SurveiRams

Project Documentation Submitted
to the Faculty of the
School of Computing and Information Technologies
of
Asia Pacific College

In Partial Fulfillment of the Requirements for Software Development

By

James Aaron Heramil
Lionel Kerwin Ejorango
Kyle Dumbrique
Mariah Rocita Mirarza
Shiaramae Faburada

ASIA PACIFIC COLLEGE
Approval Sheet

SurveiRams

Prepared and submitted by:

James Aaron Heramil
Lionel Kerwin Ejorango
Kyle Dumbrique
Mariah Rocita Mirarza
Shiaramae Faburada

In Partial Fulfilment of the Requirements for the Degree of

Bachelor of Science in Computer Science

Examined and Recommended for Acceptance and Approval for Research/Capstone Presentation

_____
Jo Anne dela Cuesta
Adviser

Panel of Judges

_____
Chairperson

Panel Members

_____ _____
Panel Member Panel Member

Acceptance and approved in partial fulfillment of the requirements for the degree of Bachelor of Science

_____
Executive Director

School of Computing and Information Technologies

SurveiRams 1
List of Figures 7
List of Tables 8
Abstract 10
I. Introduction 11
1.1 Project Context 11
1.2 Purpose and Description 11
1.3 Objectives 12
1.4 Scope and Limitations 13
II. Related Literature 15
2.1 Paperless and Cloud 15
2.2 Incidents 16
2.3 Tickets 16
2.4 Synthesis 17
III. Technical Background 18
3.1 Current System 18
3.2 Proposed System 21
3.2.2 Hardware 23
3.2.3 Peopleware 23
3.2.4 Network 24
3.3 Current and Proposed System Comparison 24
3.4 User Roles 25
IV. Design and Methodology 27
4.1 Requirements Analysis 27
4.2 Requirements Documentation 33
4.2.1 Use Case Diagrams 34
4.2.2 Use Case Description 35
4.3 Needs Assessment 40
4.4 Design of Software, Systems, Product, and/or Processes 41
4.4.1 Deployment Diagram 41
4.4.2 Entity Relationship Diagram 42
4.5 Development and Testing 42
4.5.1 Development Requirements 43
4.5.2 Development Workflow and Version Control 43
4.5.3 Testing Requirements 46
4.6 Implementation Plan 46
4.6.1 System Implementation Setup 46
4.6.2 Post-System Release Plan 47

4.7 Implementation Results 47
4.8 System Architecture 47
4.8.1 Pre-System Release Plan 48
4.8.2 Client Layer 49
4.8.3 SurveiRams Application 49
4.8.4 Google Firebase 49
4.9 Performance 50
4.10 Team Composition 51
4.11 Document Security 51
4.11.1 Frontend Security Implementation 51
4.11.2 Backend and Database Security Implementation 51
4.12 Business Continuity Plan 52
V. Results and Discussion 55
5.1 Login 55
5.2 Home 55
5.3 User Management 58
5.4 Incident Reports 60
5.5 Patrol and Logs 62
5.6 Insights 62
VI. Conclusions and Recommendations 64
VII. Appendices 65
7.1 Other Relevant Diagrams 65
7.1 1 Event Table 65
7.1.2 Activity Diagram 66
7.1.3 Class Diagram 68
7.1.4 Sequence Diagram 68
7.1.5 State Transition Diagram 68
7.1.6 Package Diagram 68
7.1.7 Component Diagram 68
7.1.8 Functional Decomposition Diagram 69
7.1.9 Data Flow Diagram 69
7.2 Relevant Links 70
7.2.1 Graphical User Interface Design 70
7.2.2 Source Code 70
7.2.3 Installation Guide 70
7.2.4 User Manual 70
7.2.5 Software Requirements Specification 70
7.2.6 Test Documents 70
7.3 Team's Curriculum Vitae 71

7.3.1 James Aaron Heramil 71
7.3.2 Kyle Dumbrique 73
7.3.3 Lionel Kerwin Ejorango 76
7.3.4 Mariah Rocita Mirarza 78
7.3.5 Shiaramae Faburada 79
References 82

Table of Contents

List of Figures

Figure III-1 Sample Written Report 18
Figure III-2 Sample Guard Monitoring Sheet 19
Figure III-3 Current Head Guard Process 20
Figure III-4 Current Guard Process 20
Figure III-5 Current BMO/ITRO Process 21
Figure III-6 Proposed Head Guard Process 22
Figure III-7 Proposed Guard Process 22
Figure III-8 Proposed BMO/ITRO Process 23
Figure IV-1 Use Case Diagram 34
Figure IV-2 Needs assessment 41
Figure IV-3 Deployment Diagram 42
Figure IV-4 Entity Relationship Diagram 42
Figure IV-5 Development Workflow and Version Control 44
Figure IV-6 System Architecture 48
Figure V-1 Default Login Screen 55
Figure V-2 Login Error Prompt 55
Figure V-3 Login Error Prompt 55
Figure V-4 Head Guard Home Screen 56
Figure V-5 Guard Home Screen 56
Figure V-6 BMO Home Screen 57
Figure V-7 Admin Home Screen 58
Figure V-8 ITRO Home Screen 57
Figure V-9 Members List 59
Figure V-10 User Management Read 59
Figure V-11 User Management Update 59
Figure V-12 User Management Create 59
Figure V-13 Unresolved Incident Reports 61
Figure V-14 Resolved Incident Reports 61
Figure V-15 View Incident Report 61
Figure V-16 View Incident Report 61
Figure V-17 Sort Incident Reports 61
Figure V-18 Resolved Incident Report 61
Figure V-19 Report 62
Figure V-20 Create Incident Report 62
Figure V-21 Submit Incident Report 62
Figure V-22 View Log 62
Figure V-23 Verified Patrol Log 62
Figure V-24 New Patrol Log 62
Figure V-25 View Insights 63
Figure VII-1 Manage Incident Report and Insights Activity 66
Figure VII-2 Manage Logs Activity 67
Figure VII-3 Manage User Activity 67
Figure VII-4 State Transition Diagram 68
Figure VII-5 Functional Decomposition Diagram 69
Figure VII-6 Data Flow Diagram Level 0 69
Figure VII-7 Data Flow Diagram Level 1 70

List of Tables

Table 1 Minimum System Requirement 23
Table 2 Minimum System Requirement (Router Wi-Fi Network Speed) 24
Table 3 System User Roles 25
Table 4 Product Backlog Items 27
Table 5 Product Backlog Items for Requested Features 31
Table 6 Use Case Description for Authentication 35
Table 7 Use Case Description for Create Incident Report 35
Table 8 Use Case Description for Read Incident Report 36
Table 9 Use Case Description for Update Incident Report 37
Table 10 Use Case Description for Create Logs 37
Table 11 Use Case Description for Read Logs 38
Table 12 Use Case Description for Update Logs 38
Table 13 Use Case Description for Read Insights 39
Table 14 Use Case Description for Manage User 39
Table 15 GitHub Active Branches 44
Table 16 Support Device Type 45
Table 17 Software Interfaces 45
Table 18 Performance Testing Result 50
Table 19 Team Composition 51
Table 20 Business Continuity Plan 52
Table 21 Failure Types 53
Table 22 Event Table 65

Abstract

SurveiRams is a mobile application designed to assist Asia Pacific College's security personnel and other departments, including the Building Maintenance Office (BMO) and Information Technology Resource Office (ITRO), in managing incident reports, logs and providing insights. Currently, their processes are conducted manually, and the security personnel record all reports and other activities in a logbook. The team provides a solution by developing a mobile application, SurveiRams, that will automate the manual documentation process to alleviate the problems caused by the manual management of security personnel, BMO, and ITRO departments. By digitizing the manual operations of security personnel and concerned departments using the SurveiRams application at Asia Pacific College, they can efficiently address any concerns or incident reports that have occurred within the school, and departments such as BMO and ITRO can effectively track, manage, and respond to incidents.

I. Introduction

Asia Pacific College (APC) is one of the prominent colleges in the Business and Information and Communications Technology (ICT) industries in Makati, Philippines [1]. Its facilities include networking and computer laboratories, sound and photography studios, and a built-in culinary kitchen [2].

Given the school's facilities, the school has implemented various security measures, including hiring security staff. Security personnel are assigned to roam and inspect each floor daily, which cannot be left unattended. Due to the tedious processes and excessively manual methods used by security personnel, productivity and efficiency are compromised. To address this issue, the team agreed to enhance and refine the manual verification system into a mobile application that serves as a patrolling assistant focusing on its reporting system aspect to develop a more digitalized, efficient, and sustainable method of keeping up with the security personnel's daily operations.

1.1 Project Context

Not long ago, routine tasks had to be completed by hand. However, as technology progresses, the need to automate manual processes is becoming necessary [3]. Unlike automated systems, which are programmed to auto-assign tasks and automatically log every action, manual processes depend on humans to do these tasks step-by-step.

APC saw the need to enhance its present system for monitoring guards' activity while checking each floor by implementing a digitalized system. Given that the existing method is still manual, it will be tedious and time-consuming to perform their daily operations. Apart from that, incident reports and logs are given manually, which means they must be written down, resulting in a repeated and time-consuming process due to the additional effort required to locate the needed information. Most of the work is accomplished by one employee, the head guard, and a liaison between other offices and divisions. The status of the office affects the head guard's productivity and the institution, mainly because it requires more time, effort, and resources to be as productive as other offices within the institution.

In this case, the entire process becomes tedious and involves unnecessary paperwork. Automating the current system can optimize reviewing system reports by reducing paper documents [4]. Aside from this, it can also improve employees' productivity by creating a more effective and efficient environment [5].

1.2 Purpose and Description

The success of an organization is contingent upon its employees' productivity, and one of the most effective ways to increase employee productivity is to invest in process improvement. The employees concerned can boost productivity, reduce errors and redundancies, and save time by implementing digital strategies that address these pain points, resulting in more efficient work by allowing employees to focus more on higher-

value tasks. Additionally, this enables the stakeholders to maintain and keep incident reports, streamline cross-functional processes, and increase the organization's dependability, all of which contribute to the organization's overall efficiency. Strategic process management is critical for organizations to leverage these characteristics to gain a competitive edge and increase overall productivity.

1.3 Objectives

The SurveiRams is designed to help the security personnel, Building Maintenance Office (BMO), and Information Technology Resource Office (ITRO) of Asia Pacific College manage incident reports and logs, which also helps building security. These issues are mostly caused by manual operations that are inefficient, resource-extensive, and unsustainable in the future. The SurveiRams attempts to identify the problems with current processes using well-known and popular technology for building industry-level systems. With that said, it has the following general and specific objectives:

General Objective:

To develop SurveiRams that will serve as a ticketing system for APC's security personnel, ITRO, and BMO in recording incident reports and logs, provide insights into guards' routes, and develop a tactical transition and digital approach to the stakeholders' present difficulties. This increases the accuracy and efficiency of the method implemented for determining whether the security personnel have completed their assigned tasks.

Specific Objectives:

- To create a mobile application that will:
  - develop a centralized location where the guards can log their patrols
  - automate the manual process of documentation
  - provide analytical insights to interpret data reports and patterns for assisted and effective decision-making

Success Criteria:

The project objectives are met if the following features are achieved:

- A repository shows that the user can access to create, read, and update incident reports and logs.
- An analytics dashboard is shown where an administrator can see the available insight for the accumulated reports. The said dashboard could present the following information:
  - Number of resolved and unresolved incident reports.
  - Which department and floor has the most incidents that occurred
  - Type of incident that occurred the most
  - Number of incidents that occurred on each level
  - Number of incidents addressed to each office

1.4 Scope and Limitations

This study aims to enhance the current system for recording and monitoring the activities of APC's security personnel. It is specifically designed for the use of the institution's security personnel and the building maintenance office.

Scope

This project's primary goal is to log the roving guards' incident reports and activities, which will aid in digitizing the process for the security personnel, ITRO, and BMO. It will also generate insights that provide statistical information regarding incidents/building damages.

This project will also assist the BMO and ITRO in reviewing anomalies or incident reports concerning their respective offices. Further, it will be feasible by using cloud services – by putting all information in an online repository that will always be accessible through their phones.

Limitations

The project will only be limited to the use of security personnel, ITRO, and BMO. Moreover, this is not intended to be used for purposes other than processes regarding patrolling, post logs, and incident reports.

II. Related Literature

2.1 Paperless and Cloud

Even a slight reduction in paper usage can result in cost savings and increased productivity. There are always benefits to reducing paper usage, regardless of whether an organization is in its infancy or has already been established. Going paperless can offer numerous advantages to a business: (1) Document organization and the ability to quickly locate and disseminate information may improve the efficiency and image of a business. Searching through stacks of paper slows response time in an age where most answers are accessible with a few keystrokes. By scanning electronic copies of receipts and invoices, documents can be quickly sorted, filed, and organized for retrieval. Businesses can easily back up reports with photo-scanning apps instead of bringing back a stack of paper documents. Electronic files can also be shared with peers via email or a network.

The transition to paperless documentation increases the efficiency of data transportation by eliminating the need for complicated fax machines and document couriers. When you inadvertently discard a vital document, it is typically irretrievable without automatic backups. Nonetheless, maintaining electronic files permits multiple backup locations. Data storage options include flash drives, the cloud, and external hard drives. Cloud-based accounting systems provide automatic, prescheduled backups of vital financial data, eliminating the need for small business owners to set aside time for manual backups [6].

