Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9942270, 10 pages
https://doi.org/10.1155/2022/9942270

Research Article

Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS)

Muhammad Nasir Mumtaz Bhutta,[1] **Surbhi Bhattia**,[1] **Mohammed Ali Alojail**,[1] **Kashif Nisar**,[2] **Yue Cao**,[3] **Shehzad Ashraf Chaudhry**,[4] **and Zhili Sun**[5]

[1]*Information Systems Department, College of Computer Science and Information Technology (CCSIT), King Faisal University, Al Ahsa, Saudi Arabia*
[2]*Faculty of Computing and Informatics, University Malaysia Sabah, Jalan UMS, Kota Kinabalu, 88400 Sabah, Malaysia*
[3]*School of Cyber Science and Engineering, Wuhan University, China*
[4]*Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey*
[5]*Institute for Communication Systems, Department of Electrical and Electronic Engineering, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, UK GU2 7XH*

Correspondence should be addressed to Muhammad Nasir Mumtaz Bhutta; mmbhutta@kfu.edu.sa

Received 21 March 2021; Revised 17 May 2021; Accepted 17 December 2021; Published 24 January 2022

Academic Editor: Jun Cai

IoT emergence has given rise to a new digital experience of payment transactions where physical objects like refrigerators, cars, and wearables will make payments. These physical objects will be storing the cardholder credentials and will directly make payments with the vendors over insecure public networks. For such payment transactions, government regulations and standards organizations require to implement PCI DSS for adapting similar set of security measures at the global level. The current version of PCI DSS is not suitable for IoT-based payment systems due to characteristics of IoT such as resource-constrained nature of devices and updating software/firmware of so many physical devices. Also, there arises an emergent need of implementing PCI DSS requirements and assessments for security of all stakeholders that store or process the user credentials in a payment. This paper is an initial effort to bring the researcher's attention to make upcoming versions of PCI DSS suitable for IoT and thus securing the new ways of IoT-based payment systems. The paper has reviewed the traditional payment process along with considerations for IoT-based payment systems to make recommendations to modify the PCI DSS in a suitable way for IoT.

1. Introduction

IoT has emerged as a new phenomenon and has revolutionized the world once again after invention of computer systems [1]. The IoT emergence has given emergence to the development of smart cities [2], machine-to-machine economy where connected devices will interact with each other. This leads to a new digital experience of payment of transactions for both consumers and businesses. Consumers can pay using a wide of range of connected devices including connected cars, household appliances, and wearables. Businesses have also adapted new point of sales including touch points, parking meters, and vending machines [3].

IoT-based payments are going to change the way payments are made for purchases in-store, online, or on phone. Many companies have already started providing their products for payments based on IoT. Amazon has launched their payment product called "Amazon Go" to change the shopping experience. Customers receive the final bill when they leave the store after finishing their shopping without going to any checkout or waiting in lines for payment. Amazon deducts the payment from registered customer account [4]. A similar effort called "SMARTBUY" is done in [5] by linking the online shopping with a coalition of small retailers as a concept of "Distributed Shopping Mall." SMARTBUY introduces a blended retailing system of combining online shopping with the attractiveness of traditional shopping in stores. On the top, the added benefits for products and services by SMARTBUY are (i) centralized inventory management, (ii) geo-location-based marketing, (iii) location-based searching facility for neighboring retailers, and (iv) personalized recommendations for products by using different business analytics [5]. Another system developed by MasterCard is “Groceries”; it is an app developed based on Samsung family’s hub refrigerator to order groceries. The app was demonstrated to connect to groceries online shopping apps (FreshDirect and ShopRite) by using their provided open APIs [3, 6]. The Visa in association with Honda and Parkwhiz has also enabled cars to make payments for fuels. Similarly, Samsung and Visa are working on payment from refrigerator [7].

In the future, even more hardware devices will make payments to give a smoother experience to humans. For example, refrigerators will be able to detect the needed grocery and will the store to deliver the required items and payment will be done from credit card linked with refrigerator and car’s dashboard consoles will make payment for fuel after finding a suitable station during travel [3, 8]. NFC technology is being considered for initiating the vehicle toll payments at highways. A mobile having NFC initiates the toll payment for car in [9] supported by cloud-based web-based payment processing system.

However, with this advancement and increase in the number of endpoint devices, vulnerabilities have also increased. Some of the important security threats to be addressed are the security of the IoT payment device itself, data leakage and privacy due to inherent low resistance of IoT devices to data leakage, and distributed denial of services attacks [3, 10]. Many such problems are also highlighted in [11] with detailed discussion on Amazon Go. To combat these threats, compliance to Payment Card Industry Data Security Standard (PCI DSS) for payment card industry is required by government and payment industry. This lack of compliance can lead to fines, lawsuits, and other ever-present negative impacts of degraded public perception within the court of public opinion [7, 12–14].

The PCI DSS provides set of technical and operational requirements to protect cardholder’s account data to make payments. It requires all entities from payment card processing industry including merchants, processors, acquirers, issuers, and service providers to be involved in this process. PCI DSS also applies to all entities that store, process, or transmit cardholder account or authentication. PCI DSS is comprised of a minimum set of twelve security requirements to protect account data which may be enhanced by additional controls and practices according to risk. Additionally, it does not supersede any government or legal requirements set to any industry [7, 15, 16].

