

CHAPTER 2 – LITERATURE REVIEW

General information on details that are adopted in this research including the hardware, software, electrical design, and previous studies will be covered in this chapter.

2.1 Theoretical Perspectives and Previous Research

2.1.1 Effect of Long Queueing Time to Warehouse Process and Efficiency

The long queueing time occurs in PT. XYZ Warehouses have a big impact to both of the warehouses' process and efficiency. Nowadays, customers want to get their package to be delivered as soon as possible. These requirements resulting in the rise of instant delivery services ranging from one hour up until three hours guaranteed delivery time around the globe (Dablanc et al. 2017). Those kinds of services add more challenge to warehousing and logistics company.

The presence of the instant delivery services beneficial from the increase of order number for e-commerce industry (Ahmed et al. 2024). Customer tends to choose to use instant delivery services instead of buy products physically in store. On the other hand, the pressure also increases especially for the warehousing company serving the e-commerce orders where they need to carefully choose warehouses locations to ensure coverage in terms of distances and stock planning to ensure coverage in terms of product availability. Having warehouses at every strategic location with adequate inventory planning is the key of the warehousing business nowadays (Novotná et al. 2022).

In reality, the economical factor limits the number of warehouses could be made increasing the warehouses coverage. The relatively large warehouses coverage area put burden more on the warehousing company. Most of the time window will be required by courier to deliver package. The time left for warehouse to fulfilling and hand overing the package could be reduced to only a few minutes. In PT. XYZ, the fastest one-hour delivery services only allow 10 minutes window for the warehouses where the time is divided into:

-
- Picking → 4 minutes
 - Packing → 1 minute
 - Handover → 5 minutes

In normal daily operations, the five minutes time span for handover process might be quite sufficient. However, due to the delivery hours policy where the instant package delivery could only be done between eight AM to eight PM, there are tons of instant delivery packages in the morning. All of the customer's order going through PT. XYZ system after eight PM will be hold for next early morning delivery. Furthermore, on the promo day where most of Indonesian e-commerce start the campaign exactly at the beginning of the day, a lot of customers putting orders before the warehouses opening hours. Due to those factors, for sure the beginning of online courier delivery handover process becoming the busiest time in PT. XYZ warehouses handover division.

In addition to the order number trends, storage management in the warehouse also taking into accounts to the long handover processes. The carryover order from the last night piles up in the morning. In addition to the piling problem, the queue of online delivery couriers claiming their package also unpredictable. The queue of the online delivery couriers arriving at the warehouse is uncontrollable. The warehouse worker needs to serve the user with the first come first serve principle to prevent riot between couriers. Every courier wants to get their package as soon as possible so that they could deliver more package in a day. Due to this issue, managing the overdue and new package pending for handover process become a big challenge.

Due to the unpredictable online delivery couriers timing, man power factor in warehouse operations also get the impact together with the waiting time for handover. It is becoming harder for PT. XYZ warehouse management team to balance the performance and cost factor for the manpower allocation to do the handover process. Meanwhile other process loads in the warehouse remain relatively constant during the day, the handover process loads peaks only in the morning. In the afternoon the loads sometimes could be close to zero even in the large warehouses. Only the close to the evening the loads start to rise for a while. Allocating more manpower for the handover process could drastically reduce the number of queue and waiting time. However, since

the manpower in PT. XYZ could only be paid at least daily due to the local regulations, there will be a lot of idle time that leads to cost inefficiencies.

Due to those reasons, smart locker solution is chosen to solve the issues. By using smart locker system, the overdue package could be stored individually inside each locker doors. The number of manpower to do the handover process could also be reduced leaving some to help socialize the system and handling special cases such as failure or large items that might not be covered up by the lockers. Implementing the smart locker system could also solves the unpredictable online delivery courier's arrival issues by digitalize the queue. Instead of physically queue, couriers could wait outside the area waiting for their package ready to be picked up hence the first come first serve method could be changed into first ready first serve making it easier for the warehouse team to arrange or storing the package.