Considering all these factors, the organization will find the applicability and benefits of going paperless to be highly suitable. This improves the organization's efficiency and speed of operations and cost savings. The benefits of eliminating paper far outweigh the cost of paper, which can be substantial. Toner cartridges and other office supplies have become less expensive. In a paperless or digital workplace, additional upgrades, or replacements of expensive office equipment, such as printers and photocopiers, may also be eliminated. Each year, the trend toward a paperless environment accelerates as data storage and electronic communication are enhanced by modern technology. By reducing its paper consumption, APC may increase its business efficiency and the level of protection for its most sensitive information.

Cloud services are in demand by most companies and customers; these services provide accessible and affordable access to applications and resources. Most employees use cloud services since they can check emails and collaborate on documents [7]. Cloud services promote flexibility in working in cloud environments, where users can quickly access cloud services with nothing more than a computer, operating system, and internet connectivity [8]. This technology uses the internet to store and manage data on remote servers and can access shared data across a network via the internet, such as Dropbox, Facebook, and Gmail. These examples used the cloud to store files by automatically synchronizing the files from the desktop. In the mentioned example, “Dropbox allows users to access files and store up to 1 terabyte of free storage. A Social Networking

platform requires powerful hosting to manage and store data in real time. Cloud-based communication provides click-to-call capabilities from social networking sites and access to the Instant messaging system" [9]. Similarly, the SurveiRams mobile application will store data or document files using cloud services.

2.2 Incidents

Multiple events occur in one location, such as a school. Specific incidents or situations endanger a student's safety, health, or well-being, and the school must pay attention to them, regardless of when or where they occurred, because they affect the student and school staff. In addition, several threats, such as security, property damage, and emergencies, might disrupt school operations [10]. The process entailed with the ticketing system will capture, document, and manage incidents, such as property damage or anomaly detection in the facilities, by completing an incident report upon the occurrence of an incident and adding additional pertinent information. These reports guarantee that occurrences will be reviewed to reduce and prevent recurrences of the same incidents or events. The reporting procedure could aid in implementing a new risk management and training procedure to assist employees in determining the causes of events [11]. In this regard, SurveiRams assures that the head guard and other security professionals can submit an incident report to the relevant office via a mobile application so that the incident report can be immediately investigated.

Reporting occurrences is crucial; whether the incident is minor or severe, it must be investigated to determine what occurred and the potential problems it produced to prevent a recurrence [12]. With the use of statistical methods in an incident report, data collection will utilize the appropriate analyses and yield successful findings [13]. Security personnel at Asia Pacific College (APC) and the respective management, including Building Maintenance Office (BMO) and Information Technology Resource Office (ITRO), will be able to view the statistics on the dashboard page of the SurveiRams mobile application. Filtering the information will determine which incidents are most frequently reported. Using statistics, the administration can make decisions and implement modifications to prevent a recurrence of the incident [14].

2.3 Tickets

Ticketing systems aid and support in addressing any concerns or incidents inside a company. These systems utilize ticketing software to facilitate incident management. Ticketing software enables IT to support being organized, focused, efficient, and successful via a ticketing system. Once the tickets flow through the ticketing software, the management software and IT support team will handle them and distribute them to the appropriate individuals who will fix the event so that the IT support team can efficiently track, manage, and deal with incidents. Ticketing software will also prioritize the most critical occurrences and assign them a higher priority. After resolving a ticket, the IT personnel will manage the resolved tickets by closing them and moving on to the next problem [15]. Similarly, the SurveiRams mobile application allows security personnel to

report incidents they have observed while on duty or patrolling, and the corresponding management will quickly resolve the issue

2.4 Synthesis

As stated previously, SurveiRam's mobile application facilitates the digitization of work processes by reducing the use of paper among employees. Using this mobile application, security personnel may quickly report incidents they encounter. Managements such as BMO and ITRO will also benefit from the program because they will be notified promptly if an incident requires resolution by their department.

III. Technical Background

3.1 Current System

Now, the institution's method of recording the activities of security personnel is still manual. The reports are manually written in a logbook. Please refer to Figure III-1 for a sample report written in the logbook by the security personnel. Also, the officer-in-charge and the guard-on-duty will have to sign the guard monitoring sheet, as seen in Figure III-2**Error! Reference source not found.**, to verify that the guards did their assigned tasks. Later, the logbooks are passed on to the security head.

Log no.	Time	activity
1962	1730	Assume post duties and responsibilities from the – And going co-guard – Include all item covered in this post.
1963	1730	Standby at lobby information
1964	1803	Psi? reading upper 35 lower 35
1915	1805	Turn on the APC, IBM and SM Signage
1916	1820	Turn on the lights at peremeter area
1917		Conduct roving inspection of _____ peremeter Area found normal status.
1918	1900	Monitoring of Humabon parking area
1919	2000	A.O.R normal status
1920	2101	Text message Mr. Jojo Castillo and Mr. Manolet?
1921	2203	Arrival of Ms. Marry Ann Romero to get the one Cooler and admission office
1922	2304	Conduct roving inspection from 12th flr to B-3 And Humabon parking area
1923	2319	Locked room 504
1924	2325	Found defective the doorknob at room 303
1925	2341	A.O.R(H)? found normal status
1926	0000	Standby at lobby information
1927	0052	Assist _____ at lobby information Conduct roving inspections
1928	0135	_____ back and lobby information
1929	0200	Standby at ___ lounge for monitoring at Humabon parking area.
1930	0300	Assist _____ and south perimeter around To conduct roving inspection
1931	0320	Conduct roving inspection of south perimeter Found normal status
1932	0438	Turn off the lights of fire exit phase I

Figure III-1 Sample Written Report

RADIO MONITORING AND CONDUCT ROVING INSPECTION OF AREA OF RESPONSIBILITY FROM 12TH FLOOR TO BASEMENT 3

Date:

Time	Post	Signature	Post	Signature	Post	Signature
2300HRS	OIC/SIC		LOBBY		SOUTH	
0000HRS	LOBBY		OIC/SIC		SOUTH	
0100HRS	SOUTH		LOBBY		OIC/SIC	
0200HRS	OIC/SIC		LOBBY		SOUTH	
0300HRS	LOBBY		OIC/SIC		SOUTH	
0400HRS	SOUTH		LOBBY		OIC/SIC	
0500HRS	OIC/SIC		LOBBY		SOUTH	

Preoared by:

OIC. Rodolfo M. Cuntapay
Officer-in-Charge

GUARD ON DUTY

SIGNATURE OVER PRINTEDNMAE

SIGNATURE OVER PRINTEDNAME

SIGNATURE OVER PRINTEDNAME

Figure III-2 Sample Guard Monitoring Sheet

The current routine of the head guard is depicted in Figure III-3. After beginning their foot patrol, they record or hand-write their activities in a logbook. Once they encounter anomalies enroute, they contact the concerned office immediately. They will then compose an incident report on a separate sheet of paper. The document is then submitted to the ITRO or BMO. Otherwise, they continue their patrol. The head guard collects the logbooks of other security personnel at the end of each day. If they have free time, they will review the submitted logs. If not, they keep the logbook.

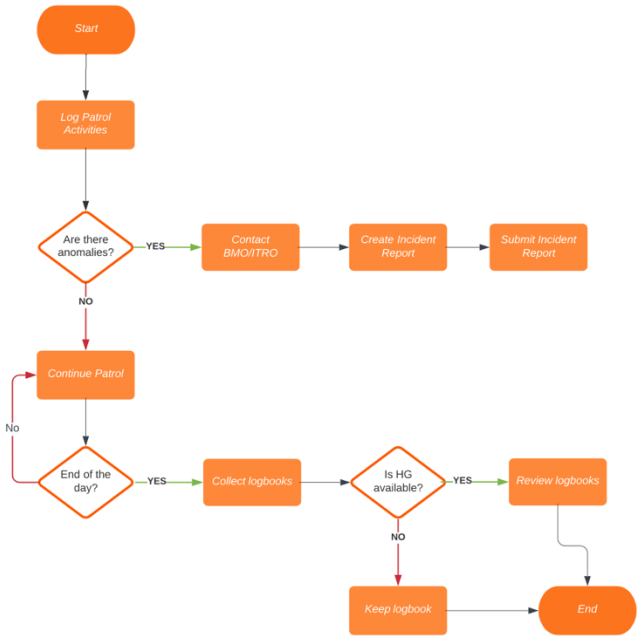

Figure III-3 Current Head Guard Process

As for the remainder of the security personnel, they record their specific activities manually while on their post. Once they encounter an anomaly, they create an incident report and submit it to the head guard. This logbook is given to the head guard at the end of each day. Refer to Figure III-3 for more details.

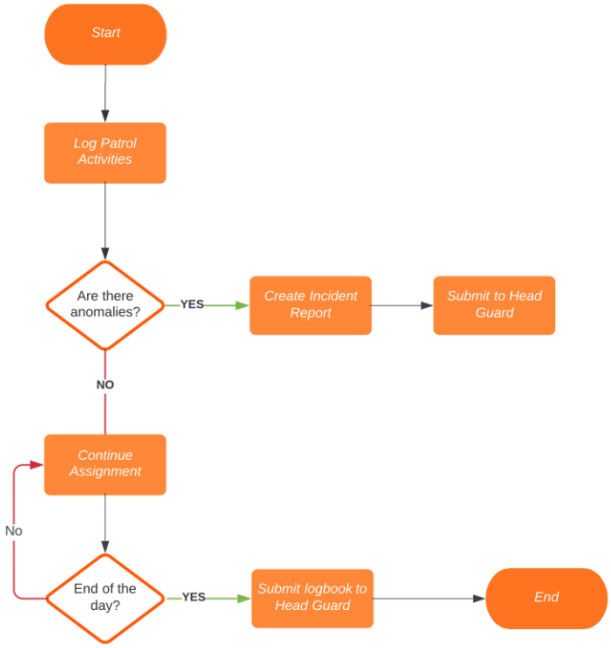

Figure III-4 Current Guard Process

Currently, the BMO and ITRO await the submission of incident reports. They will notify the head guard that the issue has been resolved once the report has been resolved. For more details on the BMO process, refer to Figure III-5.

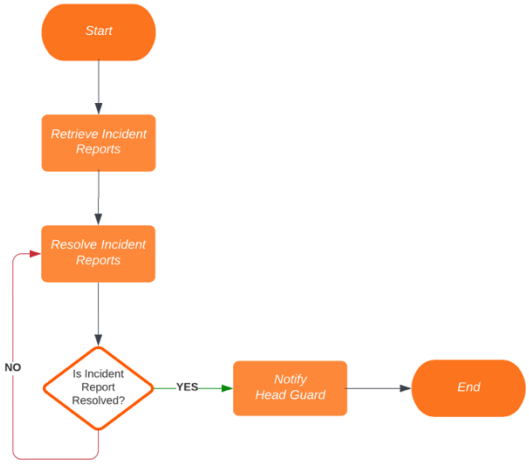

Figure III-5 Current BMO/ITRO Process

3.2 Proposed System

This section will discuss the proposed solution regarding software, hardware, peopleware, and network.

For the proposed system's process, Figure III-6, the head guard will be able to log their patrol activities while patrolling. Once they encounter an anomaly, they can immediately create an incident report and send it directly to the concerned office. Otherwise, they can continue their patrol. Concurrently, they can simultaneously or instantly check any new logs to verify them, or view incident reports submitted by other security personnel.

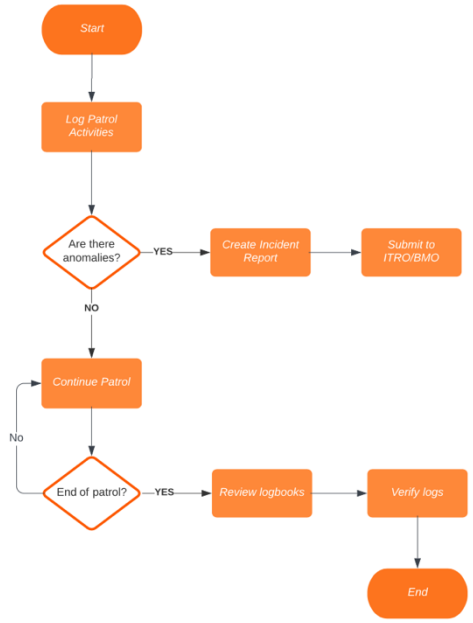

Figure III-6 Proposed Head Guard Process

Additionally, the remaining security personnel will be able to record patrol activities while on duty. Upon encountering an anomaly during their shift, they will be able to draft an incident report and submit it directly to the appropriate office. Refer to Figure III-7 for more details.

