Personal Shopper Device

Architecture Design Document

Version 2.4

January 16, 2016

Authors:

Jordan Callero,
Sukhman Ghumman,
Hunter Hammond,
Conor Leeds,
Nanya Ugwuh.

Mentor:

Christopher WIldt

Seattle Boffins

IASA

Table of Contents

Version Number	Changes
2.4	Added References
2.3	Minor grammatical changes and added overview of Infrastructure Architecture Layers
2.2	Small formatting changes
2.1	Added information to Technology Stack, Security Architecture, and minor grammatical fixes
2.0	Added Descriptions and Rearranged document
1.0	

1. Overview

This document will provide the Infrastructure, Security, and Application Architecture. It will also justify the technological decisions made for the Personal Shopper Device.

2. Application Architecture

The application architecture describes the behaviour of the application for the Personal Shopper Device. It is focused on the categorization and interactions between different components of the system. The applications architecture is specified on the basis of business requirements.

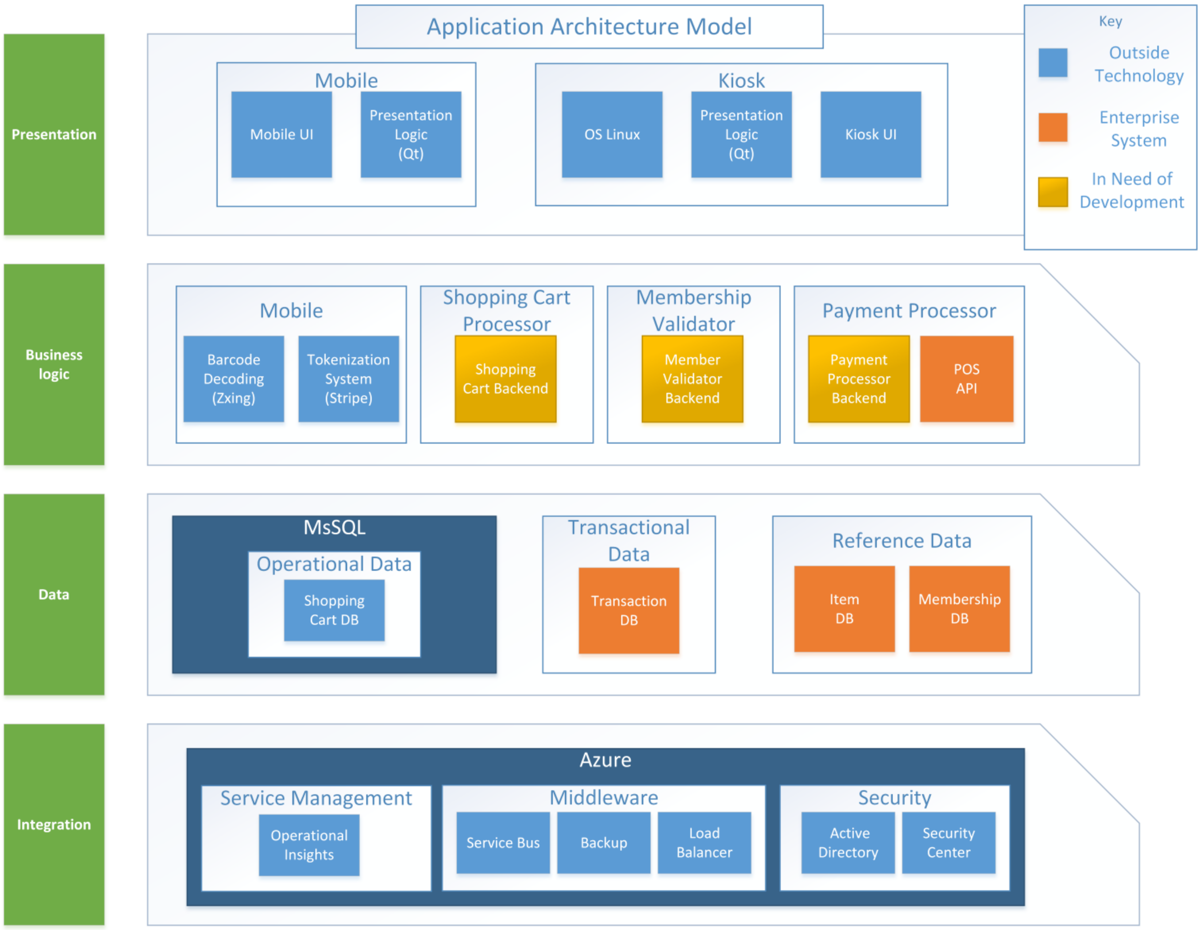

Figure 1: Application Architecture Model

2.1 *Application Architecture Overview*

The four main categories in the application architecture are presented in the following table:

