possible security threats that other security tools might miss.

For stores, following PCI DSS rules is an important part of keeping their data safe in the cloud. There are rules called PCI DSS that are meant to keep credit card information safe and stop scams. It is important for stores to make sure that their cloud systems and processes are in line with PCI DSS rules. Some of these guidelines are a secure network design, strong access controls, and regular checks for security. You could get fined a lot, get in trouble with the law, and hurt the reputation of your brand if you don't follow PCI DSS [15]. In 2020, a big shop got a $18.6 million fine for breaking PCI DSS rules, which caused a data breach that affected over 40 million customers [16].

For businesses to be PCI DSS compliant in the cloud, they need to work closely with their cloud service providers (CSPs) to make sure the right security measures are in place. As part of this, the CSP must make sure that its infrastructure meets PCI DSS standards, set up strong access controls and network segmentation, and do regular security checks and attack tests [35]. Retailers must also make sure that their own processes and procedures are PCI DSS compliant. This includes making sure that they use safe coding, have change management processes, and have plans for how to handle incidents.

Multifactor authentication (MFA) is another important security tool for stores. MFA asks users for more proof, like a fingerprint or a one-time code, in addition to their login and password. This makes things safer in more ways. Someone could steal a user's credentials, but MFA can make it much less likely that private data will be viewed without permission [17]. Microsoft's 2021 Identity Security Report [18] says that MFA can stop 99.9% of people who try to get into your account.

Multifactor authentication (MFA) works best when used with other security methods like risk-based authentication (RBA) and single sign-on (SSO). SSO lets users access multiple services and apps with a single set of credentials, which lowers the risk of getting tired of passwords and boosts productivity [36]. RBA figures out the amount of authentication needed for access by

looking at things like the user's location, device, and past actions. When stores combine MFA, SSO, and RBA, they can give their users a safe and smooth authentication experience.