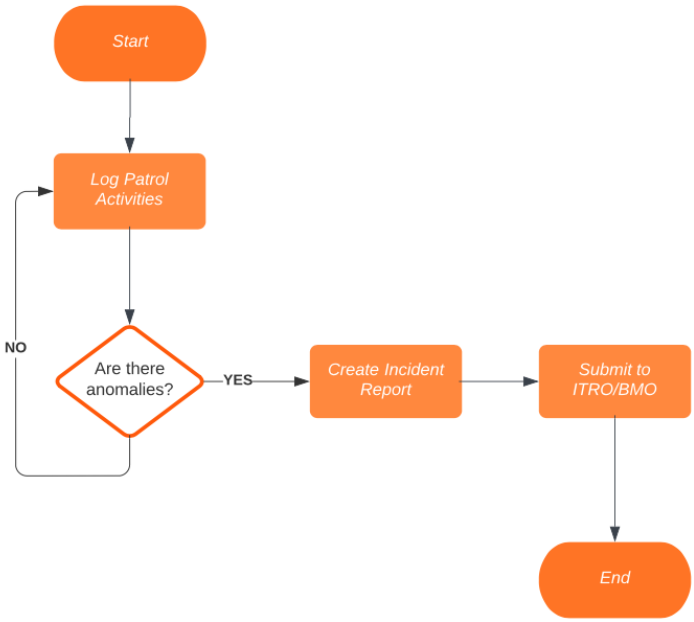

Figure III-7 Proposed Guard Process

With the proposed system, Figure III-8, the BMO and ITRO will have instant access to incident reports submitted by security personnel. Once the issue has been resolved, they can close the ticket, which will be reflected immediately on the other user's end.

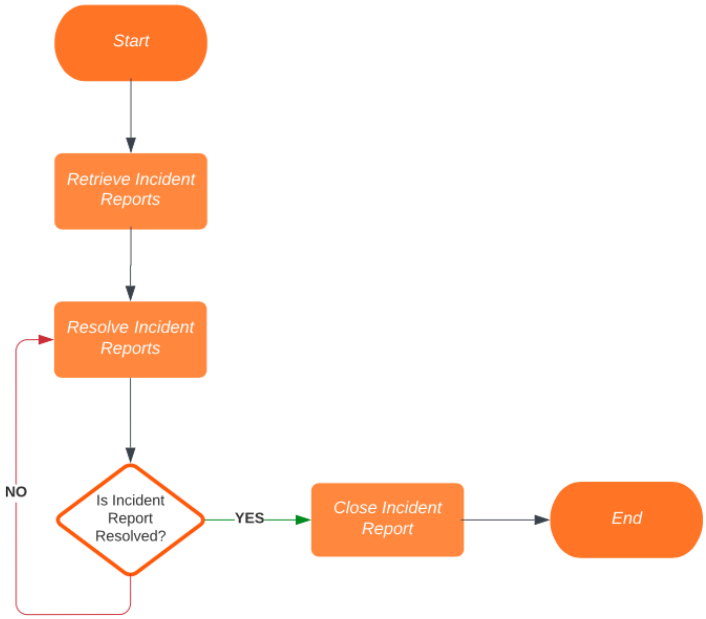

Figure III-8 Proposed BMO/ITRO Process

3.2.2 Hardware

Each security guard will be expected to have a mobile phone. Please refer to Table 1 for the minimum requirements. Each mobile phone will be utilized to access the SurveiRams system.

Table 1 Minimum System Requirement

System	Minimum Requirement
Processor	2 central processing unit (CPU) cores
Random-access memory (RAM)	1 gigabyte (GB) (Assuming no other apps are running in the background or other unnecessary apps installed)
Storage	8 GB Internal Storage

3.2.3 Peopleware

Four direct users of the SurveiRams will be required to understand how to access the program: the security personnel, head guard (HG), BMO, and ITRO. To access SurveiRams, security employees must use their assigned credentials to log in. Once logged in, the system will identify the user's role and assign them the appropriate dashboard. As an HG, they can access the patrolling functions, submit reports, and make

logs. The remainder of the security staff will not have access to the patrolling functions but will have access to the incident report and log features. The ITRO will have access to the reports and user management functionality. In contrast, the BMO will also have access to the reports.

The patrolling mode will capture pertinent information, such as date, time, position, and any user-specified anomalies. After the patrol, the user must click the "Add Report" button to submit their report to the database. In addition, the head guard, ITRO, and BMO have access to the reports that are delivered to them. Similarly, the system permits the BMO and ITRO to update the status and resolution of incident reports.

3.2.4 Network

Furthermore, an internet connection is needed to ensure that all data in the application will be synchronized in real time. With this stated, the minimum network speed requirements can be referred to in Table 2.

Table 2 Minimum System Requirement (Router Wi-Fi Network Speed)

Component	Minimum Requirement
Wireless fidelity (Wi-Fi)	150 Mbps

3.3 Current and Proposed System Comparison

The key difference between the current and proposed systems is that the manual processes have been digitized, allowing employees to focus on their core responsibilities instead of repetitive activities. In addition, less effort is necessary due to reduced human interaction. The proposed system sends reports immediately to their relevant offices, and data are synchronized. This allows the system to eliminate time-consuming and costly data silos by removing paperwork and data collection from many sources.

The current head guard process consists of eight steps, whereas the proposed process consists of only six. The same applies to the remaining guards' current procedure, which comprises five steps, whereas the proposed method only requires three. The present and proposed BMO and ITRO procedures comprise the same phases. However, the current approach requires more time and effort from the end user.

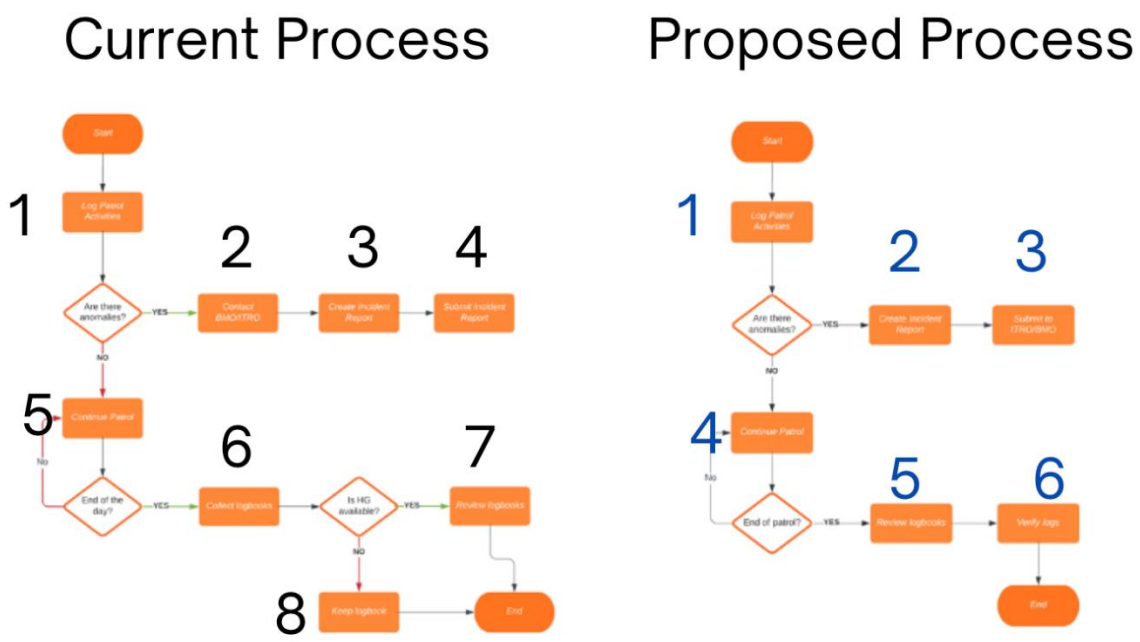

Figure III-9 Comparison of Head Guard Processes

3.4 User Roles

The SurveiRams system is projected to have four primary user types. The BMO, ITRO, and head guard should be able to retrieve and update the status of incident reports from the database. Additionally, they should have access to the dashboard, which provides report insights. Furthermore, the head guard should be able to submit incident reports and logs and retrieve status updates from the database.

Similarly, the remainder of the security personnel should be able to submit logs and incident reports. In addition, an additional user is required for an admin position with access to all features for the four user classes listed. Please refer to Table 3.

Table 3 System User Roles

Role	**RBAC**							
	Create Incident Report	View Incident Report	Update Incident Reports	Create Patrol Logs	View Patrol Logs	Update Patrol Logs	User Management	View Insights
Head Guard	✓	ALL	×	✓	✓	✓	Read only	✓
Guard	✓	Own	×	✓		×	Read only	
ITRO	×	ITRO	✓	×	×	×	CRUD	
BMO	×	BMO	✓	×	×	×	Read only	

Super Admin	✓	✓	✓	✓	✓	✓	✓	✓

IV. Design and Methodology

4.1 Requirements Analysis

The requirement analysis specification contains user stories that define what the system will accomplish, how it will be expected to perform, and a description of the functionalities required to meet the specific users' requirements, Table 4.

These requirements were attained when the team shadowed the security personnel and head guard during their patrol.

Table 4 Product Backlog Items

Epic/Roles	Product Backlog ID	Description	MoSCoW Prioritization	Effort Estimation
Head Guard	HG01	As a HEAD GUARD, I want to be able to log in, so that I can access my account.	Must-Have	2
	HG02	As a HEAD GUARD, I want to be able to create an incident report, so that I can inform the concerned office about the damage that needs to be fixed	Must-Have	8
	HG03	As a HEAD GUARD, I want to be able to upload an image about the incident, so that I can support my report with proof	Must-Have	8
	HG04	As a HEAD GUARD, I want to be able to write a description about the incident report, so that I can identify the type of incident	Must-Have	8
	HG05	As a HEAD GUARD, I want to be able to address my report to a specific department, so that I can inform the specific office about an incident	Must-Have	8
	HG06	As a HEAD GUARD, I want to be able to navigate through the incident reports page, so that I can view the incident reports I have submitted	Must-Have	3
	HG07	As a HEAD GUARD, I want to be able to view incident reports, so that I can see its specific details	Must-Have	5
	HG08	As a HEAD GUARD, I want to be able to sort the incident reports, so that I can easily look for reports based on different categories	Must-Have	5

	HG09	As a HEAD GUARD, I want to search for a specific incident report, so that I can easily locate a certain report when necessary	Must-Have	5
	HG10	As a HEAD GUARD, I want to be able to create a log so that I can write down what I did throughout the day.	Could-Have	8
	HG11	As a HEAD GUARD, I want to be able to navigate in logs page so that I can view my logs	Could-Have	5
	HG12	As a HEAD GUARD, I want to be able to view logs, so that I can see their specific details	Could-Have	5
	HG13	As a HEAD GUARD, I want to be able to sort logs so that I can view my logs based on different categories	Must-Have	5
	HG14	As a HEAD GUARD, I want to search for a specific log, so that I can easily locate a certain log when necessary	Should-Have	5
	HG15	As a HEAD GUARD, I want to verify logs so that I know that the record has been checked	Should-Have	8
	HG16	As a HEAD GUARD, I want to be able to view user profiles, so that I can see its specific details	Should-Have	5
	HG17	As a HEAD GUARD, I want to be able to search users, so that I can easily locate a user when necessary	Should-Have	5
	HG18	As a HEAD GUARD, I want to be able to navigate insight pages, so that I can view analytics for the accumulated reports	Should-Have	3
Guards	GUA01	As a GUARD, I want to be able to log in so that I can access my account.	Must-Have	2
	GUA02	As a GUARD, I want to be able to create an incident report, so that I can inform the concerned office about the damage that needs to be fixed	Must-Have	8
	GUA03	As a GUARD, I want to be able to upload an image about the incident, so that I can support my report with proof	Must-Have	8

	GUA04	As a GUARD, I want to be able to write a description about the incident report, so that I can identify the type of incident	Must-Have	8
	GUA05	As a GUARD, I want to be able to address my report to a specific department, so that I can inform the specific office about an incident	Must-Have	8
	GUA06	As a GUARD, I want to be able to navigate through the incident reports page, so that I can view the incident reports I have submitted	Must-Have	3
	GUA07	As a GUARD, I want to be able to view incident reports, so that I can see its specific details	Could-Have	5
	GUA08	As a GUARD, I want to be able to sort the incident reports, so that I can easily look for reports based on different categories	Should-Have	5
	GUA09	As a GUARD, I want to search for a specific incident report, so that I can easily locate a certain report when necessary	Should-Have	5
	GUA10	As a GUARD, I want to be able to create a log so that I can write down what I did throughout the day.	Must-Have	8
	GUA11	As a GUARD, I want to be able to navigate in logs page so that I can view my logs	Should-Have	5
	GUA12	As a GUARD, I want to be able to view logs, so that I can see its specific details	Should-Have	5
	GUA13	As a GUARD, I want to be able to sort logs so that I can view my logs based on different categories	Could-Have	5
	GUA14	As a GUARD, I want to search for a specific log, so that I can easily locate a certain log when necessary	Could-Have	5
	GUA15	As a GUARD, I want to be able to view user profiles, so that I can see their specific details	Should-Have	5
	GUA16	As a GUARD, I want to be able to navigate insight pages, so that I can view analytics for the accumulated reports	Should-Have	3
BMO	BMO01	As a BMO, I want to be able to log in so that I can access my account.	Must-Have	2

	BMO02	As a BMO, I want to be able to navigate through the incident reports page, so that I can view the incident reports I have submitted	Must-Have	3
	BMO03	As a BMO, I want to be able to view incident reports, so that I can see its specific details	Should-Have	5
	BMO04	As a BMO, I want to be able to sort the incident reports, so that I can easily look for reports based on different categories	Could-Have	5
	BMO05	As a BMO, I want to search for a specific incident report, so that I can easily locate a certain report when necessary	Could-Have	5
	BMO06	As a BMO, I want to close incident reports, so that I know that the problem has been resolved	Should-Have	8
	BMO07	As a BMO, I want to be able to include a cause and solution for resolving incidents to further explain my report	Should-Have	8
	BMO08	As a BMO, I want to be able to navigate insight pages, so that I can view analytics for the accumulated reports	Should-Have	3
	BMO09	As a BMO, I want to be able to view user profiles, so that I can see its specific details	Should-Have	5
	BMO10	As a BMO, I want to be able to search users, so that I can easily locate a user when necessary	Should-Have	5
ITRO	ITR01	As an ITRO, I want to be able to log in so that I can access my account.	Must-Have	2
	ITR02	As an ITRO, I want to be able to navigate through the incident reports page, so that I can view the incident reports I have submitted	Could-Have	3
	ITR03	As an ITRO, I want to be able to view incident reports, so that I can see its specific details	Could-Have	5
	ITR04	As an ITRO, I want to be able to sort the incident reports, so that I can easily look for reports based on different categories	Could-Have	5

	ITR05	As an ITRO, I want to search for a specific incident report, so that I can easily locate a certain report when necessary	Must-Have	5
	ITR06	As an ITRO, I want to close incident reports, so that I know that the problem has been resolved	Should-Have	8
	ITR07	As a BMO, I want to be able to include a cause and solution for resolving incidents to further explain my report	Could-Have	8
	ITR08	As an ITRO, I want to be able to navigate insight pages, so that I can view analytics for the accumulated reports	Could-Have	3
	ITR09	As an ITRO, I want to be able to create a new user, so that I can add a user when necessary	Must-Have	8
	ITR10	As an ITRO, I want to be able to view user profiles, so that I can see its specific details	Must-Have	5
	ITR11	As an ITRO, I want to be able to search users, so that I can easily locate a user when necessary	Must-Have	5
	ITR12	As an ITRO, I want to be able to update users, so that I can modify their details when necessary	Must-Have	5

Shown in Table 5 are the requested additional features by the stakeholders.