2.1.2 Smart Locker System

The smart locker system is one form of IoT implementation in storage applications. Smart lockers enable the users and service providers do not need to worry about things related to the physical locker keys management which are unique for security reasons without neglecting the security points. Instead of using physical keys that are unique to each door, the smart locker system utilized digital forms of keys that are unique and hence could be replaceable(Prasetyo and Andrianto 2021). Since the unique key is digital, the door's acceptable keys also could digitally be updated by the system. Since the digital key could also be stored or verified via user smartphones, the user experience could be remarkably improved due to keeping additional objects to access the locker irrelevant anymore.

The implementation of a smart locker system also benefices the service providers in the form of easier maintenance and less dedicated person to standby at the locker locations. Due to those particular benefits, smart locker system with simultaneous user access is chosen as a solution for PT. XYZ queueing time problem. With a smaller number of manpower, it could serve multiple users at a time making the queue line shorter. Furthermore, the queue also could be virtualized to ensure that no line hanging issues

where the queue shows up due to the presence of user's package at the front of queue is not ready yet.

Digital key is one of the major differences across all smart locker system applications. Depending on the type of key being used and the verification method, a smart locker system could be implemented for various applications. This sub-chapter will discuss the type of commonly used digital key in smart locker applications.

2.1.2.1 Online Platform

Online platforms such as Blynk could facilitate the communications of microcontrollers and smartphones via the Blynk mobile apps (Shanto et al. 2023). The data exchange occurs in Blynk's cloud server requiring both the microcontrollers and smartphone connected to Blynk's cloud server. Through the integrations done between the microcontrollers and smartphones, the user could control the actuator inside the smart locker and get notifications from the smart locker's sensor (Khokher et al. 2023; Prasetyo and Andrianto 2021). The key itself could be made accordingly in Blynk's mobile apps using the available widget for user input.

This method is commonly used for rapid prototyping or proof of concept only due to the lack of flexibility, security level, and high dependencies on the Blynk apps.

2.1.2.2 Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) technology is not a new thing. It is already being used in various applications. In essence, it is a chip embedded into an object such as a card, tag, or even sticker that could transmit the unique identifier data of the object in the form of a radio wave (Gotmare et al. 2019). The RFID technology could be implemented for a smart locker system. Each locker door will have its own RFID reader. The user then could use an RFID tag or card to open the door by scanning the RFID media to the scanner at each door. The RFID media identifier and door combination could be set via the admin dashboard for flexibility (Hananto et al. 2019; Hermawan et al. 2023).

This method is commonly used for various applications that need to serve multiple users at a time and only use the locker for a short period. The RFID media will only be carried by the user for a short period. It requires the user and the service provider to exchange a physical form key in the form of the RFID media.

2.1.2.3 One-Time Password (OTP)

A one-time password (OTP) is one form of a digital key that is uniquely generated by the service provider for users that has a short lifetime for security reasons. The user could claim their OTP from the service providers from various sources such as email, SMS, phone call, mobile apps, web apps, etc. To access their package, the user then needs to input the OTP to the physical locker interface within the OTP lifetime (Hermawan et al. 2023). The OTP-based smart locker system is already being used by PopBox, one of the largest smart locker service providers across South East Asia (PopBox 2023b). It is commonly put in the form of sets of lockers with a large touchscreen-based user interface in the public area near living spaces, transportation stations, shopping areas, etc. (PopBox 2023a).

This method is commonly used due to its simplicity and appropriate security level. The users are also quite familiar with the OTP method since it is also commonly used to authenticate a user logging into their accounts. This method is suitable for long usage applications where the users tend to use the locker for longer periods minimizing the need for more than one user accessing the lockers at the same time due to the limited number of user interfaces available.

2.1.2.4 Bluetooth

Bluetooth is one of the most popular data exchange methods available. It is commonly used by devices to exchange data over short distances with master-slave architecture (Dursch, Yen, and Shih 2004). The smart locker system applications using Bluetooth method are already being used by Amazon, a multinational technology company based in the United States of America focusing on e-commerce around the world (Amazon 2023). The Bluetooth communication protocol is used for the user's smartphone mobile apps to communicate automatically to the service provider lockers to open the door.