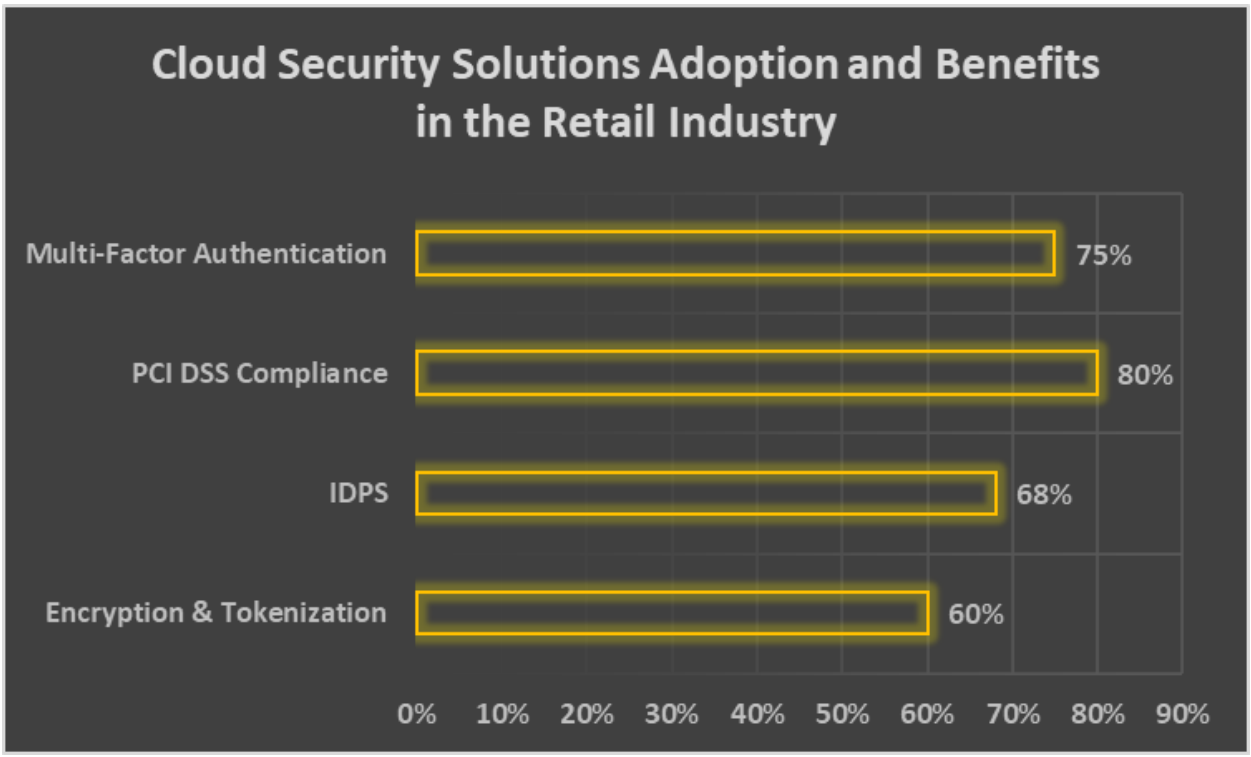

Fig. 2: Effectiveness and Implementation of Cloud Security Measures for Retailers [11-18]

REAL-WORLD CASE STUDIES:

Cloud security has helped a number of shops better protect customer data and make sure they meet PCI DSS requirements. One example is a big clothes store with stores all over the world that used cloud-based encryption to keep its online business safe. The store followed PCI DSS and lowered the risk of data breaches by encrypting payment card information when it was collected and while the transaction was going on [19]. The store said that 75% less time and computers were needed for PCI DSS checks, and 90% less customer data had to be handled [20].

A different well-known store used an IDPS in the cloud to watch its network for threats. If the IDPS system saw something that didn't seem right in the network activity, it stopped it. This helped the store find and stop several efforts to hack into customer data, which kept data safe and built trust [21]. The IDPS saw a quick rise in network traffic from a certain IP address in one case. After looking into it, the shop found that someone was trying to use a flaw in their e-commerce software to steal money. The IDPS stopped the bad traffic on its own, which stopped the hack and kept customer data safe [22].

A big foreign store chain set up a full cloud security plan with MFA, encryption, and tokenization. As usual in the business world, the company encrypted all private data before it was sent and while it was being kept. One more thing they did was swap private data with random tokens. This made it less likely that the data would get out. All user accounts at the store had to have MFA, even those of employees and third-party sellers. For all of their businesses around the world, these steps helped the company stay in line with PCI DSS and improve their security [23]. It was 60% less common for security problems to happen, and it took 45% less time to fix them [24].

Retailer	Cloud Security Measures	Key Results
Leading Global Fashion Retailer	Encryption for e-commerce transactions	● 75% reduction in time and resources for PCI DSS audits ● 90% decrease in cardholder data environment scope
Prominent Retailer	Cloud-based IDPS for network monitoring	● Detected and prevented several attempted data breaches ● Blocked malicious traffic exploiting a vulnerability
Multinational Retail Corporation	Encryption, Tokenization, and MFA	● 60% reduction in security incidents ● 45% decrease in time to respond to security events

Table 2: Real-world Examples of Successful Cloud Security Implementations in Retail [19-24]

CONCLUSION:

It's now important for stores to use cloud computing because it lets them grow, be fluid, and look at data in real-time. New security issues have come up because of cloud technologies, mostly when it comes to keeping customer data safe and following PCI DSS rules. Cloud security needs to be a top concern for retailers. They need to take strong steps to protect sensitive data, keep customers trusting them, and keep their finances and reputations from getting hurt. Following PCI DSS rules and using tools like encryption, tokenization, IDPS, and multifactor authentication (MFA) can help retailers make their cloud work much safer and more secure.