Table 5 Product Backlog Items for Requested Features

Epic/Roles	Product Backlog ID	Description	MoSCoW Prioritization	Effort Estimation
BMO	BMO11	As a BMO, I want to be able to assign a specific role for specific tasks so that I know to whom the problem is addressed to	Could-Have	5
	BMO12	As a BMO, I want to be able to create an incident report, so that I can inform the concerned office about the damage that needs to be fixed	Could-Have	8

	BMO13	As a BMO, I want to be able to upload an image about the incident, so that I can support my report with proof	Could-Have	8
	BMO14	As a BMO, I want to be able to write a description about the incident report, so that I can identify the type of incident	Could-Have	8
	BMO15	As a BMO, I want to be able to address my report to a specific department, so that I can inform the specific office about an incident	Could-Have	8
ADMIN	ADM01	As an ADMIN, I want to be able to log in, so that I can access my account.	Could-Have	2
	ADM02	As an ADMIN, I want to be able to create an incident report, so that I can inform the concerned office about the damage that needs to be fixed	Could-Have	8
	ADM03	As an ADMIN, I want to be able to upload an image about the incident, so that I can support my report with proof	Could-Have	8
	ADM04	As an ADMIN, I want to be able to write a description about the incident report, so that I can identify the type of incident	Could-Have	8
	ADM05	As an ADMIN, I want to be able to address my report to a specific department, so that I can inform the specific office about an incident	Could-Have	8
	ADM06	As an ADMIN, I want to be able to navigate through the incident reports page, so that I can view the incident reports I have submitted	Could-Have	3
	ADM07	As an ADMIN, I want to be able to view incident reports, so that I can see its specific details	Could-Have	5
	ADM08	As an ADMIN, I want to be able to sort the incident reports, so that I can easily look for reports based on different categories	Could-Have	5
	ADM09	As an ADMIN, I want to search for a specific incident report, so that I can easily locate a certain report when necessary	Could-Have	5

	ADM10	As an ADMIN, I want to close incident reports, so that I know that the problem has been resolved	Could-Have	8
	ADM11	As an ADMIN, I want to be able to include a cause and solution for resolving incidents to further explain my report	Could-Have	8
	ADM12	As an ADMIN, I want to be able to create a log so that I can write down what I did throughout the day.	Could-Have	8
	ADM13	As an ADMIN, I want to be able to navigate in logs page so that I can view my logs	Could-Have	5
	ADM14	As an ADMIN, I want to be able to view logs, so that I can see its specific details	Could-Have	5
	ADM15	As an ADMIN, I want to be able to sort logs so that I can view my logs based on different categories	Could-Have	5
	ADM16	As an ADMIN, I want to search for a specific log, so that I can easily locate a certain log when necessary	Could-Have	5
	ADM17	As an ADMIN, I want to verify logs so that I know that the record has been checked	Could-Have	8
	ADM18	As an ADMIN, I want to be able to create a new user, so that I can add a user when necessary	Could-Have	8
	ADM19	As an ADMIN, I want to be able to view user profiles, so that I can see its specific details	Could-Have	5
	ADM20	As an ADMIN, I want to be able to search users, so that I can easily locate a user when necessary	Could-Have	5
	ADM21	As an ADMIN, I want to be able to update users, so that I can modify their details when necessary	Could-Have	5
	ADM22	As an ADMIN, I want to be able to navigate insight pages, so that I can view analytics for the accumulated reports	Could-Have	3

4.2 Requirements Documentation

This subchapter consists of three parts: (1) Use Case Diagrams and (2) Use Case Full Descriptions.

4.2.1 Use Case Diagrams

A use case diagram illustrates the various ways in which a user can interact with a system. It summarizes information about the system's users/actors and their interactions. A use case description is a text-based narrative of functionality that details the actor's interaction with the system.

The use case diagram for SurveiRams is seen in Figure IV-1. It consists of four factors: security personnel, head guard, Information Technology Resource Office (ITRO) and Building Maintenance Office (BMO).

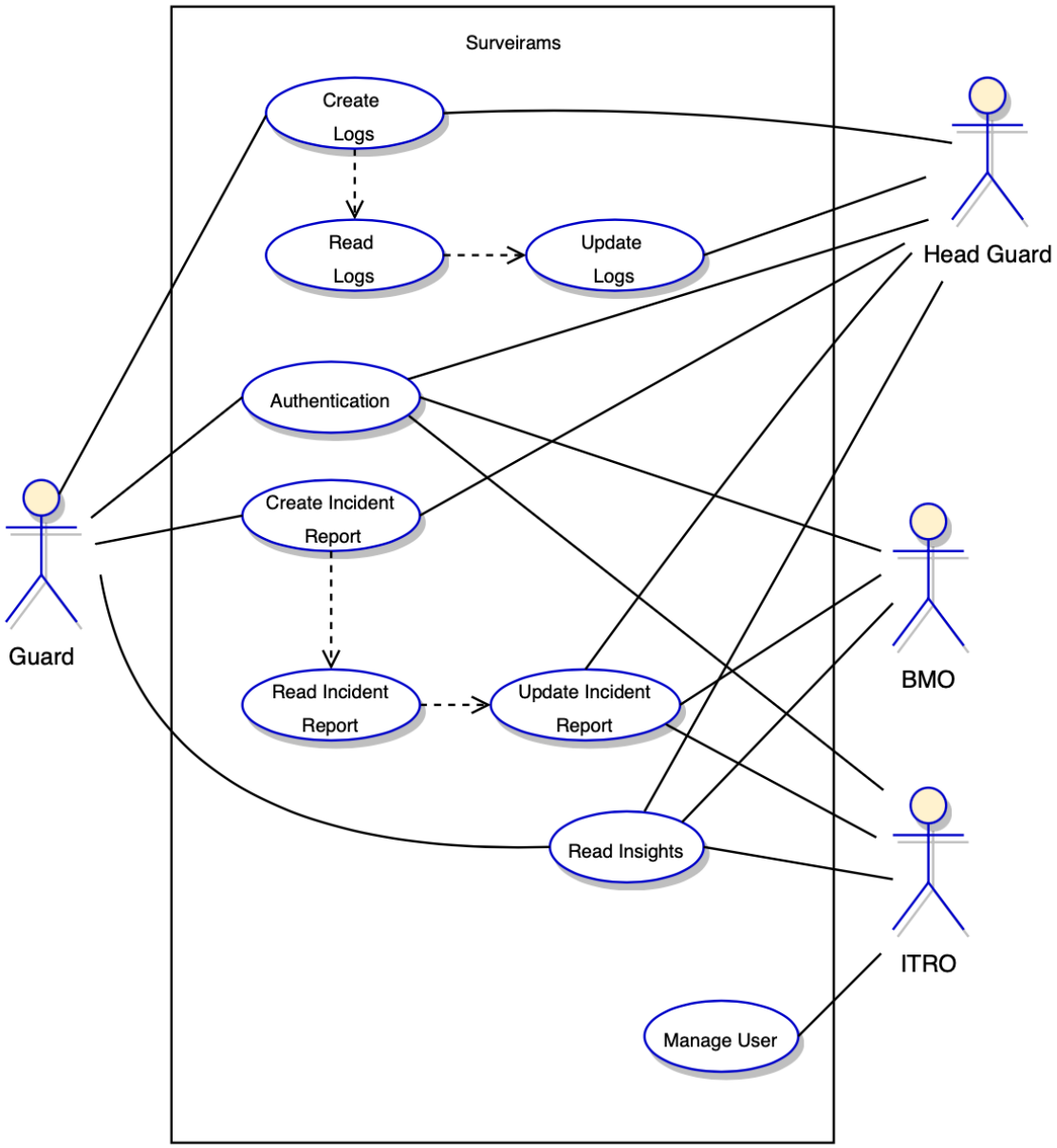

Figure IV-1 Use Case Diagram

4.2.2 Use Case Description

The following tables detail the use cases. Six use cases are included in the system.

Table 6 Use Case Description for Authentication

Use Case Number	**SurveiRams_UC1**	
User Case Name	**Authentication**	
Summary / Description	The user authenticates their account to log on to the system.	
Pre-conditions	The user's data must be registered in the system.	
Post-conditions	The system will log the user in the system.	
Actor/s	Guard, Head Guard, BMO, ITRO	
Trigger	The user enters the username and password in the system.	
Main Scenario(Basic Flow/s)	**Actor**	**System**
	[1] User inputs credentials. [2] The user will be logged in once.	[1.1] The system will check its database and authenticate the user. [2.1] The system redirects the user to their respective home page.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt.	

Table 7 Use Case Description for Create Incident Report

Use Case Number	**SurveiRams_UC2**	
User Case Name	**Create Incident Report**	
Summary / Description	The user creates their incident report for any anomalies encountered.	
Pre-conditions	User must be logged in.	
Post-conditions	New incident reports have been added to the system.	
Actor/s	Head Guard, Guard and BMO	
Trigger	The user clicks on create incident report button.	
	Actor	**System**

Main Scenario (Basic Flow/s)	[1] User logs in to the system. [2] User clicks on the create incident report button. [3] User inputs necessary incident report details.	[1.1] The system redirects the user to their respective home page. [2.1] The system redirects the user to the create incident report page. [3.1] The system adds new data to the system.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt. [3.1] If an error occurs, changes will not reflect to the system.	

Table 8 Use Case Description for Read Incident Report

Use Case Number	**SurveiRams_UC3**	
User Case Name	**Read Incident Report**	
Summary / Description	The user reads submitted incident report for any encountered anomalies.	
Pre-conditions	User must be logged in. At least one incident report should be submitted to the system.	
Post-conditions	Display home page.	
Actor/s	Head Guard, Guard, BMO and ITRO	
Trigger	The user clicks on a specific incident report.	
Main Scenario (Basic Flow/s)	**Actor**	**System**
	[1] User logs in to the system. [2] User clicks on the incident reports page button. [3] User clicks on a specific incident report.	[1.1] The system redirects the user to their respective home page. [2.1] The system redirects the user to the incident report page. [3.1] The system displays corresponding data.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt.	

Table 9 Use Case Description for Update Incident Report

Use Case Number	**SurveiRams_UC4**	
User Case Name	**Update Incident Report**	
Summary / Description	The user updates the status of incident reports whether they have been resolved or not.	
Pre-conditions	User must be logged in. At least one incident report should be submitted to the system	
Post-conditions	Updated incident reports have been added to the system.	
Actor/s	BMO and ITRO	
Trigger	The user clicks on resolve button	
Main Scenario (Basic Flow/s)	**Actor**	**System**
	[1] User logs in to the system. [2] User clicks on the incident reports page button. [3] User clicks on an unresolved incident report. [4] User clicks on resolve button.	[1.1] The system redirects the user to their respective home page. [2.1] The system redirects the user to the incident report page. [3.1] The system displays respective data. [4.1] System updates existing data.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt. [4.1] If an error occurs, changes will not reflect to the system.	

Table 10 Use Case Description for Create Logs

Use Case Number	**SurveiRams_UC5**	
User Case Name	**Create Logs**	
Summary / Description	The user generates their logs for their activities while patrolling and on their post.	
Pre-conditions	User must be logged in.	
Post-conditions	New logs have been added to the system.	
Actor/s	Head Guard and Guard	
Trigger	The user clicks on create log button	
Main Scenario (Basic Flow/s)	**Actor**	**System**
	[1] User logs in to the system. [2] User clicks on logbook button. [3] User clicks on the create log button.	[1.1] The system redirects the user to their respective home page. [2.1] The system redirects the user to the logbook page.