Therefore, to implement secure IoT payments, these connected IoT devices and payment systems must also comply with PCI DSS and Payment Application Data Security Standard (PA DSS) as per government and industry standard requirements as being practiced previously [14, 17]. The current version of PCI DSS is 3.2 and now looking forward to version 4 [15]. However, these IoT-based payment systems will not be able to comply with PCI DSS recommendations in its original form to achieve security due to inherent characteristics of IoT. There are a variety of IoT devices available in the market with varying level of capabilities for various types of applications. However, the paper discussion focuses on resource-constrained devices with limited capabilities as majority of IoT devices are resource constrained. Further, almost all types of IoT systems require efficiency anyways [1, 3]. These characteristics especially resource-constrained nature of devices, limited capability of operating systems, diverse array of hardware computing platform, frequent use of alternative networking protocols, updating software/firmware of so many physical devices, interconnectivity, physical aspects of things, heterogeneity, dynamic changes, enormous scale, safety and connectivity, and lack of documentation make it difficult to comply with PCI DSS [1, 3, 8, 18].

This is the main motivation of this paper to not only shape the upcoming versions PCI DSS to consider IoT-based payments but also highlight important relevant research issues for secure IoT payments and give recommendations for future research directions. So the main contribution of this paper is to make a first attempt to analyze the payment process and standard PCI DSS in detail for IoT-based payment system and make recommendations for extension in a suitable way for IoT. At the end, the paper is concluded in Section 4.

2. PCI DSS and Payment Systems

2.1. Purpose of PCI DSS. The purpose of PCI DSS is to enhance cardholder data security by providing consistent security measures globally for all entities involved in payment processing including merchants, processes, service providers, acquirers, and issuers. It provides the minimum technical and operational requirements for the security of cardholder data as summarized in Table 1. The security is achieved once these requirements are met. The PCI DSS also lays down the testing procedures to assess the security measures applied by the organization [7]. However, the PCI Data Security Council separates the security of payment application security from security of card payment processing as discussed in Section 2.2.

2.2. Payment Application Data Security Standard (PA DSS). PA DSS lays down the security requirements and assessment procedures to ensure implementation of recommended security measures for the organizations of payment applications. These requirements and assessment procedures are derived from PCI DSS requirements and assessment procedures. Thus, payment processing applications must be implemented in a PCI DSS compliant environment considering the recommendations of PA DSS [17]. The following points elaborate the relationship between PCI DSS and PA DSS [7, 16].

Table 1: Control objectives and security requirements of PCI DSS [7].

Control objectives	PCI DSS security requirements	PA DSS security requirements
CO1: build and maintain a secure network	R1: install and maintain a firewall configuration to protect cardholder data	RA1: do not retain full track data, card verification code, or value
	R2: do not use vendor-supplied defaults for system passwords and other security parameter	RA2: protect stored cardholder data
CO2: protect cardholder data	R3: protect stored cardholder data	RA3: provide secure authentication features
	R4: encrypt transmission of cardholder data across open, public networks	RA4: log payment application activity
CO3: maintain a vulnerability management program	R5: protect all systems against malware and regularly update antivirus software or programs	RA5: develop secure payment applications
	R6: develop and maintain secure systems and applications	RA6: protect wireless transmissions
CO4: implement strong access control measures	R7: restrict access to cardholder data by business need to know	RA7: test payment applications to address vulnerabilities and maintain payment application updates
	R8: identify and authenticate access to system components	RA8: facilitate secure network implementation
	R9: restrict physical access to cardholder data	RA9: cardholder data must never be stored on a server connected to the Internet
CO5: regularly monitor and test networks	R10: track and monitor all access to network resources and cardholder data	RA10: facilitate secure remote access to payment application
	R11: regularly test security systems and processes	RA11: encrypt sensitive traffic over public networks
CO6: maintain an information security policy	R12: maintain a policy that addresses information security for all personnel	RA12: encrypt all nonconsole administrative access
		RA13: maintain a PA-DSS implementation guide for customers, resellers, and integrators
		RA14: assign PA-DSS responsibilities for personnel and maintain training programs for personnel, customers, resellers, and integrators

(i) All applications implementing or not implementing PA DSS security measures are in scope of PCI DSS security requirements and assessments for storage, processing, and transmission of cardholder data

(ii) The PCI DSS assessment should verify that PA DSS payment applications are properly configured as per PCI DSS security requirements to minimize the potential breaches leading to compromise of cardholder's data

2.3. PCI DSS and PA DSS Requirements. PCI DSS lays down 12 security requirements (R1 to R12) usually classified into 6 groups (CO1 to CO6) called "control objectives" [7] as shown in Table 1.

These security requirements apply to all payment system components including computing devices, network devices, servers, and applications [7]. All the 14 PA DSS requirements as outlined in Table 1 are in line with PCI DSS requirements and are analyzed in Section 3 for IoT as well.

To understand the applicability of these requirements, it is vital to understand the payment working models and processes.

2.4. The Traditional Payment Process. Before discussing the process in detail, let us discuss first the entities and their roles in the payment process [16].

(1) Merchant: an organization who provides the payment facility via card payment terminal at their premises or via an online website by entering the card details

(2) Merchant acquirer: a merchant acquirer is a financial institution responsible for providing services to merchants for payment processing

(3) Payment card networks: there are two models for payment card networks. In the first model, payment card networks do not directly issue cards like MasterCard and Visa, and in the second model, payment card networks issue cards directly to customers like American Express. Such networks play two roles of merchant acquirer and payment network

The payment process consists of two steps: transaction flow and clearing and settlement of funds [16].