This method is commonly used due to its higher security level since mobile apps and lockers communicate internally. However, this method is suitable for low-intensity usage with a small occurrence of a lot of people accessing the locker at the same time. The Bluetooth radio wave itself tends to have disturbance when being used near other similar 2.4Ghz-based communications methods which are commonly found in public places (Pandit and Pandit 2021).

2.1.2.5 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a form of authentication that require the users to give more than one form of authentication. The authentication method is commonly in the form of something the user has, knows, and is. The usage of MFA has increased recently due to the higher security offered by the method (Williamson and Curran 2021). The implementation of MFA in the smart locker system increases locker security and eases up the maintenance of the locker. Due to the presence of additional keys after the primary keys, the maintenance process during missing key accidents is much easier. The user still could be authenticated using the other keys (Hermawan et al. 2023).

This method offers a high-security level due to the different forms of authentication required. This method is suitable for personalized locker ownership in public spaces where the user has a dedicated locker for a long period.

2.1.2.6 Biometrics

Biometrics is the biological data of individuals. Individuals' biometric data are unique and hard to be duplicated. Biometrics data could be in behavioural and physical form. Using biometrics data instead of physical objects as a key is safer due to its uniqueness and attached physically to the user. Due to those reasons, the use of biometrics data as an authentication method is increasingly deployed (Al Rousan and Intrigila 2020). The usage of biometrics data in smart locker applications enables a higher level of security. However, the application will depend on the availability of biometrics sensors that are integrated able with microcontrollers such as fingerprint readers (Chavan et al. 2018).

This method offers a high-security level due to the unique key from biometrics data. Nonetheless, it highly depends on the user biometrics database and is only suitable for known user applications with a limited number of known users such as office space applications.

2.1.2.7 Barcode

Barcode is a scannable arrangement of bars and spaces on a surface representing data. The data is represented by the bars and spaces arrangement representing readable content consisting of characters, numbers, and symbols such as coma, dot, semi-colon, etc. Barcode is mainly used to easily identify objects in the real world by using a laser or camera-based scanner. By using the scannable identifier and database system, the user could easily get details information about the object from a single scan operation (Saad, Mohd, and Hashim 2013).

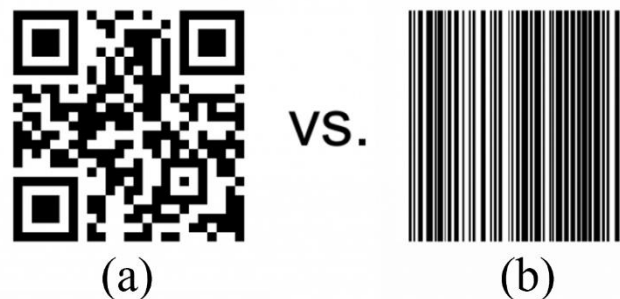


Figure 2.1 (a) 1 Dimension Barcode and (b) 2 Dimension Barcode

The Figure 2.1 above shows two kinds of mostly used barcodes in daily applications. The 1D (one-dimensional) barcode on the right side is the oldest version of the barcode. The width of the bars and spaces indicates differentiation in the content of the data. The 1D barcode is traditionally scanned by using a laser-based scanner to read the difference in the reflection caused by the bars and spaces (Saad et al. 2013). The 2D (two-dimensional) barcode at the left side is commonly known as Quick Response Code (QR code). QR code was initially developed by Denso Wave, part of the Toyota group. QR code or 2D barcode consists of grids of black and white blocks with three big squares as the anchor point. The combinations of the block's arrangement differentiate the data contained inside the QR code (Lotfipanah 2020). Due to the usage of two-dimensional arrangement (width and height) resulting in higher combination possibilities. Hence,

QR codes could contain more data of the same size compared to traditional 1D barcodes. In the presence of the three data points, QR code scanning is more verbose compared to the barcode. Modern computer vision algorithms could easily do corrections on the QR code scan concerning the three datum points (Wan et al. 2018).

The implementation of barcode technology in smart locker systems mainly utilizes QR codes instead of traditional 1D barcodes. QR code is chosen due to its verbosity to ease the user to claim their package. The larger content capacity also could increase the security by adding more characters to make brute force penetration harder and longer to be done. In general, the QR code-based smart lockers have two variations, the QR code scanning at the side of the locker and the QR code scanning at the user side.