	[4] User inputs necessary log details.	[3.1] The system redirects the user to the create log page. [4.1] The system adds new data to the system.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt. [4.1] If an error occurs, changes will not reflect to the system.	

Table 11 Use Case Description for Read Logs

Use Case Number	**SurveiRams_UC6**	
User Case Name	**Read Logs**	
Summary / Description	The user reads submitted logs	
Pre-conditions	User must be logged in. At least one log should be submitted to the system.	
Post-conditions	Display home page.	
Actor/s	Head Guard and Guard	
Trigger	The user clicks on a specific log.	
Main Scenario (Basic Flow/s)	**Actor**	**System**
	[1] User logs in to the system. [2] User clicks on the logbooks page button. [3] User clicks on a specific log.	[1.1] The system redirects the user to their respective home page. [2.1] The system redirects the user to the logbook page. [3.1] The system displays corresponding data.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt.	

Table 12 Use Case Description for Update Logs

Use Case Number	**SurveiRams_UC7**
User Case Name	**Update logs**
Summary / Description	The user will update the status of logs whether they have been verified or not.
Pre-conditions	User must be logged in. At least one log should be submitted to the system.
Post-conditions	Updated incident reports have been added to the system.

Actor/s	Head guard	
Trigger	The user clicks on the verify button.	
Main Scenario (Basic Flow/s)	**Actor**	**System**
	[1] User logs in to the system. [2] User clicks on the logbook page button. [3] User clicks on an unverified log. [4] User clicks on verify button.	[1.1] The system redirects the user to their respective home page. [2.1] The system redirects the user to the logbook page. [3.1] The system displays respective data. [4.1] System updates existing data.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt. [4.1] If an error occurs, changes will not reflect to the system.	

Table 13 Use Case Description for Read Insights

Use Case Number	**SurveiRams_UC8**	
User Case Name	**Read Insights**	
Summary / Description	User views the insights for incident reports.	
Pre-conditions	User must be logged in. At least one log should be submitted to the system.	
Post-conditions	The system will display the insights.	
Actor/s	Head guard, Guard, BMO, and ITRO	
Trigger	User clicks on insights button.	
Main Scenario (Basic Flow/s)	**Actor**	**System**
	[1] User logs in to the system. [2] User clicks on the insights page button.	1.1] The system redirects the user to their respective home page. [2.1] The system redirects the user to the insights page.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt.	

Table 14 Use Case Description for Manage User

Use Case Number	**SurveiRams_UC9**
User Case Name	**Manage user**

Summary / Description	User manages user information allowing them to create, read and update a user profile.	
Pre-conditions	User must be logged in.	
Post-conditions	Changes are reflected in the system	
Actor/s	Guard, Head Guard, BMO, and ITRO	
Trigger	User clicks on members' button.	
Main Scenario (Basic Flow/s)	**Actor**	**System**
	[1] Admin logs in to the system. [2] Admin clicks on the User Management page button. [3] Admin performs create, read, and/or update operation to a user account.	[1.1] The system redirects the user to the Dashboard Home page. [2.1] The system redirects the user to the User Management page. [3.1] System adds and updates existing data.
Exception Conditions	[1.1] If the user fails to provide valid credentials, the system will display a login error prompt. [3.1] If an error occurs, changes will not reflect to the system.	

4.3 Needs Assessment

A gap analysis technique enables businesses to discover the most effective way to accomplish their business objectives.

Given the clients' problem, which is that they have limited ways of verifying if the guards are roving on their assigned routes, the researchers created a problem pyramid to quickly identify the causes of why the problem is being experienced. For reference, see Figure IV-2.

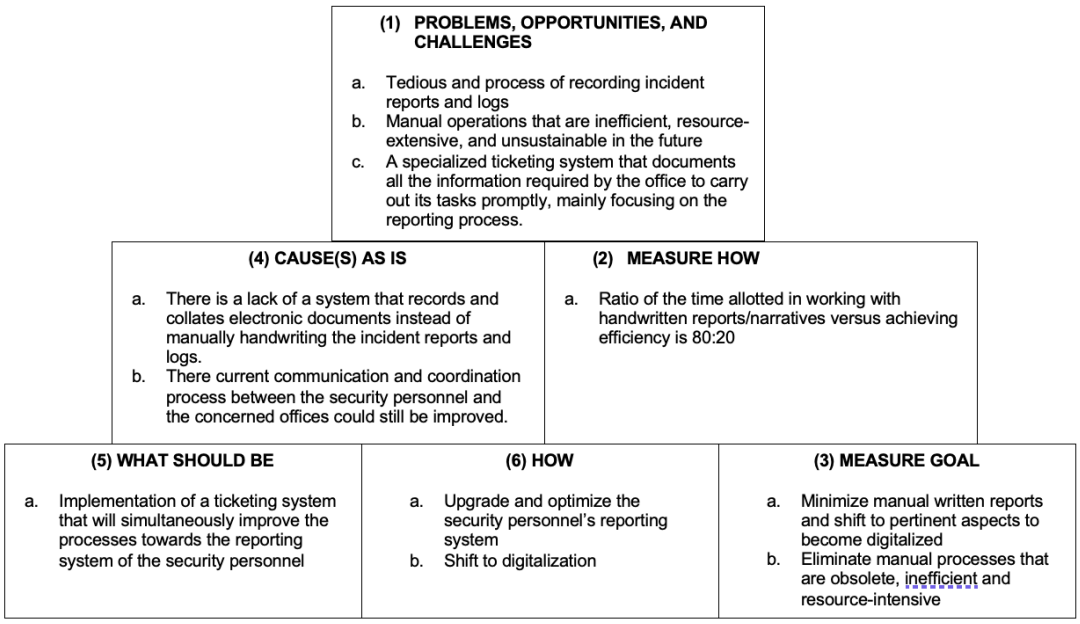

Figure IV-2 Needs assessment

4.4 Design of Software, Systems, Product, and/or Processes

4.4.1 Deployment Diagram

SurveiRams deployment diagram is shown in Figure IV-3. The system is comprised of three nodes, the first of which identifies the clients, which contains the Information Technology Resource Office (ITRO), Building Maintenance Office (BMO), Head Guard (HG), and Security Personnel. The second includes the application itself with the components (1) User Management, (2) Incident Reports, (3) Insights, and (4) Patrol and Logs. The last node would be Firebase which holds the database for the application. This contains the User Credentials, Incident Reports and Logs Records, and Proof of Incidents images.

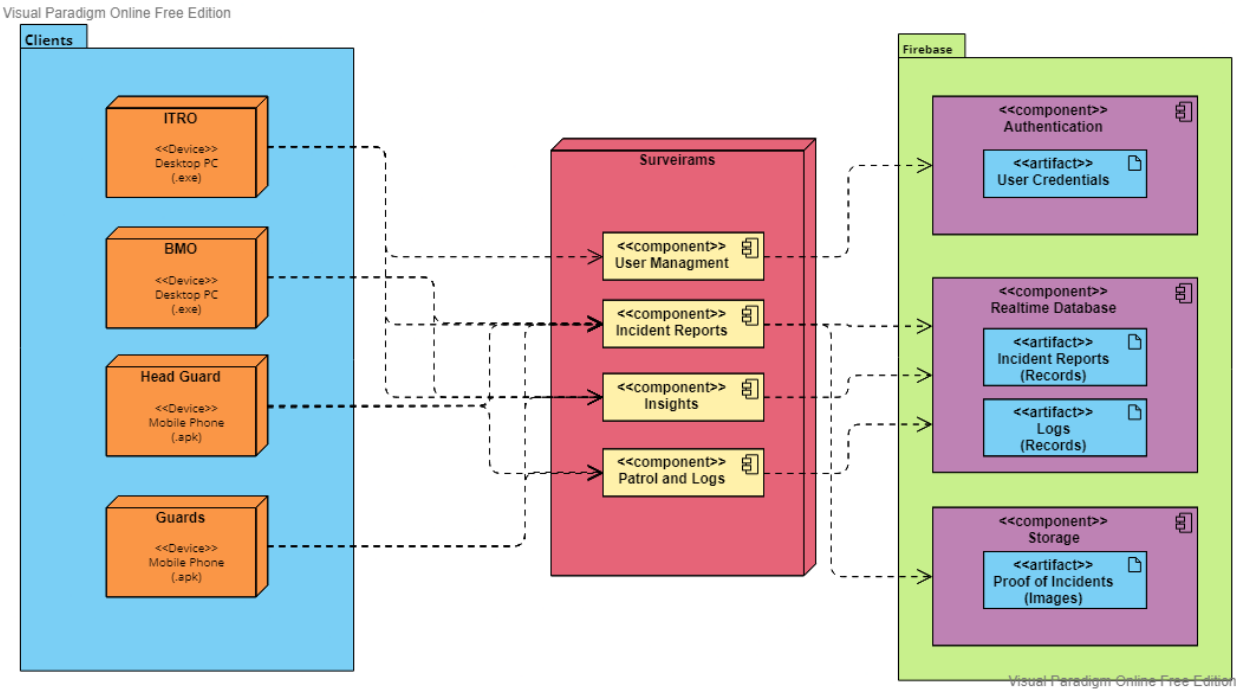

Figure IV-3 Deployment Diagram

4.4.2 Entity Relationship Diagram

The entity relationship diagram of the proposed system is shown in Figure IV-4.

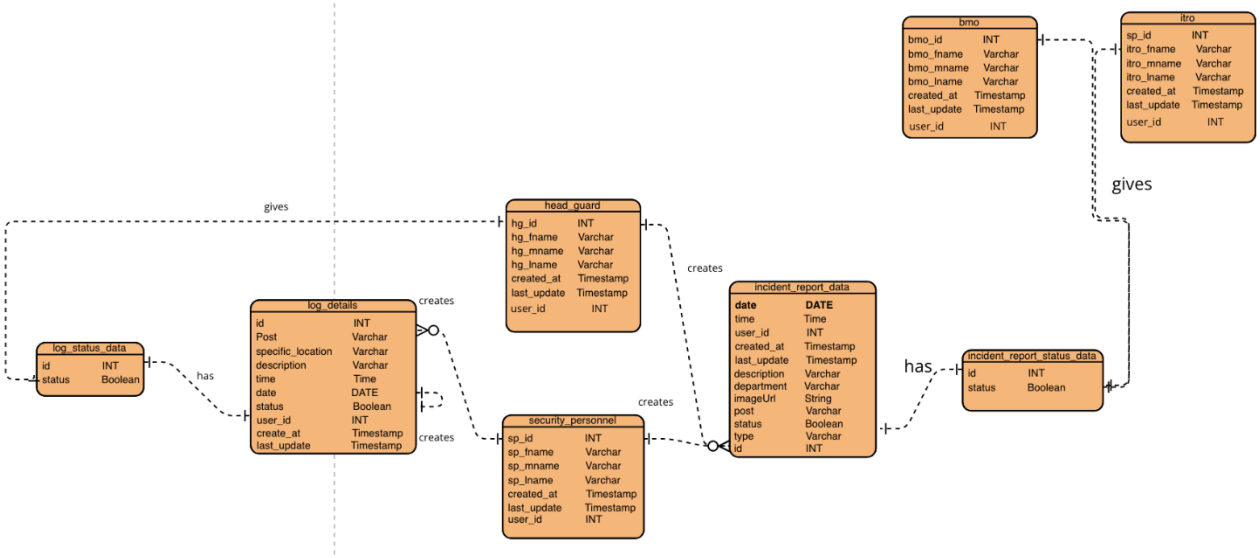

Figure IV-4 Entity Relationship Diagram

4.5 Development and Testing

SurveiRams is being developed in an Agile Development Lifecycle. This method reduces the overall development and operations by completing product backlogs in short

increments, known as sprints. Sprints typically last one to four weeks, whereas this project is set to two weeks a sprint. Moreover, for every sprint, the team would then do retrospectives or learnings in which the group may have done well or not and what are the following action plans for the next sprint iteration [16].

4.5.1 Development Requirements

1. Frontend

To develop the application, the team used Visual Studio Code as the code editor for building and debugging. The programming language on which SurveiRams is being built is Quasar Framework, with VueJS components as the front end. Furthermore, VueJs is a JavaScript framework for developing user interfaces. It is built on top of standard HTML, CSS, and JavaScript. It offers a declarative and component-based programming model that allows you to create simple or complex user interfaces quickly [18].

2. Backend and Database

Firebase is a Backend-as-a-Service (BaaS) that was used for the Authentication and Realtime Database services of the application's backend, allowing the team to focus on the front end. It is a cloud-hosted real-time NoSQL database that will enable users to store and sync data in real time and receive automated updates with the most recent data. With Firebase's real-time capabilities, whenever a user creates an incident report, it will automatically synchronize, and the new report will be immediately accessible. Please refer to 4.9.3 for a more detailed explanation.

3. Data Center

The adaptability, scalability, and speed of cloud data centers make them the ideal setting for mobile application development. Today's mobile applications must be able to process massive amounts of data, causing bottlenecks and poor performance if a business chooses a conventional data center. By opting for a cloud data center, enterprises may take advantage of nimble expansion, enhanced application performance and dependability, continuity, lower costs over time, and a better capacity to develop future-proof applications.