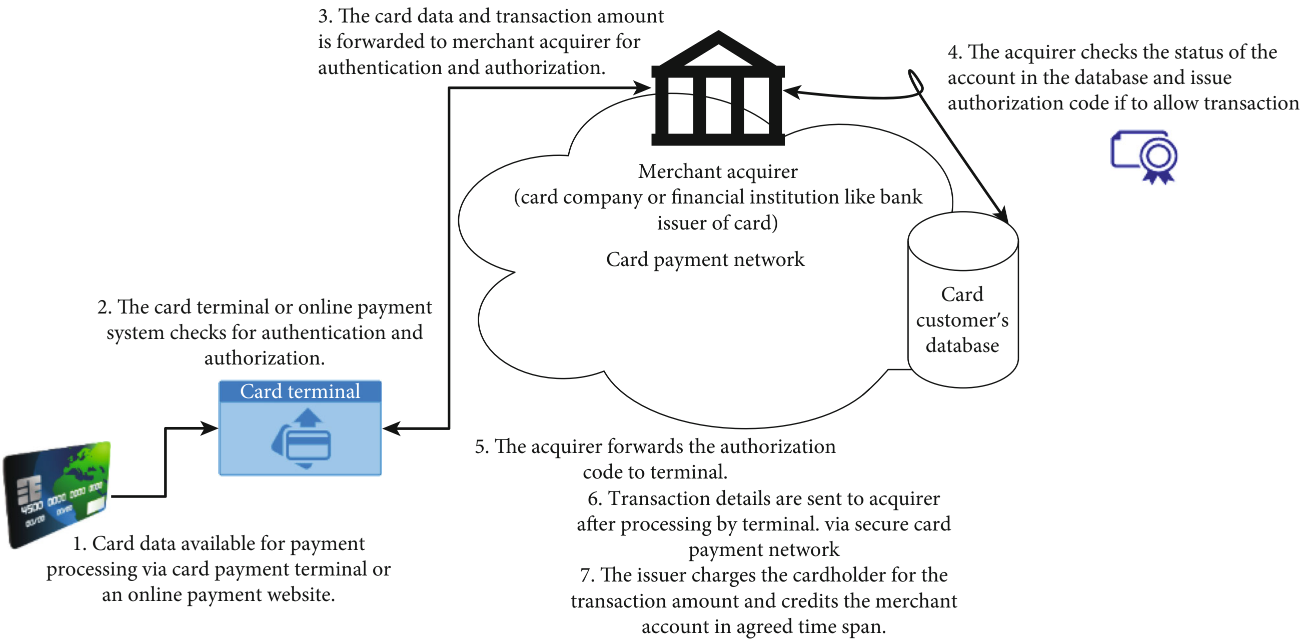
3. The card data and transaction amount is forwarded to merchant acquirer for authentication and authorization.
4. The acquirer checks the status of the account in the database and issue authorization code if to allow transaction
Merchant acquirer (card company or financial institution like bank issuer of card)
Card payment network
Card customer's database
2. The card terminal or online payment system checks for authentication and authorization.
Card terminal
5. The acquirer forwards the authorization code to terminal.
6. Transaction details are sent to acquirer after processing by terminal. via secure card payment network
7. The issuer charges the cardholder for the transaction amount and credits the merchant account in agreed time span.
1. Card data available for payment processing via card payment terminal or an online payment website.

Figure 1: The components of traditional point of sale-based payment process [16].

(1) Transaction flow: as shown in step 1 of Figure 1, the payment process begins after a customer swaps a card on a payment terminal (POS (point of sale)) or details of the card are entered on an e-commerce website. After that, the following steps are taken:

(i) The card payment terminal or website payment processing merchant records the card data, e.g., account number, the card type, expiry date, and other required data, and forwards it to the merchant acquirer as step 3 in Figure 1

(ii) The merchant acquirer then forwards the transaction data to the card issuer using a secure payment card network as described in step 4 in Figure 1. In some cases, the acquirer can directly authorize the transaction without getting verification from the issuer

(iii) The issuer then verifies the status of then customer account and replies to the merchant acquirer

(iv) The acquirer then forwards an authorization code to the card terminal device or website for completing the transaction process on successful verification of funds in database

In this transaction flow process, the actual funds are not collected; instead, it is merely a confirmation that issuer has authorized the transaction and agrees to settle the transaction with merchant customer and merchant acquirer. The funds are settled in a process called "clearing and settlement" [16].

(2) Clearing and settlement: the clearing and settlement processes start when the transaction details are sent to the acquirer as described from step 4 in Figure 1. Usually, the small merchants send the transaction details at the end of the day while the large merchants send the transaction details in real time [16].

The following steps are followed in this process [16]:

(i) The acquirer forwards the transaction data to the issuer via the appropriate payment card network (such as Visa and MasterCard) as mentioned in steps 5 and 6 in Figure 1

(ii) The issuer then charges the amount to the customer card and remits the funds to the acquirer via same secure payment card network as described in step 7 in Figure 1

(iii) The acquirer deducts the fees for issuer, the network, and itself before depositing the funds to the merchant's account

Typically, this process takes 24 to 72 hours for charging the customer and transferring funds to the merchant [16].