2.1.2.7.1 QR Code Scanning at Lockers Side

The QR code scanning at the lockers' side utilizes a barcode scanner embedded at the locker side consisting of several locker slots to scan the QR code from the user side. The users get uniquely generated QR codes via the service provider apps. At the same time, the service provider system also tells the computer inside the locker the newly generated QR code locker slot access. When the QR code is pointed by the user to the scanner, the locker system will recognize which locker slot should be opened to be claimed by the user. This method is being used by Paxel, an Indonesian delivery service provider that also starts to provide smart locker solutions (Paxel 2023b). The Paxel smart locker system could be found in public spaces such as shopping areas, residential areas, and public transportation stations (Paxel 2023a).

This method does not require the user to keep additional physical assets from the service provider. The security level offered by the method is also high due to the capability to completely lock the locker slot whenever there is no request to open the specific locker slot. However, this method is only suitable for applications where users are not intensely accessing the locker at the same time due to the limited number of scanners available. Furthermore, this method might not offer the best user experience since the user need to point the QR code to the scanner without any clear visual guide compared

to the commonly method of user scan static QR code that they could clearly see the position of the target.

2.1.2.7.2 QR Code Scanning on the User Side

The QR code scanning on the user side is a variation of the previously stated method. Instead of scanning the QR code from the user, the locker shows the QR code to be scanned by the user. The user then could scan the given QR code from the locker to be inputted to the service provider apps. The service provider apps could match the user scanning the QR code and the content itself to open which segment of the locker. This system has been developed and tested in campus areas for students' usage (Sanghiampak et al. 2019).

Similarly, to the previously mentioned method, this method also equally offers both an excellent user experience and a high-security level. This method is slightly better compared to the previously mentioned method. Users tend to be more comfortable and used to scanning QR codes instead of pointing QR codes to scanners. The downside of this method is the need for an additional display component to show the QR code which could only serve users once at a time. The display itself could also be embedded in every door to enables the simultaneous user access capabilities.

2.1.3 Internet of Things (IoT)

The Internet of Things (IoT) is one example of the evolutionary stage of the Internet. IoT bridge human and machine interactions. Furthermore, IoT also removes the physical barrier between machine-to-machine and human-to-machine interactions. It could be implemented in every aspect of human lives due to its implementation flexibility. Shortly, IoT is one of the necessary sources of information required by artificial intelligence (AI) and machine learning (ML) development that heavily requires data (Ramasamy and Kadry 2021).