4.5.2 Development Workflow and Version Control

Managing the workflow and maintaining version control is vital to any development. It is a method for managing changes and determining those to update or delete. To manage the development workflow, the team uses Git and GitHub. Git maintains a reference to a snapshot of the current state of all files when you commit or save the state of your project. To be as efficient as possible, it only stores links to previously stored comparable files when those files have not changed. Unlike Git, a version controller, GitHub is now more available to the public and is mainly used for posting repositories, requesting changes, and working on a platform.

As Illustrated in Figure IV-5, it is here that software developers will be using Firebase, Quasar Framework, and Visual Studio Code for building SurveiRams. In managing the codes across developers, the team will use Git for version control and then send it to the repository in GitHub, where each developer would be able to collaborate and review changes as orderly as possible.

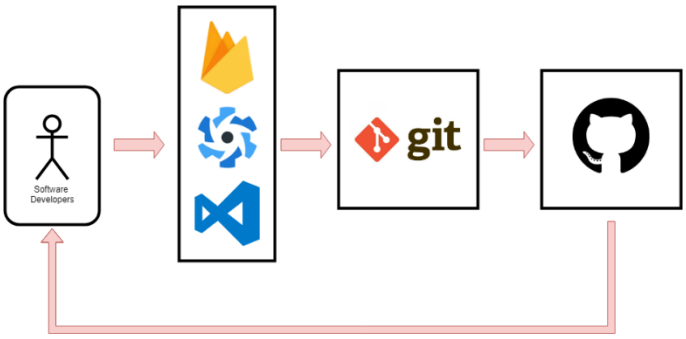

Figure IV-5 Development Workflow and Version Control

In using GitHub, separating development work from other features or the main repository is necessary when handling and merging versions. Branching handles these situations by isolating a new branch off an existing branch. For this development, Table 15 lists all active branches in which the development team has been managing for testing and later for merging to the master branch.

Table 15 GitHub Active Branches

Branch	Type	Description
Master	Production/Default	For Deployment
incident_report_branch	Development	All modules and functions regarding incident report are developed and tested in this branch.
patrolling_branch	Development	All modules and functions regarding patrolling are developed and tested in this branch.
user_manage_branch	Development	All modules and functions regarding user management and authentication are developed and tested in this branch.
logbook_branch	Development	All modules and functions regarding logbook are developed and tested in this branch.
qa_ir_branch	Testing	All modules and functions regarding incident report are to be tested for QA here.

1. Hardware Interfaces

SurveiRams will operate with the following environment and software components and applications. The application developed will be running under Android OS 10 and Windows 10 and 11. Since the application must run over the internet, all hardware is

required to connect to the internet. The hardware and the following specifications that will be running SurveiRams are specified in Table 16. No other hardware is required.

Table 16 Support Device Type

Device	Minimum Requirement	
Mobile Phone/Tablet	Processor	2 central processing unit (CPU) cores
	Random-access memory (RAM)	1 gigabyte (GB) (Assuming no other apps are running in the background or other unnecessary apps installed)
	Storage	8 GB Internal Storage
Computers/Laptop	Processor	2 central processing unit (CPU) cores
	Random-access memory (RAM)	8 gigabyte (GB) RAM
	Hard Drive	At least 1 gigabyte (GB)

2. Software Interfaces

The researchers developed SurveiRams, a mobile application that will record incident reports and activities while patrolling. SurveiRams are the primary medium that will be used to exchange information between security guards and the concerned administration.

The mobile application covers a wide range of features. One of its features will enable users to log their activities to report on completed tasks on each floor or location. In addition, while on patrol, the user will be able to record any incidents discovered.

Besides the guards themselves and the administration, no one else will know the security personnel's tasks. Additionally, a dashboard will be accessible to authorized users – the security head, BMO, and ITRO where they can view the reports submitted and gain insights into the overall reports.

The project makes use of a variety of software interfaces. The user interfaces were created using the Quasar Framework. It acts as the primary application server, utilizing Firebase as the central database server. Table 17 shows the software used for the development of SurveiRams application:

Table 17 Software Interfaces

Software used	Description
Database	Firebase
Operating System	Windows, Android OS 10

Programming Language	Vue, JavaScript, Java, HTML, SCSS
Front end	Quasar
Browser	Brave, Microsoft Edge, Google Chrome
Source Code Editor	Visual Studio Code

3. Communication Interfaces

The communication architecture must follow the client-server model. The main communication link that SurveiRams will be using is the internet to communicate with Android devices. In terms of database connection, Firebase handles requests and returns responses to the client via WebSocket. This allows Firebase to provide real time updates to browsers or mobile apps, such as push notifications or chat. Web sockets keep the connection open without closing it, allowing the client to get data from the server without explicitly asking for it. Firebase services encrypt data in transit with HTTPS and logically isolate customer data. Additionally, Firebase Hosting supports TLS 1.2. The messages transmitted between the server and its clients are expressed and stored as JavaScript Object Notation (JSON) and synchronized in real time to every connected client.

4.5.3 Testing Requirements

The QA Test and Staging/Pre-Production Environment that will be used are seen in https://sway.office.com/LEKldgtZ9KHEEaxB. Further instructions on how to install the application are detailed in the given link.

4.6 Implementation Plan

SurveiRams aspires to give valuable experience that will improve the stakeholders' quality of life and innovate their processes. To ensure this objective is realized, the system's developers will employ an agile methodology that allows them and their stakeholders to be more dynamically involved in the system's development. In this section, the developers will discuss how SurveiRams will continue to expand and improve the lives of its users before, during, and after the system's release.

4.6.1 System Implementation Setup

During their development, SurveiRams will undergo numerous modifications. To ensure that the system continues to improve with each iteration, the system's developers and stakeholders will continuously test the output of each module. For this to be possible, the system's modules must be accessible to stakeholders, even throughout the development phase, for testing and feedback. This section will enumerate the equipment and resources that the stakeholders will need to complete the following tasks:

- Guards & Head Guard
    - Android Mobile Phone
    - Cellular Data or Wi-Fi

- BMO & ITRO
    - Windows Desktop PC or Laptop
    - LAN Connection or Wi-Fi

With the tools and resources listed above, the stakeholders can consistently test and use every feature and iteration of the proposed system. They will then be able to give feedback corresponding to their needs.

4.6.2 Post-System Release Plan

After the system is fully released to the stakeholders, it will undergo regular tests to continue improving and maintaining its functionalities. The testing phase involved is referred to as Post-Development Testing.

1. Post-Development Testing

Testing after the system has been deployed to production is known as post-deployment testing. This sort of testing is performed on the system after it has been tested. Even with all the planning and testing before the system is finally deployed, getting user feedback is essential to improving a system. This testing may help us spot issues not discovered before the system was put into production. It ensures that the system conforms to the requirements of the user in question. The feedback provided by users may take several forms, such as the reporting of errors or the provision of recommendations for enhancing the system.

4.7 Implementation Results

Overall, the system is expected to yield great results. Once the client's specifications and requirements have been resolved, the system has undergone proper quality assurance and control. The developers anticipate that the system will become an essential asset to its stakeholders' daily tasks. This will allow them to perform previously paper-based functions in a digital and simpler medium that will not only be accessible online but also provide them with a better quality of life.

4.8 System Architecture

The figure below is an abstract representation of the component architecture of the system (SurveiRams). It gives a concise description of the component architecture of the system to facilitate component to component connections and system operation.

Figure IV-6Figure IV-6 depicts the system architecture visually. It illustrates the relationships between the system's many components and describes the functions of each. The general system model illustrates the system's primary functions and the interactions between its many components.

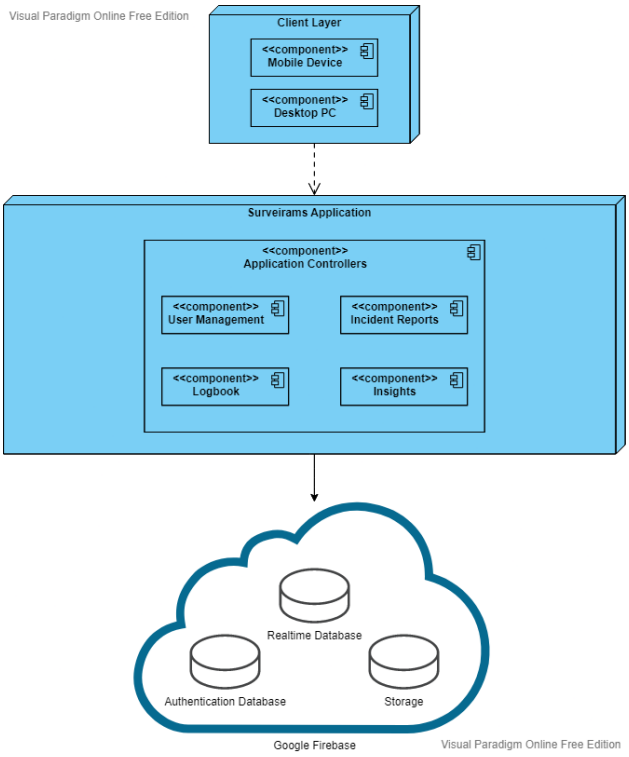

Figure IV-6 System Architecture

4.8.1 Pre-System Release Plan

Before the system is fully released to the stakeholders, the developers and stakeholders will undergo two types of testing phases. This is to ensure that all the modules and components are at par with the stakeholder's specifications and requirements by the system's release. The two testing phases are as follows (1) Module User Acceptance Test (MUAT) and (2) System User Acceptance Test (SUAT).

1. **Module User Acceptance Test (MUAT)**

The purpose of this test is to let the stakeholders evaluate the current state of each module the system will provide. This phase will come after the developers and quality assurance have finished developing and testing one of the modules of the system. The module will then be sent and tested on each stakeholder's setup and document their reaction and feedback towards the module. This will enable the developers to improve each module further before merging it into the QA-Integrated System Branch for the next testing phase.

2. **System User Acceptance Test (SUAT)**

Once all modules have been integrated into the QA-Integrated System Branch, the next testing phase will begin. This test aims to enable stakeholders to use and test the consolidated modules in one system. This will allow the developers and stakeholders to observe and evaluate how each module will interact and garner more feedback on what

the stakeholders think can be done to improve the system before its release. Once this phase has concluded and the developers have improved the system based on the final feedback of the stakeholders, they will then merge the branch to the Master Branch, which will then be used to build the production application.

4.8.2 Client Layer

The system architectural layer primarily converts data between the SurveiRams Application and the user. Data may be sent in many forms through various channels. Consequently, the client layer is responsible for combining various formats into a standard format to facilitate efficient and successful communication. The client layer also adheres to the programming structure schemes defined for various languages. It offers the real time syntax necessary for communication between two objects, such as layers, systems, and networks.

4.8.3 SurveiRams Application

The SurveiRams Application serves as the container for all controllers that manage the modules necessary for the users to continue with their everyday tasks. The application's responsibility is to give data and exchange data with the cloud database to allow dynamic data consumption between the user and Google Firebase.

4.8.4 Google Firebase

Google developed the Google Firebase mobile application development platform. It provides robust tools for developing, managing, and enhancing mobile applications. Firebase is a backend platform used to develop mobile and web applications. Firebase is, at its core, a set of tools that developers can depend on to build apps and grow those applications in response to user demand. SurveiRams utilizes the core features of Firebase, and are its database management, file storage, and authentication.

1. Realtime Database

The Firebase Realtime Database enables the development of sophisticated, collaborative apps by providing direct, secure database access from client-side code. Data is stored locally, and real time events continue to trigger even when the user is offline, offering the user a responsive experience. Realtime Database synchronizes local data changes with distant updates that happened while the client was offline, instantly resolving any discrepancies.

The Realtime Database offers a robust, expression-based rules language called Firebase Realtime Database Security Rules for defining how data should be formatted and when it may be read or written. When Firebase Authentication is implemented, developers may specify who has access to which data and how they can access it.

As a NoSQL database, the Realtime Database offers different optimizations and capabilities than a relational database. The Realtime Database API is intended to provide those actions that can be done rapidly. This allows the system to create a responsive real-time experience capable of serving millions of visitors. Therefore, it is essential to consider how users will need to access and organize the system's data correctly.

2. Authentication

Firebase Authentication offers backend services, simple SDKs, and pre-built UI frameworks to authenticate users inside the system. It allows authentication using passwords, phone numbers, and well-known federated identity providers such as Google, Facebook, and Twitter, among others.

Firebase Authentication interacts directly with other Firebase services and utilizes industry standards like OAuth 2.0 and OpenID Connect, making it simple to connect with the system's backend.

3. Cloud Storage

Cloud Storage for Firebase is a robust, easy-to-use, cost-efficient object storage solution designed for the Google scale. Regardless of network condition, the Firebase SDKs for Cloud Storage give Google security to file uploads and downloads for Firebase applications.

The system may store photos, music, video, and other user-generated material using our SDKs. The system may access duplicate files on the server using Google Cloud Storage APIs.

4.9 Performance

The team has executed the testing of the performance of the application where the expected outcome should be less than three seconds when a user executed an action. With that said, Table 18 shows the performance of the application.

Table 18 Performance Testing Result

Test	Expected Result	Actual Result
Login	Less than or equal to 3 seconds	1 user = 400 ms Average 20 users = 443 ms Average 100 users = 525 ms Average
Create Incident Report / Log		1 user = 579 ms Average 20 users = 631 ms average 100 users = 746 ms Average
Create User		1 user - 336 ms Average 20 users = 376 ms Average 100 ers = 435 ms Average

4.10 Team Composition

Table 19 depicts all the roles and responsibilities of the team.