2.5. IoT-Based Payment Systems. Digital payments have evolved with inclusion of payment-enabled IoT devices. Customers can pay with a new range of connected devices including cars, household appliances like refrigerators, or wearables. The retail point of sales in relation to traditional payment process are changed as well with new touch points like parking meters, fitting mirrors, and vending machines [3, 19].

There are five key components of IoT-based payment systems [4]:

(1) Devices: IoT devices like cars and refrigerators trigger the payment for various payment technologies implemented depending upon the environment

(2) Connectivity: the connectivity channel is used by IoT devices for triggering the payment

(3) Credentials: the user credentials for payment are stored either in clouds or in edge computing device or in a secure local element

(4) Experience: there are different payment use cases according to consumer experiences ranging from voice command or pushing a button to a frictionless payment experience based on location and sensors

(5) Security: various security measures are used to authenticate the customer and transmission of these payment credentials

2.6. Taxonomy of IoT-Based Payment Models. The IoT payment landscape is not yet defined or standardized, and no one can predict the future with complete certainty. However, three different payment models are identified in literature as shown in Figure 2: (1) card scheme payment model, (2) bank credit transfer model, and (3) digital currency payment model. These models are abstract level descriptions of the payment process [20].

(1) Card scheme provider model: many international card scheme providers have successfully deployed noncard payment through payment tokenization technology. One example of tokenization is Near Field Communication (NFC), as a replacement of a Primary Account Number (PAN). The card tokenization can turn IoT devices into payment-enabled devices. For example, an autonomous vehicle can have a tokenized payment card installed in it which can be used to pay for all kind of services at gas stations, tolling, parking, drive-in restaurants, etc. The standardization of this model is being led by card scheme owners [20]

(2) Bank credit instant transfer model: instant payment is currently an exciting development in many countries including Europe and Middle East. The banks are executing payments in real time with this model if both the participating banks are participants of this scheme. An example of such technology being used in Europe is SCT Inst (SEPA Instant Credit Transfer) scheme. This scheme covers both person-to-person and person-to-business payments. The integration of instant payment systems with open APIs enables most of the IoT payment use cases that are imaginable with card scheme payments [20]

(3) Digital currency payment model: blockchain distributed ledger technology (DLT) is being considered very suitable for IoT environment. The distributed nature of blockchain allows IoT devices to have direct transactions with or without the involvement of a trusted third party. It is still uncertain how such digital currency-based payment model will be adapted in the future; however, a possible scenario is converging towards regulated digital currency networks where central banks will play a crucial regulating role as of blockchain nodes with possible interchange of different currencies. Currently, different standardization efforts are going on to help facilitate interoperability of digital currency networks [20, 21]. However, blockchains and DLT technologies will require further optimization to be truly effective as an IoT payment platform [21]

Whichever payment model or multiple models are used, the organizations will be required to implement PCI DSS recommendations to achieve a defined level of security according to compliance and regulatory authority recommendations. Let us discuss the considerations of IoT-based payments with above defined models in mind as compared to traditional payment systems.

2.7. Considerations for IoT-Based Payment Systems as Compared to Traditional Payment Systems. Despite many similarities between IoT-based payments and traditional payment process as described above, there are many differences as well. The IoT device itself is a payment component which can store, process, or communicate user credentials using cloud or any other technology like edge or fog computing. So, it raises the following considerations, based on IoT characteristics, for designing IoT-based payment systems in comparison to traditional payment systems [3, 19]:

(i) No physical POS is required in IoT-based payment systems as IoT devices can itself route the transaction to the network

(ii) The customer experience can vary depending upon the means to initiate the payment, e.g., voice command or a tap on a wearable

(iii) The customers can be recognized automatically based on smart sensors

(iv) The customer identity can be verified using biometrics or other technologies

(v) The payment card credentials can be stored on variety of hosts including a secure element or cloud or edge

(vi) IoT-based payments move from private controlled networks to public networks for processing of payments as IoT devices are connected to variety of public networks

(vii) IoT devices are in variety of form ranging from very resource-constrained devices to powerful machines. Devices can have limited capability and different ways to connect to payment network.