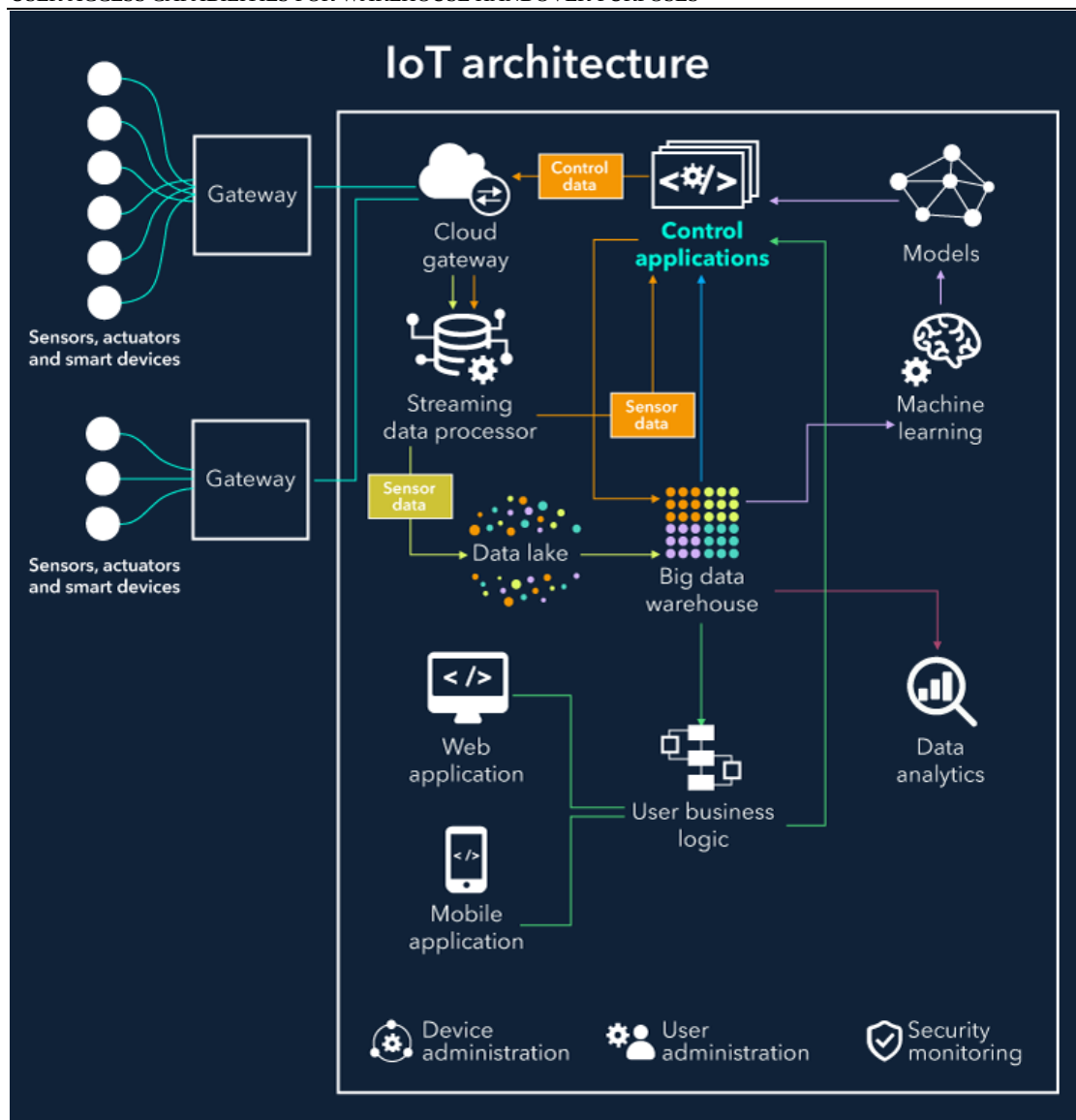


Figure 2.2 Internet of Things (IoT) Architecture

The Figure 2.2 above shows the overview of the IoT Architecture diagram. IoT devices consist of sensors and actuators embedded in physical objects that could transfer data over both wired and wireless networks (Fahd Al-Mutawa and Albourae Eassa 2020). It relies on the microcontrollers to facilitate communications over networks via gateways to low-level sensors and actuators (Prasetyo and Andrianto 2021). In the implementations, all IoT devices could communicate and share data through the cloud. After getting into the cloud, the data could be utilized for various purposes. Cloud connectivity also enables IoT devices to interact with human users in the form of notifications, alerting, and even feedback from humans to machines to do some

actions(Villamil, Hernández, and Tarazona 2020). The data collected in the cloud could satisfy the needs of data for various advanced machine learning, deep learning, and artificial intelligence applications (Bzai et al. 2022).

2.1.4 Message Queuing Telemetry Transport Protocol

Message Queueing Telemetry Transport (MQTT) protocol is one of the well-known communication protocols with the publisher-subscriber communication model. It runs over the TCP/IP protocol for a reliable communication. The MQTT protocol enables the publisher to do another task without bothering whether if the subscribers already received the message. The publisher could proceed to another task after publishing the message and let the broker does it job to ensure the subscribers got the message. (Im and Lim 2023). Due to those nature of MQTT protocol, it is commonly used in the industry especially Internet of Things where most of the devices being used are resource constrained with efficient and reliable communications feature (Tian and Vassilakis 2023).