Table 19 Team Composition

Role		Assigned to	Responsibilities
Stakeholders	ITRO Head	Jojo Castillo	They contribute to achieving a project's strategic goals because they are either actively involved in the project or have interests that its success may impact.
	BMO Head	Marr Bringas	
	Head Guard	Mervin Quilang	
Product Owner		Mariah Mirarza	Manages the product backlog and ensures the system realizes maximum value from a product
Scrum Team	Scrum Master and Quality Engineer	Kyle Dumbrique	Maintains the development team's orderly organization and progress on the agreed-upon tasks. Test products to ensure they fulfill quality standards and specifications
	Software Engineer	James Heramil	Back-end and System Security
	Software Engineer	Lionel Ejorango	Front-end and Database
	Technical Writer	Shiaramae Faburada	Responsible for writing product documentation that describes the product's features and benefits.

4.11 Document Security

4.11.1 Frontend Security Implementation

The Quasar server and clients communicate using Transport Layer Security (TLS). This protocol provides privacy, data integrity, and authentication between interacting components. The application data comprises an unsigned message length of 4 bytes and a serialized message. The maximum message length is 2^{32} bytes, and the maximum message size is 5 MB to prevent client or server resources from being depleted.

4.11.2 Backend and Database Security Implementation

SurveiRams' backend applies role-base access control. In terms of user access, users can only access their specific roles using the backend logic. The system applies authentication with proper credential handling, thus, making sure that access to the system is always secure.

A secure, dependable, and scalable database is quickly becoming necessary for any application, regardless of the programming language used to create it. Firebase provides real time database functionality for building web applications and built-in data storage and access security. The Firebase Realtime Database Security Rules specify who has read and written access to the database, how data is formatted, and which indexes are present.

These rules are stored on Firebase's servers and are automatically enforced. Every read-and-write request will only be processed if the rules allow it. By default, the rules prevent anyone from accessing your database. This is done to avoid the exploitation of the database until these rules can be adjusted or authentication implemented. Furthermore, Firebase services encrypt data in transit through SSL 1.2 and logically isolates customer data with HTTPS, and Firebase Realtime Database encrypts data at rest. The Personally Identifiable Information (PII) stored in the database includes the following:

- Name
- E-mail address
- Contact Number

4.12 Business Continuity Plan

Table 20 shows the business continuity plan for SurveiRams.

Table 20 Business Continuity Plan

<table>
<tr><td>Business Function:
Operations –</td><td>Recovery Time Objective:
1 week maximum</td></tr>
<tr><td colspan="2">Business Category
• Operations
• Technology and Process Development</td></tr>
<tr><td>Departments impacted:
Building Security Office
Building Maintenance Office
I.T. Resource Office</td><td>Key Personnel:
Security Head
BMO Head
I.T Head</td></tr>
<tr><td>Lost Sales and Income:
N/A
One week estimate:
N/A
One month estimate:
N/A</td><td>Regulatory Fines:
N/A
Contractual Penalties:
N/A</td></tr>
</table>

The Failure Types to Identify can be seen in Table 21.

Table 21 Failure Types

Failure Type	Probability	Impact	Recovery Action	Recovery Mode
Client-Side Injections	Unlikely	High Risk	Patch Vulnerability	Manual
Data Breach	Unlikely	High Risk	Initiate a Fraud Alert	Manual
Improper Handling of Session	Unlikely	High Risk	Patch Vulnerability	Manual
Insecure data storage	Unlikely	High Risk	Contact Vendor for Handling (Google Firebase)	Manual
Security Misconfiguration	Unlikely	High Risk	Update Security Configuration	Manual
Server Shutdown	Unlikely	High Risk	Contact Vendor (Google Firebase)	Manual
Substandard Authentication and Authorization	Unlikely	High Risk	Contact Vendor for Handling (Google Firebase)	Manual
Absence of API Protection	Unlikely	Medium Risk	Patch Vulnerability	Manual
Hardware Failure	Unlikely	Medium Risk	Repair or Replacement Hardware	Manual
Insufficient Transport Layer Protection (TLS)	Unlikely	Medium Risk	Contact Vendor for Handling (Google Firebase)	Manual
Internet Loss	Likely	Medium Risk	Utilize Mobile Data or Contact ISP	Manual
Power Outage	Unlikely	Medium Risk	Backup Generators	Automatic
Server Overload	Unlikely	Medium Risk	Load balancing	Automatic
Theft	Unlikely	Low Risk	Disable Account and Contact Law Enforcement	Manual

Glossary:

- **Absence of API Protection** – Occurs when third party APIs available within a system have little to no security measures.
- **Client-Side Injections** - Resulting in the execution of malicious code on the mobile device via the mobile application.
- **Data Breach** - Is a security breach that occurs when sensitive, protected, or confidential information is copied, communicated, viewed, stolen, or utilized by an unauthorized person.

- **Hardware Failure** - Failure of the electrical circuitry or electromechanical components
- **Improper Handling of Session** - Upon a future transaction between the mobile app and the backend servers, the session token is mistakenly shared with the attacker.
- **Insecure Data Storage** - Arise when development teams presume that users or malware will not be able to access a mobile device's filesystem and sensitive information stored in its data storage.
- **Insufficient Transport Layer Protection (TLS)** - Is a security vulnerability caused by programs failing to safeguard network traffic
- **Internet Loss** - Is the whole or partial breakdown of internet services.
- **Power Outage** - Is the interruption of an electrical power network's supply to a consumer.
- **Security Misconfiguration** – Happens when important security parameters are not implemented or are implemented incorrectly
- **Server Overload** - Server Overload occurs when circumstances deplete a server's resources to the point where it cannot handle incoming requests.
- **Server Shutdown** - Describes the process of stopping all system processing in a controlled manner.
- **Substandard Authentication and Authorization** – To enable an attacker to anonymously execute functionality inside the mobile app or the mobile app's backend server.
- **Theft** - Is the act of stealing computer equipment.

V. Results and Discussion

The following are the wireframes of the system:

5.1 Login

The first set of wireframes is the Log screen of the SurveiRams application. The three figures show and discuss the result of login. In Figure V-1, users can see the login page where they will input their credentials to log in to their accounts. However, if the user inputs an invalid credential shown in Figure V-2 and Figure V-3 the system will prompt the user to enter a valid email or address.

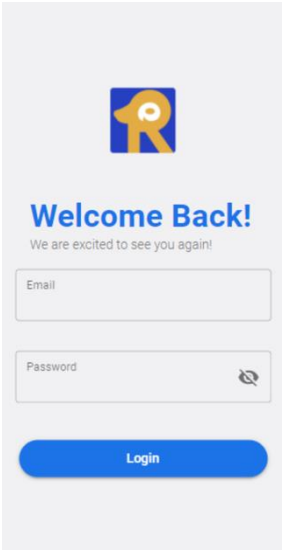

Figure V-1 Default Login Screen

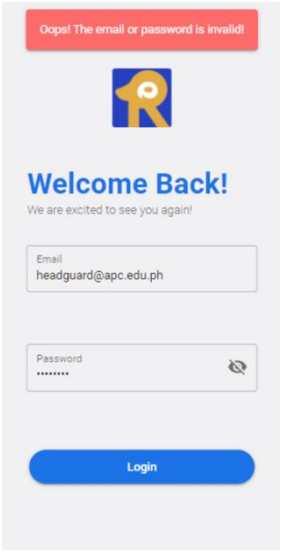

Figure V-2 Login Error Prompt

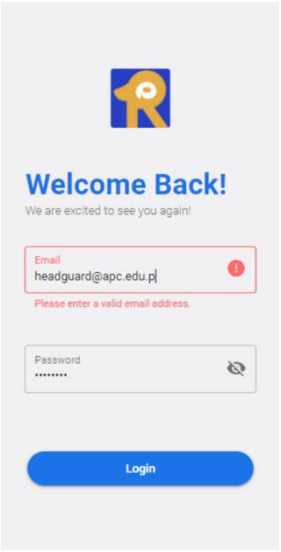

Figure V-3 Login Error Prompt

5.2 Home

The home screen of the SurveiRams application has a four-type of view for the head guard, guard, BMO, and ITRO home screen. In Figure V-4, the head guard home screen can view the incident report, logbook, and insight. Head guards are the only ones with a start patrol feature on their home screen and can view the other guard's incident reports. While in the guard's home screen on Figure V-5, they can create logs and view incident reports.

For Figure V-6 and Figure V-7, BMO and ITRO users can both see the user management system and view reports and insights. Lastly, Figure V-8, Admin user can view all the activities in application such as incident report, user management, logbook and insights.Figure III-1