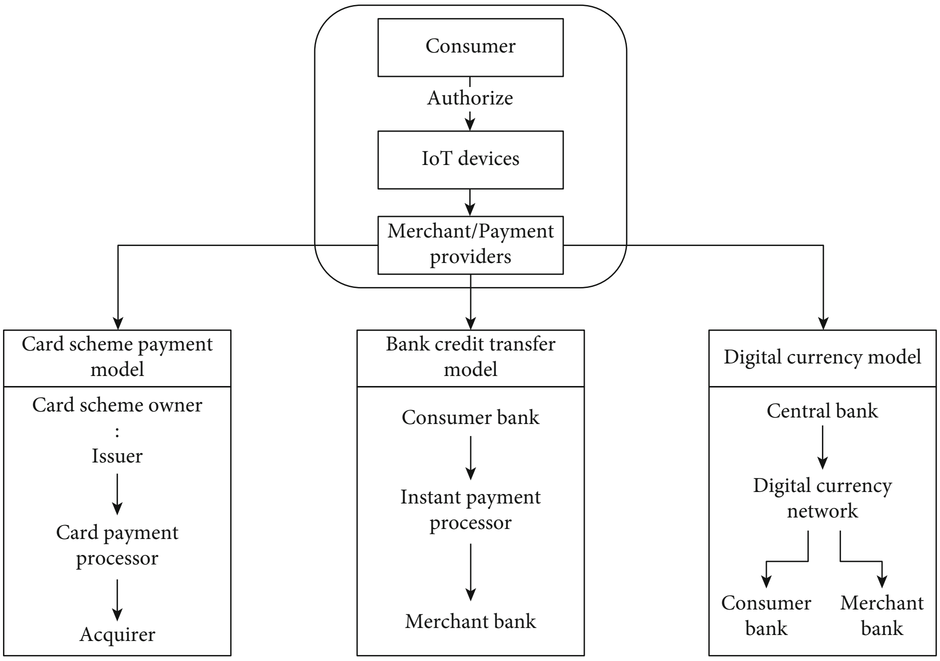

Figure 2: Taxonomy of IoT-based payment models [20].

So, all IoT devices cannot have the same resources and potential means for customization

(viii) There should be a special consideration for the capabilities of IoT devices for implementing security. That is the basic consideration in analysis of PCI DSS for IoT-based payments

(ix) There may not be a single authentication mechanism suitable for all IoT devices. So, adaptive authentication models may be adapted based on type of IoT system

(x) The trust model will also vary depending upon the capability and security of IoT devices and connectivity with third-party services

These considerations are important factors for the analysis of PCI DSS suitability for IoT.

3. Analysis of Extension of PCI DSS Suitability for IoT

This section analyzes the PCI DSS and PA DSS requirements and assessment procedures and gives recommendations for their extension for suitability of IoT as also summarized in Section 4. The IoT device lifecycle is an important consideration for applicability of PCI DSS and PA DSS, as the PCI DSS security requirements will apply to IoT device manufacturers for designing and building payment-enabled IoT devices and PA DSS will be applicable to cloud and connectivity API providers for storing and processing of user's credentials. The analysis has also taken into account the IoT characteristics and considerations for IoT-based payment systems.

3.1. Control Objective 1: Build and Maintain a Secure Network

3.1.1. PCI DSS and PA DSS Requirements, Assessment Procedures, and Guidelines. For building and maintaining a secure network, PCI DSS focuses on deployment of firewalls in personal computers as well as in networks and secure configuration of routers along with segregation of networks. It recommends deploying the servers like database servers and application servers in internal secure network. PCI DSS also emphasizes on explicitly changing the default vendor supplied passwords and security parameters before installing the IoT devices in the network [7]. In line with that, PA DSS put more focus on changing the default passwords of applications which are used for managing the user, application, and services accounts. It also recommends to use cryptography to securely store the account's data and deploy database servers in separate machines from application servers [17].

3.1.2. Analysis and Recommendations for IoT-Based Payment Systems. As discussed above, IoT devices may have limited capability to implement security measures. In this consideration, how can a resource-constrained IoT device implement personal firewall which should be active all the time to provide security? The limited power and computational capability of IoT devices will not allow such firewall installations, thus failing the compliance rule implementation on IoT devices. The firewalls must be modified to consider the resource-constrained nature of IoT devices. Already research efforts are going to design firewalls suitable for IoT in industry as well as academia as addressed in [22–24]. Furthermore, efficient suitable encryption/decryption mechanisms for low-powered IoT systems are also required. The traditional public key cryptography-based algorithms RSA and DSA and symmetric key cryptography-based algorithms like 3DES and AES will not be suitable for IoT-based payment systems [25]. The literature recommends to use Elliptic Curve Cryptography- (ECC-) based algorithms for IoT-based systems [26]. PCI DSS must consider the resource-constrained nature of IoT devices for this controlled objective of building and maintaining a secure network.

3.2. Control Objective 2: Protect Cardholder Data

3.2.1. PCI DSS and PA DSS Requirements, Assessment Procedures, and Guidelines. The cardholder data containing account number, cardholder name, service code, Personal Identification Number (PIN), security code, and expiration date must be protected according to control objective 2 [7, 16]. Fort this purpose, PCI DSS focuses on secure storage and transmission of cardholder data on the public unsecure Internet by relying on cryptographic encryption, authentication, authorization, and hashing mechanisms. It also takes extra measures by limiting the size of storage data and only allowing limited vendors and service providers to store the cardholder data in the payment network [7]. In line with it, PA DSS also recommends by not storing the cardholder data at most of the locations in the application and payment processing network with exceptions of limited controlled network locations. It emphasizes to implement strong authentication and authorization mechanism to access and process the cardholder data [17].

3.2.2. Analysis and Recommendations for IoT-Based Payment Systems. There are many considerations for IoT-based payment networks in this regard of securely storing and transmitting the cardholder data. The first most important one is that IoT devices have very small amount of memory and limited processing capability so cardholder data will be stored and processed in cloud to save computation and communication power of IoT devices. In this regard, research efforts are being focused on using tokens instead of actual exchange of cardholder data called tokenization in clouds [3, 27]. The other consideration is authentication of IoT device and relevant cardholder data. In traditional payment processing, the cardholder is authenticated by using PIN, but in IoT-based payment systems, the payment credentials are programmed in IoT devices and cardholder can be authenticated by sensors or even biometrics. Hence, PCI DSS must consider the diversity of authentication mechanisms depending upon the model of payments in IoT-based payment systems [3, 28].