Application Layer	Description
Presentation	The presentation layer contains the components responsible for displaying user interfaces as well as the logic which manipulates how business objects are displayed.
Business Logic	Components in the business layer are responsible for encoding business rules, which in turn determine how the application's data is calculated or transformed.
Data	Data creation, access, and modification are controlled in the data layer. This includes databases specific for this application as well as existing enterprise databases.
Integration	Integration layer components exist to integrate existing enterprise applications through services, which include Service Management, Middleware, and Security.

Table 1: Application Layer Overview

2.2 Application Architecture

The components of the Architecture are presented in the following table.

Application Layer	Component	Sub-Component	Description
Presentation	Mobile	UI	The application’s user interface for all personal or in-store mobile devices, which receives input for all shopping actions and some payment options.
		Presentation Logic (Qt)	The application logic which controls the presentation of business objects, such as the shopping cart, member authentication, and checkout, to the mobile user. This will be implemented using the Qt framework.
	Kiosk	OS Linux	The chosen operating system for running the Kiosk.
		Presentation Logic (Qt)	The application logic which controls the presentation of business objects, such as the shopping cart, and checkout, to the kiosk user. This will be implemented using the Qt framework.
		UI	The application’s user interface for all kiosks, which receives input for shopping cart modifications and all payment options.
Business Logic	Mobile	Barcode Decoding (Zxing)	The module responsible for barcode image processing/decoding into a numerical format. Zxing (“zebra crossing”) is an open-source, multi-format 1D/2D barcode image processing library implemented in Java, with ports to other languages.
		Tokenization System (Stripe)	The module responsible for tokenizing sensitive information transported over the network, such as credit card information. Stripe is an open-source software development kit for collecting credit card details within our mobile application through the creation of tokens.
	Shopping Cart Processor	Shopping Cart Backend	The business logic responsible for managing the flow of payment and shopping cart information. This component interacts with existing infrastructure such as transaction history and item databases.
	Membership Validator	Membership Validator Backend	The business logic responsible for returning the state of a member’s membership, such as active, expired, or blocked. This component queries an existing member validation database.
	Payment Processor	Payment Processor Backend	The business logic responsible for validating transaction payment, interacting directly with the point of sale system (POS) as well as the shopping cart processor.
		POS API	The application programming interface for the point of sale system (POS). Used by the payment processor backend for completing transactions.
Data	Operational Data	Shopping Cart DB	Contains current shopping cart session information, such as items, quantities, prices, current balance, tokenized payment information, as well as transaction receipts.

	Transactional Data	Transaction DB	Enterprise database which contains archived transactions. Transaction receipts from the shopping cart DB are transferred here upon completion of a shopping session.
	Reference Data	Item DB	Enterprise database which contains item information relevant to a particular store. This information is retrieved from an item master database. Lookup is achieved using numerical barcode data.
		Membership DB	Enterprise database which contains membership information, such as current state of membership (active, expired, blocked), as well as personal information, such as names, addresses, registered devices, and stored payment options.
Integration (Azure)	Service Management	Operational Insights	SaaS solution for collecting, storing, and analyzing log data, which is then turned into real-time operational intelligence.
	Middleware	Service Bus	Generic, cloud-based messaging system for connecting applications, services, and devices.
		Backup	Protection for critical applications such as files, folders, mail servers, SQL servers, as well as virtual machines.
		Load Balancer	Automatic scaling with increasing application traffic. Supports TCP/UDP-based protocols such as HTTP, HTTPS, and SMTP.
	Security	Active Directory	User and group cloud management solution which helps secure access to on-premises and cloud applications.
		Security Center	Configure security of Azure resources, such as firewalls and antimalware.

Table 2: Application Layer In-Depth

2.3 Business Requirement Mapping

The justification for fulfilling the business requirements are presented in the following table.