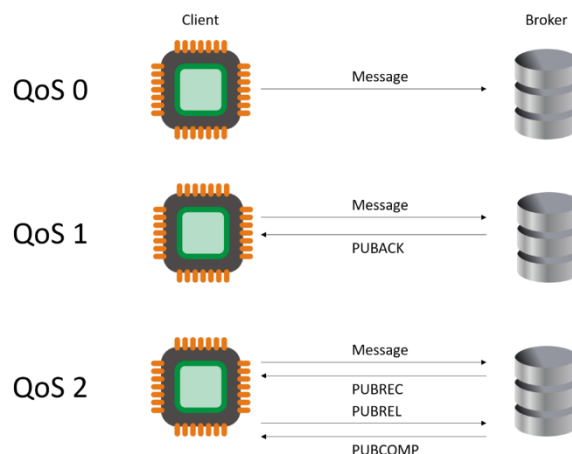


Figure 2.3 MQTT Protocol Quality of Services Level

In terms of reliability, MQTT protocol supports three level of reliability level or commonly known as Quality of Services (QoS) as shown in the Figure 2.3. The QoS 0 does not care whether if the message is received or not. It has the lowest reliability. Both of the QoS level 1 and 2 ensure the message is received providing higher reliability. The only difference between is QoS level 2 ensure that the message is received exactly once utilizing the four-way handshake that might be critical for some applications. The higher QoS level comes with a cost of longer delays. (Lee et al. 2013)

The MQTT protocol also has retain flag that make it even more suitable for applications with low processing power devices and potentially bad signal conditions. When a message is published with the retain flag set to be true, the broker then will hold or remember the message while forwarding it to all active subscribers. When a subscriber just connected to the broker, it will always receive the last retained message of the topic it is subscribing to (Nazir and Kaleem Muhammad 2019). This feature is really useful since in the actual implementation with resource constrained microcontrollers could face unintended power cycle either because of the watchdog triggered, or even when power failure occurs. By adding the retain flag to all important topic, the devices could directly operational every time after it restarts.

2.2 Summary

Table 2.1 Literature Review Summary

References	Technology Used	Summary	Common Applications
(Prasetyo and Andrianto 2021)	Blynk (Online IoT Platform)	Implementation of IoT where all devices could communicate one another. The Blynk apps in mobile phone communicates with the locker as a digital key form. This method is commonly used for testing or prototyping only due the lack of security level.	Internal company deposit box
(Hananto et al. 2019) (Hermawan et al. 2023)	RFID Card / Tag	Implementation of RFID card that could be used to open locker doors, each door has individual RFID scanner. The acceptable RFID card code could be adjusted accordingly in case of missing cards. This method commonly used for temporary storage time in public spaces.	Sports centers
(Hermawan et al., 2023)	One Time Password	Implementation of IoT for smart locker where the user will receive unique one-time	Public deposit box services

(PopBox 2023b)		password (OTP) via the apps when the user wants to open the door. The lockers of 20-30 doors have dedicated keyboard and screen to input the OTP. This system is being used by PopBox and many smart locker providers.	
(Amazon 2023)	Bluetooth	Implementation of localize IoT where the smart locker could connect with users' mobile phone apps via Bluetooth. The mobile phone apps than will communicate with the locker to open the door. This system is being used by Amazon at the pick-up points.	Public deposit box services
(Hermawan et al. 2023)	Multi Factor Authentication	Implementation of more than 1 step of verification to increase the security level. Besides RFID scan, the user needs to input PIN that are generated by the system as a confirmation method. This method is useful to tackle missing RFID card problems.	Public and internal deposit box services
(Chavan et al. 2018)	Biometrics	Implementation of fingerprint scanner to open the smart locker system. The system could store multiple user biometrics data and assign specific access of the door to specific user. This system mainly used for internal purposes only due to the needs to maintain all users' biometrics data.	Internal deposit box services or asset access
(Paxel 2023b)	QR Code (At users' side)	Implementation of QR Code usage to replace OTP / PIN and remove the needs of monitors and keyboard in the lockers. The mobile apps will generate a QR code that could be pointed to the QR scanner at the locker to open the door. Each locker set of 20-30 doors shares common QR	Public deposit box services

(Luís et al. 2022)	QR Code (At lockers side)	scanner. This method is being used by Poxel. Implementation of QR Code shown in the lockers doors that could be scanned by the user using the provided mobile apps to access the door. This method is being researched for university usage and use e-papers to show the QR Code.	Have not been used publicly, for research purposes only
-----------------------	------------------------------	---	---