3.3. Control Objective 3: Maintain a Vulnerability Management Program

3.3.1. PCI DSS and PA DSS Requirements, Assessment Procedures, and Guidelines. PCI DSS recommends all personal and organizational devices to be protected against malwares including viruses, worms, and trojans. It is recommended that all participating devices including personal computers must install antivirus software along with additional antimalware software. It is also recommended that all participating entities must regularly download and install the security patches from the vendors. These security patches are updated version of the software to address the recently known attacks or vulnerabilities in the system [7]. In this regard, PA DSS emphasizes on secure development of payment applications in accordance with industry standards and best practices to protect against at least well-known vulnerabilities like buffer overflow, insecure communication, and improper error handling. It is also recommended that any code change or addition must be reviewed for security issues before release. PA DSS recommends that any accounts, IDs, and passwords created during application development must be removed before installation of the payment application [17].

3.3.2. Analysis and Recommendations for IoT-Based Payment Systems. The major problems which can be encountered in IoT-based payment systems are as follows. (a) It will be difficult to regularly download and install the new security patches for so many IoT devices with extra consideration for their small-sized memory and limited computation power. (b) It will not be suitable to install antivirus and antimalware software to be installed on resource-constrained IoT devices. The diverse capabilities of IoT devices and diverse mechanisms to download and apply patches to these devices may put extra challenges for new version of PCI DSS suitability for IoT. However, research efforts are already in progress to address this issue, e.g., it is recommended to develop behavioral-based antimalware like Intrusion Detection/Prevention Systems (IDPS) for IoT-based systems rather than using signature-based systems where loaded signature databases can slow down the performance of IoT-based systems [29]. Some research efforts are also on the way to improve the behavior-based antimalware further by using machine learning techniques such as Hierarchical Extreme Learning Machine (H-ELM) [30] and machine learning techniques in Hardware-based Malware Detectors (HMDs) [31, 32]. Furthermore, spatial firewalls equipped with state-of-the-art security and antimalware programs are also being designed to protect the IoT-based systems [24].

3.4. Control Objective 4: Implement Strong Access Control Measures

3.4.1. PCI DSS and PA DSS Requirements, Assessment Procedures, and Guidelines. According to PCI DSS, access control systems and processes including authentication and physical access control must be implemented to ensure that critical account data is only accessible to authorized personal. It focuses on using cryptographic and other authentication means to valid users and provide limited access according to the roles and privilege levels. It must be ensured that users change their password regularly and security policies are in action all the times [7, 33–35]. In line with it, PA DSS recommends assigning unique IDs to all users, implementing multifactor authentication to validate them, and implementing password change and revocation policies to ensure security. It also emphasizes on implementing user

Table 2: Control objectives of PCI DSS and recommendations for IoT-based payment security.

Control objectives (COs) of PCI DSS	Recommendations to make security compatible for IoT-based payments
CO1: build and maintain a secure network	The firewalls must be modified to consider the resource-constrained nature of IoT devices.
CO2: protect cardholder data	(i) Cardholder data must be stored and processed in cloud to save computation and communication power of IoT devices. (ii) PCI DSS must consider the diversity of authentication mechanisms depending upon the model of payments in IoT-based payment systems.
CO3: maintain a vulnerability management program	(i) The security patches must be lightweight in terms of storage and computation and must be released in a fashion to optimize the memory usage for older releases. (ii) Antiviruses and antimalware must be designed suitable for resource-constrained natures of IoT devices for payments.
CO4: implement strong access control measures	There is also a need to pay special attention to physically access the individual IoT devices securely (e.g., physically accessing the refrigerator with installed security credentials) which have already installed cardholder credentials.
CO5: regularly monitor and test networks	The manufacturing and distribution models and day-to-day usage according to diverse capabilities of IoT devices must be considered for access control and logging activities.
CO6: maintain an information security policy	Over-the-air updates are being considered as a viable solution to update so many devices in IoT networks in a manageable way.

roles and access control mechanisms to only allow limited access to validated authorized users [17].

3.4.2. Analysis and Recommendations for IoT-Based Payment Systems. There are many considerations in this regard. The first one is providing varying methods of authentications and providing access controls to device manufacturers and service providers in a limited authorized way to process secure payments. Certificateless and blockchain-based solutions can be a way to provide such facilities [19, 21, 36]. There is also a need to pay special attention to physical access to IoT devices which have already installed cardholder credentials. These physical IoT devices are provided more vulnerable due to remote access for configuration and physical access for their easy deployment [3].

3.5. Control Objective 5: Regularly Monitor and Test Networks

3.5.1. PCI DSS and PA DSS Requirements, Assessment Procedures, and Guidelines. To track, alert, and analyze the user activities (including access to network resources and access to cardholder data by privileged users) must be monitored, logged, and regularly tested to store the user identification and event type along with date and time. PCI DSS also ensures that these audit logs are not alterable and any updation and deletion of these logs must also be recorded [7]. Besides that, PA DSS also recommends to store all the activities of the users for payment applications including additions, changes, and deletions to application accounts in the recommended format for logs.

3.5.2. Analysis and Recommendations for IoT-Based Payment Systems. To regularly monitor the network, the aspects related to storing and accessing the credentials in cloud or edge and in physical devices are of critical importance. Also, the manufacturing and distribution models and day-to-day usage according to diverse capabilities of IoT devices must be considered for access control and logging activities [3, 19].