Business Requirements	**Architecture Components**	**Description**
R-1.1	Mobile UI/Presentation Logic (Qt)	Allows shoppers to access the application through a mobile device.
R-1.2	Mobile UI/Presentation Logic (Qt) Membership Validator Backend Membership DB	Ensures the full application functionality is available only to shoppers with an active membership.
R-1.3	Mobile UI/Presentation Logic (Qt) Membership DB	Shoppers may deregister past mobile devices using another mobile device.
R-1.4	Mobile UI/Presentation Logic (Qt) Membership DB	Displays a login page for shoppers to login or create a new membership.
R-2.1	Membership Validator Backend Membership DB	Able to retrieve and verify membership through integration with the existing verification system.
R-2.2	Mobile UI/Presentation Logic (Qt) Membership Validator Backend Membership DB	Allows shoppers to verify membership through manual entry or card scanning/image processing.

R-2.3	Mobile UI/Presentation Logic (Qt) Membership Validator Backend Membership DB	Displays a greeting upon successful member verification.
R-2.4	Mobile UI/Presentation Logic (Qt) Membership Validator Backend Membership DB	Notifies shoppers if their membership has expired and provides renewal options.
R-3.1	Mobile UI/Presentation Logic (Qt) Barcode Decoding (Zxing) Shopping Cart Backend Item DB	Supports application barcode scanning/image processing and subsequent item lookup.
R-3.2	Mobile UI/Presentation Logic (Qt) Kiosk UI/Presentation Logic (Qt) Shopping Cart Backend Shopping Cart DB	Allows shoppers to modify the quantity of scanned items in their shopping cart.
R-3.3	Mobile UI/Presentation Logic (Qt) Kiosk UI/Presentation Logic (Qt) Shopping Cart Backend Shopping Cart DB	Allows shoppers to create, view, update, or delete scanned items from their shopping cart.
R-3.4	Mobile UI/Presentation Logic (Qt) Kiosk UI/Presentation Logic (Qt) Shopping Cart Backend Shopping Cart DB	Asks for user confirmation before deleting scanned items from the shopping cart.
R-4.1	Mobile UI/Presentation Logic (Qt) Kiosk UI/Presentation Logic (Qt) Tokenization System (Stripe) Shopping Cart Backend Shopping Cart DB Payment Processor Backend	Supports transaction payment via card, cash, check, and other forms of electronic payment.
R-4.2	Transaction DB Shopping Cart Backend	Updates transaction database with newly archived transaction data.
R-4.3	Shopping Cart Backend	Resets an in-store mobile device upon completion of a transaction.
R-4.4	Tokenization System (Stripe) Payment Processor Backend POS API	Processes payments by transferring data over the store’s internet connection before handing the information off to the POS.
R-4.5	Membership DB Shopping Cart Backend Payment Processor Backend	Allows payments to be made through retrieval of a stored payment option.
R-4.6	Mobile UI/Presentation Logic (Qt) Kiosk UI/Presentation Logic (Qt) Shopping Cart Backend Shopping Cart DB	Generates receipt of transaction to be printed at a kiosk, as well as emailing an optional e-receipt.
R-5.1	Shopping Cart Backend Shopping Cart DB	Tracks current shopping cart information during a particular shopping cycle.
R-6.1	Transaction DB Shopping Cart Backend Shopping Cart DB	Archives and resets shopping cart at the end of a particular shopping cycle.

Table 3: Business Requirement Mapping

3. Security Architecture

Security Architecture focuses mainly on information security throughout the enterprise.

3.1 Data Analysis

3.1.1 Data Classifications

Two Types of Data: Classified and Unclassified. Unclassified data is anything that would be public knowledge and would not be considered a security or legal risk if leaked. Things like item prices, item identifiers, and shopping lists. Classified data is any personal data of the customer or any sensitive data from the company that would cause a security or legal risk if leaked. Things like credit card numbers, shopper information.

3.1.2 Data Security

Data Security measures will be different depending on whether or not information is Unclassified or Classified. While everything will be sent over encrypted means, any classified information will be tokenized whenever possible. Additionally any classified information sent over wireless MUST be tokenized and will be authenticated once the information has been sent.

3.1.3 Data Logging

Every action taken by a User of the Personal Shopper device system will be logged within the same server as the personal shopper. Additionally all data logged will be stored on a separate Server that can only be accessed by a System Administrator.

3.1.4 Data Redundancy

All data in the Personal Shopper system must have a hot standby server ready at all times, and every piece of data must also have at least two backup locations to store the data for as long as company policy dictates.