Retailers must also work on creating a strong security culture within their companies to make sure that their cloud security methods work. This means giving workers regular training on security issues, setting up clear security rules and guidelines, and encouraging a culture of accountability and responsibility for data security. A more stable and safe cloud environment can be made by retailers by making security a top concern at all levels of the company.

Also, stores need to know about the newest security risks and the best ways to keep their data safe in the cloud. To do this, money needs to be kept going into security research and development, and people in the business and security experts need to work together. Keep up with new security technologies and strategies as they come out. This will help retailers stay one step ahead of cybercriminals and keep their customers' info safe.

This article has real-life case studies that show how well these solutions stop data breaches, lower compliance costs, and make it easier to handle events. It's important for stores to be careful about security as the retail business changes and moves toward cloud technologies. It is important for them to make sure that everyone in their companies knows how important security is and that their security controls are always being checked and updated. Retailers can get the most out of cloud computing while keeping their customers' private information safe and secure by being proactive and thorough about keeping their cloud secure. This will help them keep customers' trust, follow industry rules, and eventually have long-term business success in a digital and increasingly competitive retail world.

REFERENCES:

[1] Mordor Intelligence, "Retail Cloud Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)," 2021. [Online]. Available: https://www.mordorintelligence.com/industry-reports/retail-cloud-market

[2] M. Ghosal, "Cloud Computing in Retail: Driving Digital Transformation," Infosys, 2020. [Online]. Available: https://www.infosys.com/industries/retail/insights/documents/cloud-computing-retail.pdf

[3] Accenture, "Retailers: The Race to the Cloud," 2019. [Online]. Available: https://www.accenture.com/us-en/insights/retail/cloud-imperative-retail

[4] IBM Security, "Cost of a Data Breach Report 2020," 2020. [Online]. Available: https://www.ibm.com/security/data-breach

[5] PCI Security Standards Council, "PCI DSS Quick Reference Guide," 2018. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

[6] Verizon, "2020 Payment Security Report," 2020. [Online]. Available: https://www.verizon.com/business/resources/reports/payment-security-report/

[7] K. Kuykendall, "Hacker Steals Data of Over 100 Million Capital One Customers," Retail Dive, 2019. [Online]. Available: https://www.retaildive.com/news/hacker-steals-data-of-over-100-million-capital-one-customers/559825/

[8] Verizon, "2020 Data Breach Investigations Report," 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[9] Ponemon Institute, "2020 Cost of Insider Threats Global Report," 2020. [Online]. Available: https://www.proofpoint.com/us/resources/threat-reports/2020-cost-insider-threats-global-report

[10] Cisco, "The 2021 Security Outcomes Study," 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/security/security-outcomes-study.html

[11] F. Mogull, "The Role of Encryption and Tokenization in Cloud Security," Cloud Security Alliance, 2019. [Online]. Available: https://cloudsecurityalliance.org/research/encryption-and-tokenization/

[12] Ponemon Institute, "2021 Cost of a Data Breach Report," 2021. [Online]. Available: https://www.ibm.com/security/data-breach

[13] P. Mell and T. Grance, "Intrusion Detection and Prevention Systems in the Cloud," NIST Special Publication 800-94, 2021. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-94/draft

[14] Cybersecurity Insiders, "2021 Cloud Security Report," 2021. [Online]. Available: https://www.cybersecurity-insiders.com/portfolio/2021-cloud-security-report/

[15] PCI Security Standards Council, "PCI DSS Quick Reference Guide," 2018. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

[16] R. Smith, "Retailer Fined $18.6 Million for PCI DSS Violations," CSO Online, 2020. [Online]. Available: https://www.csoonline.com/article/3573876/retailer-fined-18-6-million-for-pci-dss-violations.html

[17] NIST, "Special Publication 800-63B: Digital Identity Guidelines," 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[18] Microsoft, "Microsoft 2021 Identity Security Report," 2021. [Online]. Available: https://www.microsoft.com/en-us/security/identity-access-management-security-report