3.6. Maintain an Information Security Policy

3.6.1. PCI DSS and PA DSS Requirements, Assessment Procedures, and Guidelines. PCI DSS also emphasizes to establish, publish, maintain, and disseminate a security policy to enforce all security requirements. It also encourages to educate all the permanent employees, temporary employees, contractors, and consultants of payment vendors to participate in enforcing the security policy. The security policies must be revised at least annually or with changes in environment [7]. In line with it, PA DSS encourage to pay special attention to payment application updates delivered via remote access. It focuses on the role of vendors to educate customers to keep remote-access off most of the time and only be turned on when needed from vendor and then turned off immediately [17].

3.6.2. Analysis and Recommendations for IoT-Based Payment Systems. The regular security updates of IoT firmware is of utmost importance in IoT research. Over-the-air (OTA) updates are being considered as a viable solution to update so many devices in IoT networks in a manageable way. The firmware updation of resource-constrained IoT devices is also an important consideration for extension of PCI DSS and for IoT research community.

4. Recommendations and Future Research Directions

Table 2 summarizes the recommendations drawn in this paper for each of the control objectives.

The future research directions in the light of above discussions for achieving security in IoT-based payment systems and drawing PCI DSS guidelines are listed below.

(i) Firewalls are very important components to achieve security for any IoT-based system. To design scalable and efficient firewalls for large rules set in a suitable way for IoT is a research topic of high importance for IoT and PCI DSS research communities. Furthermore, efficient antivirus and antimalware software are to be developed for IoT

(ii) Authentication methods based on biometrics, tokenization, and secure efficient methods to process the stored data in cloud are of great research interests as well

(iii) The regular updation of so many IoT resource-constrained devices of security is a challenging research issue. Over-the-air (OTA) types of methods to be defined

(iv) Blockchain- and certificate-based access control methods are recommended to be developed based on above research to provide access to card and IoT device's manufacturers for updating firmware

5. Conclusion

The next generation of interconnected payment-enabled IoT devices will play a significant role in consumers' and vendors' life by providing a unique payment experience. This process, of improving people's life by allowing the IoT devices to store user credentials and make payments in an autonomous way, must be secured by adapting the same PCI DSS requirements and assessment procedures at the global level. This paper has focused on highlighting that PCI DSS is not applicable to such IoT-based payments in its current form. PCI DSS must be modified by considering the issues highlighted in this paper to make it suitable for IoT. The important issues are highlighted in this paper, such as installing antiviruses, firewalls, and other antimalware on all resource-constrained IoT devices, addressing the unique diverse authentication requirements, over-the-air security updates for IoT devices, logging mechanisms, and implementing access control using blockchain must be addressed in research.

This paper presents the limited study in theory by critically analyzing the recommendations of PCI DSS and PA DSS for IoT-based secure payments. For future studies, it is highly recommended that the recommended security issues and technologies should be studied for implementation and practicability using simulations.

Data Availability

Data availability is not relevant for this paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the Deanship of Scientific Research, King Faisal University, Saudi Arabia, for partial financial support under Nasher track grant no. 206097.

References

[1] K. K. Patel and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International journal of engineering science and computing*, vol. 6, no. 5, 2016.

[2] K. Soomro, M. N. M. Bhutta, Z. Khan, and M. A. Tahir, "Smart city big data analytics: an advanced review," *WIREs Data Mining and Knolwedge Discovery*, vol. 9, no. 5, 2019.

[3] Secure Technology Alliance, "IoT and payments: current market landscape," version 1.0.

[4] Amazon, "Amazon Go," March 2020, https://www.amazon.com/b?ie=UTF8&node=16008589011.

[5] K. Wankhede, B. Wukkadada, and V. Nadar, "Just Walk-Out technology and its challenges: a case of Amazon Go," in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA),*, pp. 254–257, Coimbatore, India, 2018.

[6] MasterCard, "MasterCard, Samsung make everyday shopping easier in tomorrow's smart home with launch of Groceries by MasterCard app," May 2021, https://newsroom.mastercard.com/press-releases/mastercard-samsung-make-everyday-shopping-easier-in-tomorrows-smart-home-with-launch-of-groceries-by-mastercard-app/.

[7] DSS and PCI, *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2.*, PCI Security Standards Council, LLC, 2016.

[8] O. Ogundele, P. Zavarsky, R. Ruhl, and D. Lindskog, "The implementation of a full EMV smartcard for a point-of-sale transaction and its impact on the PCI DSS," in *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, pp. 797–806, Amsterdam, Netherlands, 2012.

[9] M. Woźniak, J. Siłka, M. Wieczorek, and M. Alrashoud, "Recurrent neural network model for IoT and networking malware threat detection," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5583–5594, 2021.

[10] S. A. Chaudhry, M. S. Farash, H. Naqvi, and M. Sher, "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography," *Electronic Commerce Research*, vol. 16, no. 1, pp. 113–139, 2016.

[11] A. Ensor, S. Schefer-Wenzl, and I. Miladinovic, "Blockchains for IoT payments: a survey," in *2018 IEEE Globecom Workshops (GC Wkshps*, pp. 1–6, Abu Dhabi, United Arab Emirates, 2018.