3.1.5 Login Information Storage

All login information will be kept encrypted at all times. Plaintext Usernames and Passwords will never be transferred over any wired or wireless communication. Usernames and Passwords for Users and Store Associates will be kept at the Store Server. Usernames and Passwords for Store Managers and System Admin will be kept at the main corporate office.

3.2 Compliance Enablement

3.2.1 Role-Based Access

Every privilege from a lower level user is authorized for a higher level user. A cellular device can only have the privilege level of User.

User Level	Function
Shopper	Ability to scan, remove, and change the quantities of items.
	Ability to send shopping list to Kiosk.
Store Associate	Ability to access Shopper Lists and modify them.
	Ability to modify item prices on a Shopper List within the limitations of an Associate.
Store Manager	Ability to modify item prices on a Shopper List within the limitations of a Store Manager.
	Ability to view logs of all actions done by Shoppers, Store Associates, and Store Managers for their specific store location.
	Ability to authorize a device for wireless access.
System Admin	Ability to view all logs of all actions done by System Administrators.
	Ability to access logs from all store locations.

Table 4: User Privileges

3.2.2 Role Authorization

This section details the only circumstances any user can rise above the rank of Shopper.

User Level	Circumstance
Store Associate	A Store Manager or System Admin may create a Store Associate User. This will be done as the associate is being hired. Whenever someone is hired a Username and Password will be created for them before their first day of work.
Store Manager	A System Admin may promote a Store Associate User to the rank of Store Manager in the event a new manager is being hired. They will be given a new Username and Password and if there is an old Username and Password, it will be deleted as soon as the Store Manager account is created.
System Admin	Only the Chief Security Officer of the company can authorize and create a System Admin User.

Table 5: Role Authorization

3.3 Fraud Detection

3.3.1 Wired Fraud Prevention

Any Wired Access to any level of User above Shopper will require two factor authentication. A username and password and then a time sensitive entry sent to the person through an alternative form of identification.

3.3.2 Wireless Fraud Prevention

Any Wired Access to any level of User above Shopper will require two factor authentication. A username and password and then a time sensitive entry sent to the person through an alternative form of identification. Additionally any wireless connection made from a device must be authorized to do so. Only a Store Manager or a System Administrator can Authorize wireless device connections.

3.4 Relationships

The following diagram and table illustrate the communication network for the Personal Shopper Device system.

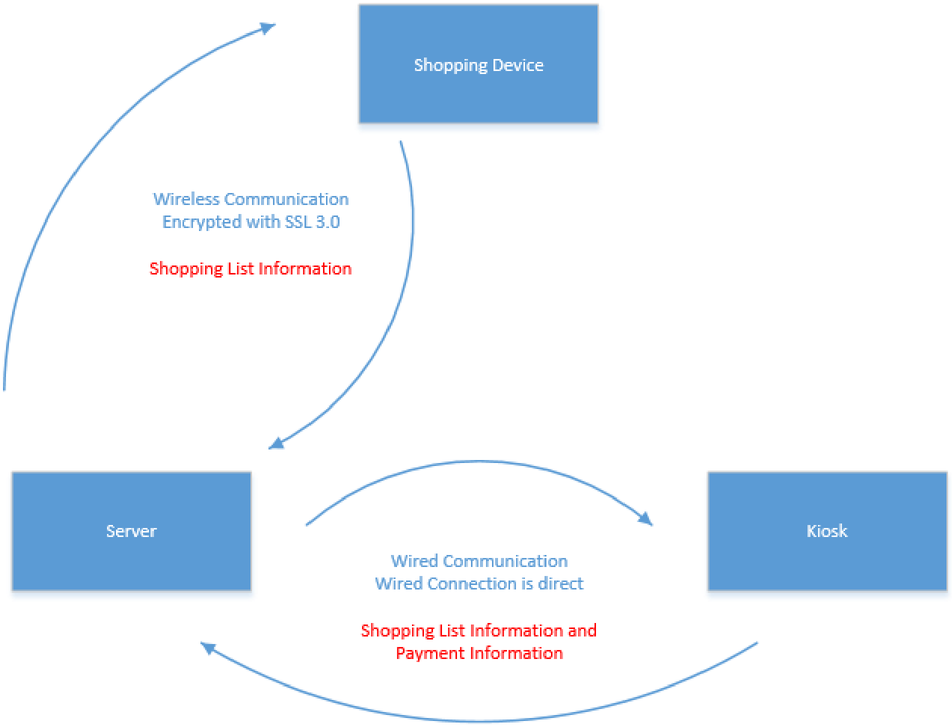

Figure 2: Security Relationship Model

Communication Line	Wired or Wireless	Encryption Method	Information Sent
Shopping Device and Server	Wireless	SSL 3.0	Shopping List changes and updates.
Server and Kiosk	Wired	SSL 3.0	Shopping List Information and Payment Information.