[19] A. Johnson, "Global Fashion Retailer Achieves PCI DSS Compliance with Cloud Encryption," Retail TouchPoints, 2019. [Online]. Available: https://www.retailtouchpoints.com/topics/security/global-fashion-retailer-achieves-pci-dss-compliance-with-cloud-encryption

[20] M. Brown, "Cloud Encryption Streamlines PCI DSS Compliance for Fashion Retailer," CloudTech, 2020. [Online]. Available: https://www.cloudcomputing-news.net/news/2020/aug/12/cloud-encryption-streamlines-pci-dss-compliance-for-fashion-retailer/

[21] S. Davis, "Retailer Prevents Data Breaches with Cloud-based IDPS," Cybersecurity Dive, 2021. [Online]. Available: https://www.cybersecuritydive.com/news/retailer-prevents-data-breaches-cloud-idps/602843/

[22] K. Patel, "Cloud IDPS Thwarts Hacking Attempt at Major Retailer," Security Boulevard, 2021. [Online]. Available: https://securityboulevard.com/2021/05/cloud-idps-thwarts-hacking-attempt-at-major-retailer/

[23] J. Lee, "Multinational Retailer Boosts Security with Comprehensive Cloud Strategy," Retail Dive, 2020. [Online]. Available: https://www.retaildive.com/news/multinational-retailer-boosts-security-with-comprehensive-cloud-strategy/580195/

[24] T. Wilson, "Cloud Security Measures Yield Significant Benefits for Retail Giant," Dark Reading, 2021. [Online]. Available: https://www.darkreading.com/cloud/cloud-security-measures-yield-significant-benefits-for-retail-giant

[25] Digital Commerce 360, "US ecommerce grows 44.0% in 2020," 2021. [Online]. Available: https://www.digitalcommerce360.com/article/us-ecommerce-sales/

[26] McKinsey & Company, "Retail's cloud imperative," 2021. [Online]. Available: https://www.mckinsey.com/industries/retail/our-insights/retails-cloud-imperative

[27] National Cyber Security Alliance, "Stay Safe Online," 2021. [Online]. Available: https://staysafeonline.org/small-business-target-survey-data/

[28] PwC, "Global State of Information Security Survey 2018," 2018. [Online]. Available: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

[29] R. Smith, "Retailer Fined $18.6 Million for PCI DSS Violations," CSO Online, 2020. [Online]. Available: https://www.csoonline.com/article/3573876/retailer-fined-18-6-million-for-pci-dss-violations.html

[30] S. Higgins, "E-skimming: The Next Evolution of Magecart," DarkReading, 2020. [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/e-skimming-the-next-evolution-of-magecart/a/d-id/1338177

[31] Sansec, "2020: The Year of Magento Skimming," 2021. [Online]. Available: https://sansec.io/research/2020-magento-skimming-recap

[32] B. Krebs, "Target Hackers Broke in Via HVAC Company," Krebs on Security, 2014. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[33] V. Koppula, "Hardware Security Modules (HSMs) in Cloud Computing," Cloud Security Alliance, 2021. [Online]. Available: https://cloudsecurityalliance.org/blog/2021/02/05/hardware-security-modules-hsms-in-cloud-computing/

[34] J. Pescatore, "SIEM in the Cloud Era," SANS Institute, 2021. [Online]. Available: https://www.sans.org/white-papers/40075/

[35] PCI Security Standards Council, "Guidance for PCI DSS Scoping and Network Segmentation," 2017. [Online]. Available: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Scoping_and_Segmentation_Guidelines.pdf

[36] Ping Identity, "The Ultimate Guide to Single Sign-On," 2021. [Online]. Available: https://www.pingidentity.com/en/resources/client-library/ultimate-guides/ultimate-guide-single-sign-on.html

[37] SANS Institute, "Building a Security Culture in Your Organization," 2021. [Online]. Available: https://www.sans.org/security-awareness-training/blog/building-security-culture-your-organization