[12] S. Yulianto, C. Lim, and B. Soewito, "Information security maturity model: a best practice driven approach to PCI DSS compliance," in *2016 IEEE Region 10 Symposium (TENSYMP)*, pp. 65–70, Bali, Indonesia, 2016.

[13] J. Hizver and T.-c. Chiueh, "Automated discovery of credit card data flow for PCI DSS compliance," in *2011 IEEE 30th International Symposium on Reliable Distributed Systems*, pp. 51–58, Madrid, Spain, 2011.

[14] M. R. Shihab and F. Misdianti, "Moving towards PCI DSS 3.0 compliance: a case study of credit card data security audit in an online payment company," in *2014 International Conference*

on Advanced Computer Science and Information System, pp. 151–156, Jakarta, Indonesia, 2014.

[15] L. K. Gray, "PCI DSS: looking ahead to version 4.0," PCI DSS website, March 2020, https://blog.pcisecuritystandards.org/pci-dss-looking-ahead-to-version-4.0.

[16] Jing Liu, Yang Xiao, Hui Chen, S. Ozdemir, S. Dodle, and V. Singh, "A survey of payment card industry data security standard," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 3, pp. 287–303, 2010.

[17] PCI Security Sandards Council, "Payment application data security standard: requirements and security assessment procedures," in *Version 3*,, PCI Security Standards Council, 2013.

[18] M. Piazza, J. Fernandes, J. Anderson, and A. Olmsted, "Cloud payment processing without ritualistic sacrifices reducing PCI-DSS risk surface with thin clients," in *2016 International Conference on Information Society (i-Society)*, pp. 166–168, Dublin, Ireland, 2016.

[19] Z. Hao, R. Ji, and Q. Li, "FastPay: a secure fast payment method for edge-IoT platforms using blockchain," in *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, pp. 410–415, Seattle, WA, USA, 2018.

[20] M. Le and D. Hattab, "How IOT is shaping future payment models," Wordline Corporate, May 2021, https://worldline.com/en/home/knowledgehub/blog/2020/july/how-iot-shaping-future-payment-models.html#:~:text=IoT%2C%20opening%20up%20alternative%20payment%20models&text=The%20card%20tokenisation%20can%20be,drive%2Din%20restaurants%2C%20etc.

[21] R. R. Kanojia and S. Pathak, "Secured vehicle toll payment system using NFC," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, pp. 1–6, Pune, India, 2018.

[22] F5 network security for IoT, "Securing the number one attack target on the Internet: IoT devices," October 2020, https://www.f5.com/pdf/solution-center/f5-network-security-for-iot.pdf.

[23] A. M. Escolar, J. M. Alcaraz Calero, and Q. Wang, "Highly-scalable software firewall supporting one million rules for 5G NB-IoT networks," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[24] A. Zhaikhan, M. A. Kishk, H. ElSawy, and M.-S. Alouini, "Safeguarding the IoT from malware epidemics: a percolation theory approach," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 6039–6052, 2021.

[25] I. Chatzigiannakis, A. Vitaletti, and A. Pyrgelis, "A privacy-preserving smart parking system using an IoT elliptic curve based security platform," *Computer Communications*, vol. 89-90, pp. 165–177, 2016.

[26] L. Bourg, T. Chatzidimitris, I. Chatzigiannakis et al., "Enhancing shopping experiences in smart retailing," *Journal of Ambient Intelligence and Humanized Computing*, vol. 1-19, pp. 1–19, 2021.

[27] B. Ozdenizci, V. Coskun, K. Ok, and T. Karlidere, "Significance of tokenization in promoting cloud based secure elements," in *Conference on Big Data, IoT and Cloud Computing (BIC)*, pp. 1–12, Osaka, Japan, 2015.

[28] Y. Chen, W. Xu, L. Peng, and H. Zhang, "Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT," *IEEE Access*, vol. 7, pp. 15210–15221, 2019.

[29] K. Hughes and Q. Yanzhen, "Performance measures of behavior-based signatures: an anti-malware solution for platforms with limited computing resource," in *2014 Ninth International Conference on Availability, Reliability and Security*, pp. 303–309, Fribourg, Switzerland, 2014.

[30] O. Eboya, J. B. Juremi, and M. Shahpasand, "An intelligent framework for malware detection in Internet of things (IoT) ecosystem," in *2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC)*, pp. 1–6, Kuching, Malaysia, 2020.

[31] A. P. Kuruvila, S. Kundu, and K. Basu, "Analyzing the efficiency of machine learning classifiers in hardware-based malware detectors," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 452–457, Limassol, Cyprus, 2020.

[32] A. P. Kuruvila, S. Kundu, and K. Basu, "Defending hardware-based malware detectors against adversarial attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 9, pp. 1727–1739, 2021.

[33] S. A. Chaudhry, M. S. Farash, N. Kumar, and M. H. Alsharif, "PFLUA-DIoT: a pairing free lightweight and unlinkable user access control scheme for distributed IoT environments," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4431–4438, 2021.

[34] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244–139254, 2020.

[35] M. Rana, A. Shafiq, I. Altaf et al., "A secure and lightweight authentication scheme for next generation IoT infrastructure," *Computer Communications*, vol. 165, no. 1, pp. 85–96, 2021.

[36] K.-H. Yeh, "A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments," *IEEE Systems Journal*, vol. 12, no. 2, pp. 2027–2038, 2018.