Table 6: Communication Relationship

4. Infrastructure Architecture

The Infrastructure Architecture describes the systems in the Personal Shopper Device relating to Access, Processing, Storage, and Networking.

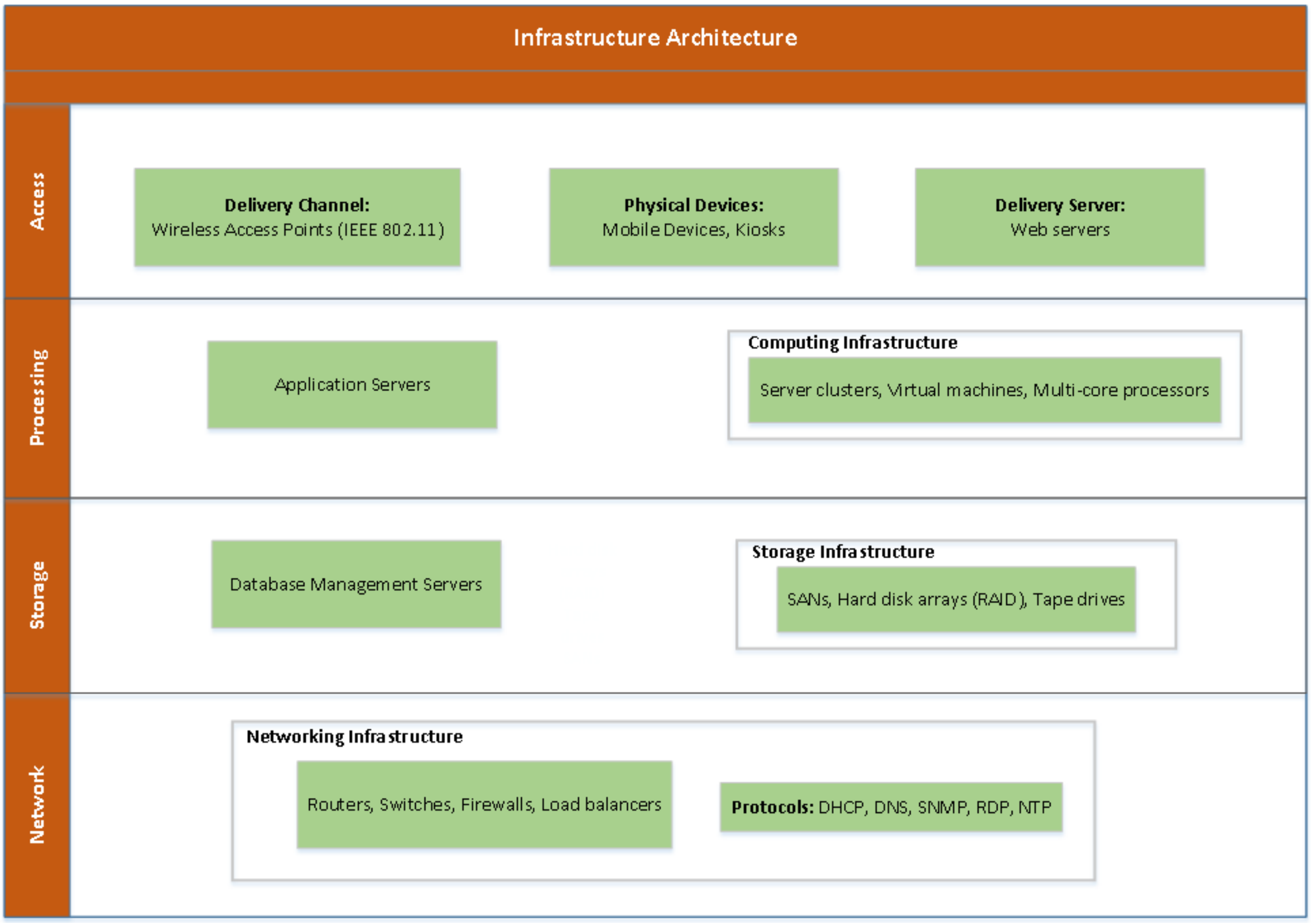
Infrastructure Architecture
Access
Delivery Channel: Wireless Access Points (IEEE 802.11)
Physical Devices: Mobile Devices, Kiosks
Delivery Server: Web servers
Processing
Application Servers
Computing Infrastructure
Server clusters, Virtual machines, Multi-core processors
Storage
Database Management Servers
Storage Infrastructure
SANs, Hard disk arrays (RAID), Tape drives
Network
Networking Infrastructure
Routers, Switches, Firewalls, Load balancers
Protocols: DHCP, DNS, SNMP, RDP, NTP

Figure 3: Infrastructure Architecture Model

4.1 *Infrastructure Architecture Overview*

The four main categories in the infrastructure architecture are presented in the following table.

Infrastructure Layer	Description
Access	This layer contains the components responsible for providing and enabling access to the Personal Shopper system.
Processing	This layer contains components responsible for providing the computing resources and platforms required for application processing.
Storage	This layer is required to provide a storage system for persistent data. Hence, it contains components that make up this storage system.
Networking	The network layer contains components that provides the communication network required to support the Personal Shopper system.

Table 7: Infrastructure Architecture Overview

4.2 Infrastructure Architecture

The components of the architecture are presented in the following table.

Infrastructure Layer	Component	Sub-Component	Description
Access	Delivery Channels	Wireless Access Point	The access layer is where end users connect to the network through IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN).
	Physical Devices	Mobile	The application's user interface for all personal or in-store mobile devices, which receives input for all shopping actions and some payment options.
		Kiosk	The application logic which controls the presentation of business objects, such as the shopping cart, and checkout, to the kiosk user.
	Delivery Servers	Web Servers	The primary function of a web server is to store, process and deliver web pages to clients. The communication between client and server takes place using the Hypertext Transfer Protocol (HTTP).
Processing	Application Server		An application server is a software framework that provides both facilities to create web applications and a server environment to run them.
	Computing Infrastructure	Server Clusters	A server cluster is a group of independent servers running and working together as a single system to provide high availability of services (to protect data, keep applications and services running) for users.
		Virtual Machines	A virtual machine (VM) is an operating system OS or application environment that is installed on software which imitates dedicated hardware.
		Multi-core Processors	A multi-core processor is an integrated circuit (IC) to which two or more processors have been attached for enhanced performance, reduced power consumption, and more efficient simultaneous processing of multiple tasks i.e. parallel processing.
Storage	Database Management Servers		Database Server Management is about managing, controlling and administering the database server. This includes areas such as instance, session storage and security management.
	Storage Infrastructure	Hard disk arrays (RAID)	Redundant array of independent disks (RAID) is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both.
		Tape Drives	A tape drive is a data storage device that reads and writes data on a magnetic tape. Magnetic tape data storage is typically used for offline, archival data storage.
		Storage area network (SAN)	A storage area network (SAN) is a network which provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear to the operating system as locally attached devices.

Network	Networking Infrastructure	Switches	Switches are devices that provide point-to-point inter-connections between ports and can be thought of as a central component of a network.
		Routers	Routers are devices that can route one or more protocols, such as TCP/IP, and bridge all other traffic on the network. It also determines the path of network traffic flow.
		Load balancers	Load balancers divide work between two or more servers in a network. Load balancers are used to ensure that traffic and CPU usage on each server is as well-balanced as possible.
		Firewalls	Firewalls are devices that you use to separate a safe internal network from the internet.
	Protocols	Dynamic Host Configuration Protocol (DHCP)	DHCP is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the network.
		Domain Name System (DNS)	The Domain Name System (DNS) is a standard technology for managing public names of Web sites and other Internet domains. DNS technology allows you to type names into your Web browser like Costco.com and your computer to automatically find that address on the Internet.
		Simple Network Management Protocol (SNMP)	Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.
		Remote Desktop Protocol (RDP)	Remote Desktop Protocol (RDP) provides remote display and input capabilities over network connections for applications running on a server. RDP is designed to support different types of network topologies and multiple LAN protocols.
		Network Time Protocol (NTP)	Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers.

Table 8: Infrastructure Architecture In-Depth

5. Technology Stack

The technology stack is where all choices involved in either hardware or software is justified. The table below gives a full justification for the technology used in the Personal Shopper system.

Architecture component	Technology Choice	Justification
Wireless Access Points	IEEE 802.11ac	This provides high throughput WLAN of at least 1 gigabit per second. These access points will allow for an extensive coverage of high speed wireless signal around the store.
Web Servers	Apache HTTP server	This is a popular and robust web server. It comes free under the Apache Software Foundation. It is integrates easily with application servers such as JBoss application server.
Application Servers	JBoss (now known as Wildfly)	It is a free and open-source application server developed by Redhat. It is platform independent and has high availability services including clustering and load-balancing services. Also, it can be easily deployed on cloud or non-cloud platform.
Database Management Server	Microsoft SQL server 2014	This is a stable, fast, secure, and affordable database engine with huge amount of community support and resources available on the web. Also, it will be a compatible database platform to use with the proposed cloud technology (Azure) that comes from the same vendor.
Computing / Storage / Networking Infrastructure	Microsoft Azure (IaaS)	This provides the compute, storage, and network infrastructure as a cloud service. The advantage of this technology is that allows for a cost effective and scalable enterprise solution without the complexities and overhead costs of physical hardware infrastructure.
Mobile / Kiosk Application	Qt framework	An application framework used widely for developing application software that can run on various different software and hardware platforms, including iOS and Android, whilst still being a native application. It is used mainly for developing application software with graphical interfaces (GUIs).
Barcode Decoding	Zxing (“zebra crossing”)	This is an open-source, multi-format, 1D/2D barcode processing library which supports decoding and generating of barcodes (like QR Code, PDF 417, EAN, UPC, Aztec, Data Matrix, Codabar) within images. It is implemented in Java and offers ports to other languages. A Qt wrapper exists for this library, called QZXing.
Tokenization System	Stripe	This handles the bulk of PCI compliance by offering tokenization of sensitive credit card information. It is an open-source software development kit which has bindings for iOS and Android, as well as several popular programming languages.

Table 9: Technology Stack

6. References

Owen, Sean. “Official ZXing ("Zebra Crossing") project home.” GitHub, Inc. <https://github.com/zxing/zxing>.

“Repositories.” Stripe. GitHub, Inc. <https://github.com/stripe>.

“Desktop, Mobile,& Embedded C++ Libraries & Tools.” The Framework & Tools. The Qt Company. <http://www.qt.io/qt-framework/>.

“Services that matter and power you can depend on.” Microsoft Azure. Microsoft. <https://azure.microsoft.com/en-us/services/>.

“Presentation logic.” Search Wikipedia. Wikipedia. <https://en.m.wikipedia.org/wiki/Presentation_logic>.

“Business logic.” Search Wikipedia. Wikipedia. <https://en.m.wikipedia.org/wiki/Business_logic>.

“Data access layer.” Search Wikipedia. Wikipedia. <https://en.m.wikipedia.org/wiki/Data_access_layer>.

“Enterprise application integration.” Search Wikipedia. Wikipedia. <https://en.m.wikipedia.org/wiki/Enterprise_application_integration>.

Jumelet, Daniel. “Infrastructure Architecture.” Developer Network. March 2007. Microsoft.< https://msdn.microsoft.com/en-us/library/bb402960.aspx>.

“Access Layer Security Design.” Cisco service ready architecture.Cisco.<http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Education/SchoolsSRA_DG/SchoolsSRA-DG/SchoolsSRA_chap9.html>.

“RAID.” Search Wikipedia. Wikipedia. <https://en.wikipedia.org/wiki/RAID>.

“Tape drive.” Search Wikipedia. Wikipedia. < https://en.wikipedia.org/wiki/Tape_drive>.

“Storage are network.” Search Wikipedia. Wikipedia. < https://en.wikipedia.org/wiki/Storage_area_network>.

“Dynamic Host Configuration Protocol”. Search Wikipedia. Wikipedia. < https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>.

“Domain name system.” Search Wikipedia. Wikipedia. <https://en.wikipedia.org/wiki/Domain_Name_System>.

“Simple network management network.” Search Wikipedia. Wikipedia. <https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol>.

“Remote desktop protocol.” Search Wikipedia. Wikipedia. <https://en.wikipedia.org/wiki/Remote_Desktop_Protocol>.

“Network time protocol.” Search Wikipedia. Wikipedia. <https://en.wikipedia.org/wiki/Network_Time_Protocol>.

NIST Cloud Computing Security Working Group 12. "NIST Cloud Computing 5 Security Reference Architecture 6." <http://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf.>