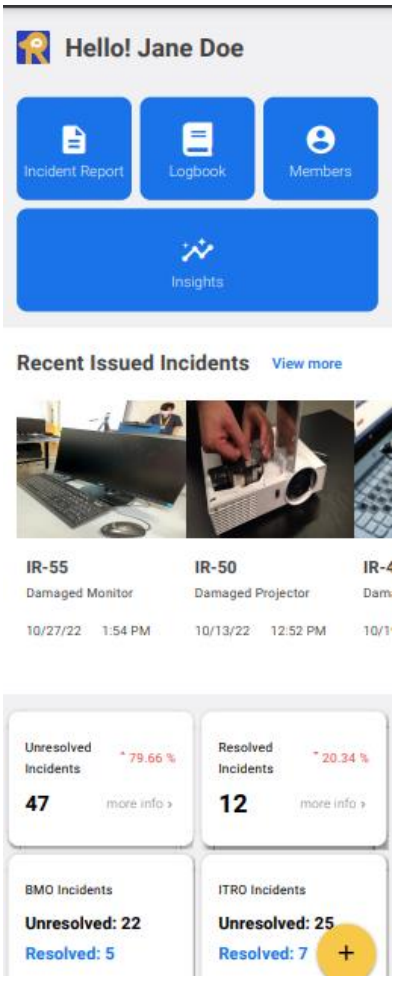

Figure V-4 Head Guard Home Screen

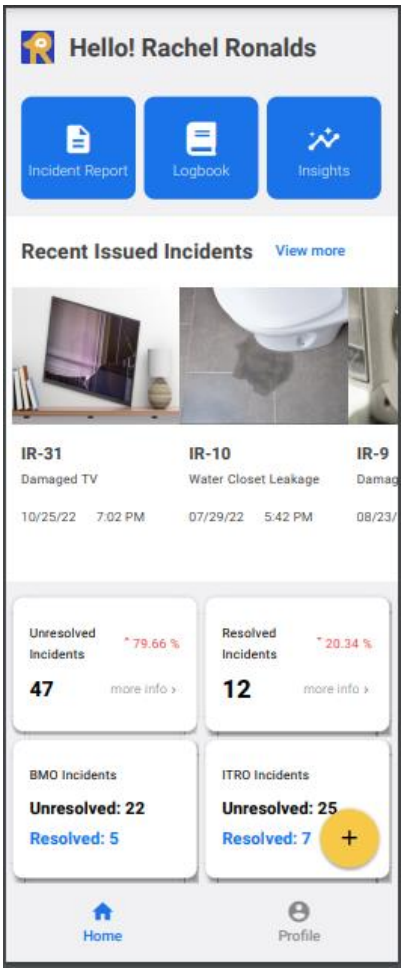

Figure V-5 Guard Home Screen

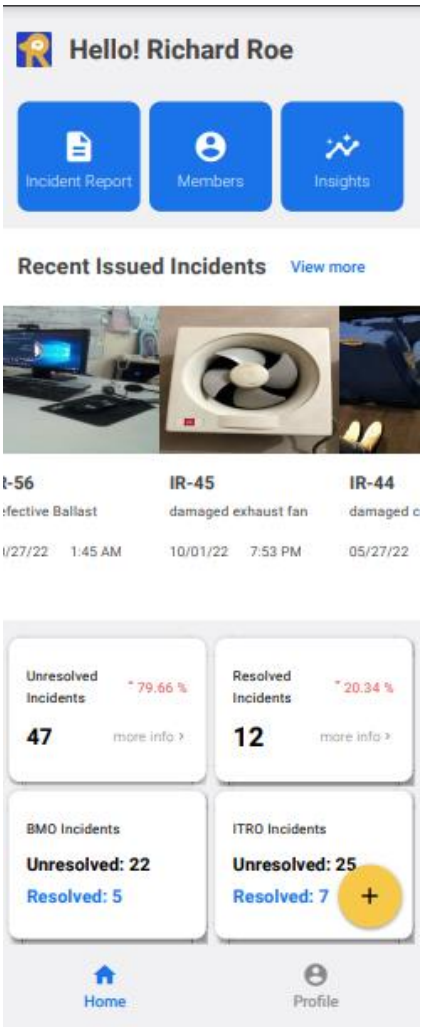

Figure V-6 BMO Home Screen

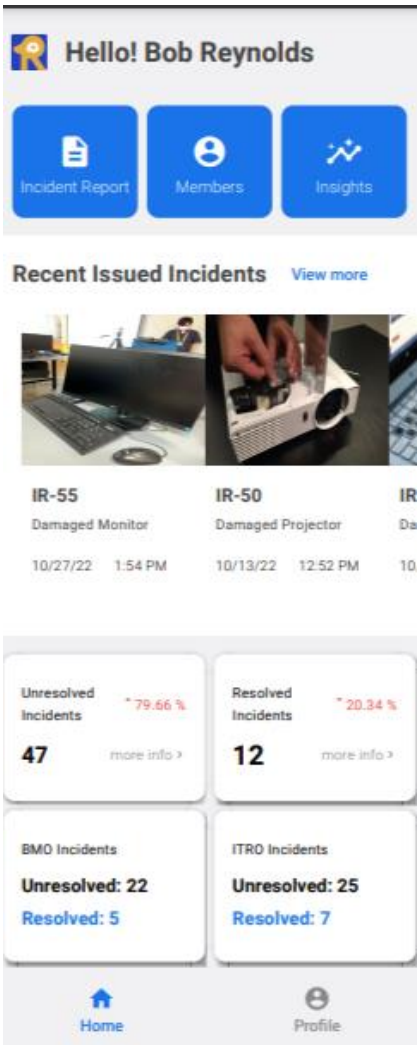

Figure V-8 ITRO Home Screen

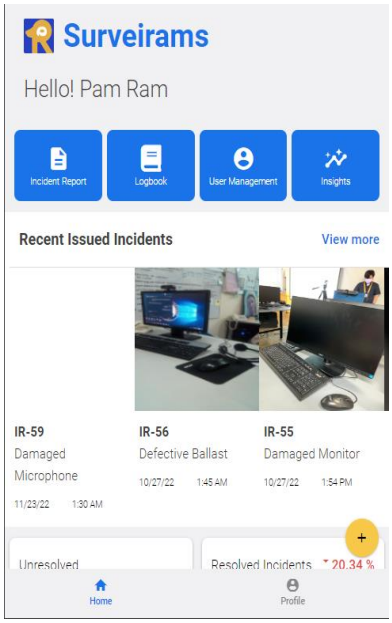

Figure V-7 Admin Home Screen

5.3 User Management

For user management, BMO can only view the user's information from their user management view, unlike ITRO user management, the user can read, update, and create a user registration. Figure V-9 can view the member list, while in Figure V-10 user can read and edit the user's account information and update it shown in Figure V-11. ITRO users can create or register a new user, as shown in Figure V-12.

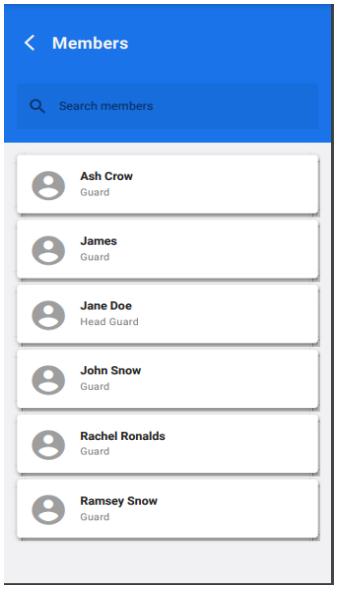

Figure V-9 Members List

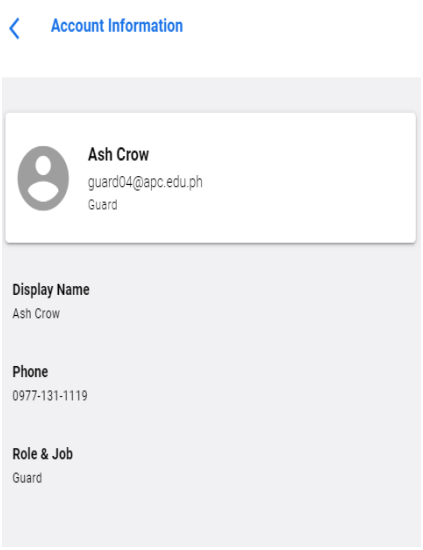

Figure V-10 User Management Read

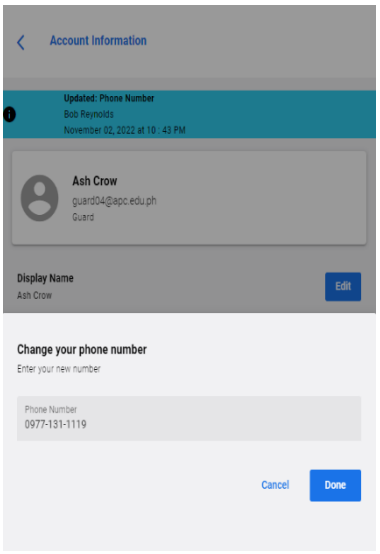

Figure V-11 User Management Update

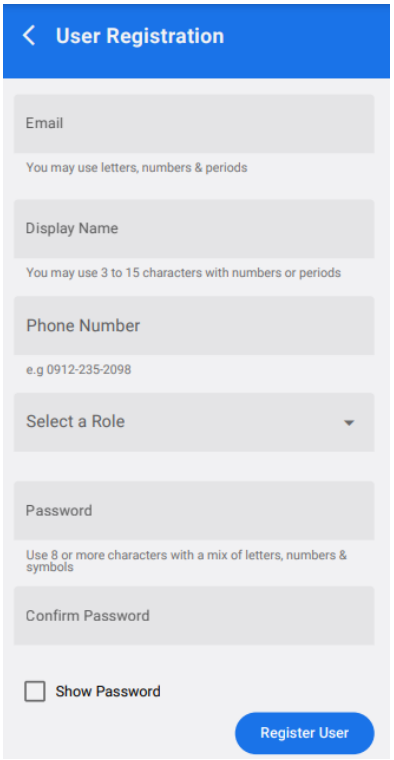

Figure V-12 User Management Create

5.4 Incident Reports

The incident reports page has a feature where users can view the resolved and unresolved incident reports shown in Figure V-13 and Figure V-14. Each incident report can view the details in Figure V-15. It indicates there the incident number and which department issued the incident. For incident details in Figure V-16, the type of incident location, photos of the incident, and the description can be seen there. Figure V-17 shows the features of sorting the incident report from the past to the latest report.

Figure V-18 shows the view of the resolved incident. There is a date and time of the resolved incident and who resolved it, while in Figure V-19, the department who resolved it will fill up the description, root cause, and solution. Figure V-20 shows how to create an incident report by filling-up the date and time of the incident and the responsible department. In Figure V-21, by selecting the type of incident and location, the users need to upload a photo of the incident to be able to submit the incident reports.

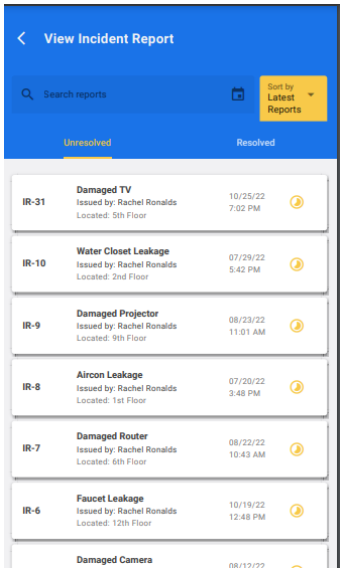

Figure V-13 Unresolved Incident Reports

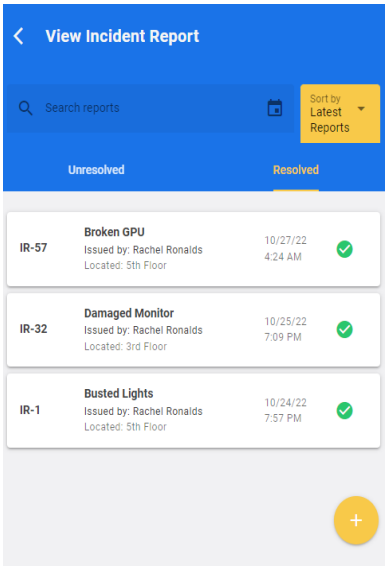

Figure V-14 Resolved Incident Reports

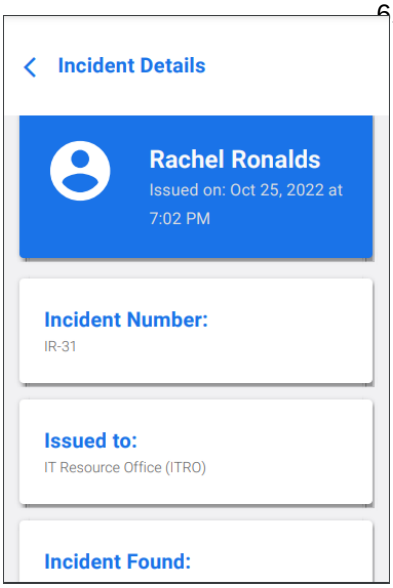

Figure V-15 View Incident Report

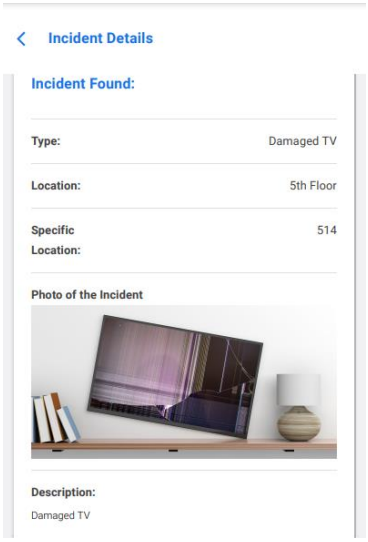

Figure V-16 View Incident Report

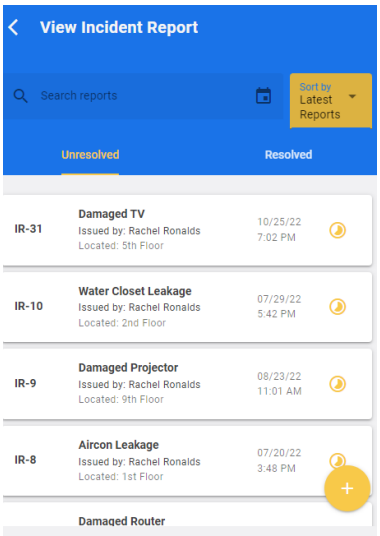

Figure V-17 Sort Incident Reports

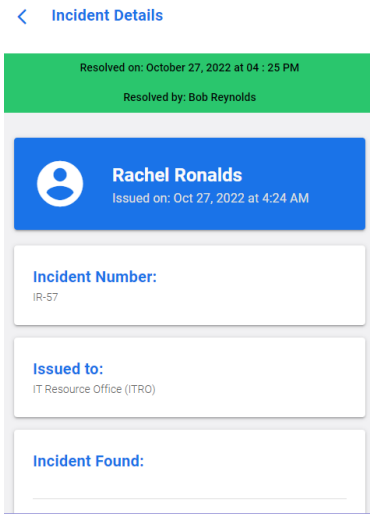

Figure V-18 Resolved Incident Report

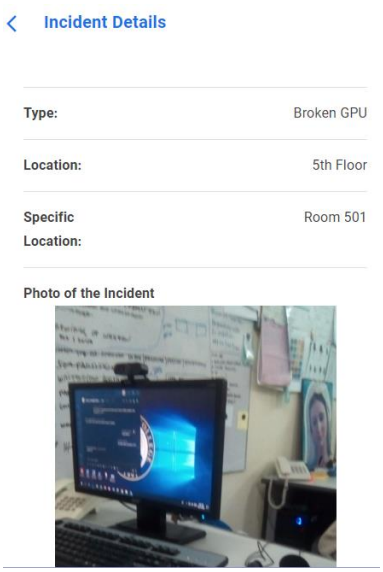

Figure V-19 Report

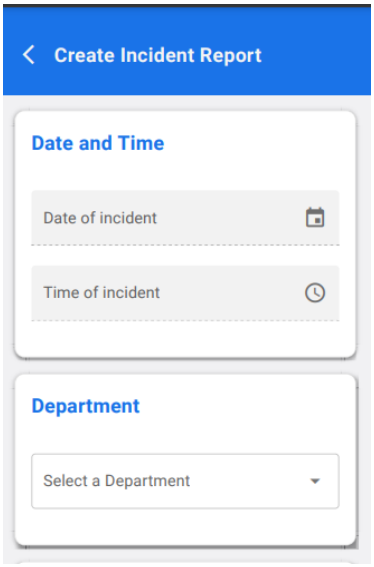

Figure V-20 Create Incident Report

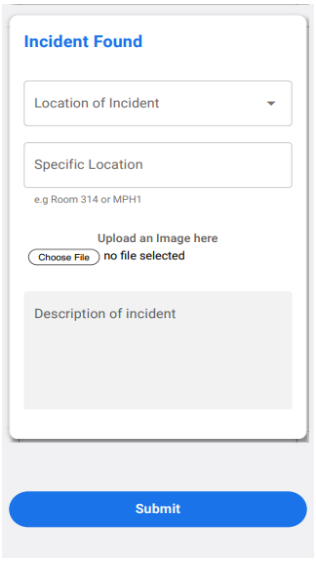

Figure V-21 Submit Incident Report

5.5 Patrol and Logs

Figure V-22 shows the list of incident reports in view logs. While Figure V-23 shows the verified patrol logs of every guard who is assigned to a specific floor. To create a patrol log, one needs to select a location and fill in the necessary information, such as location, descriptions, and tasks accomplished, as shown in Figure V-24.

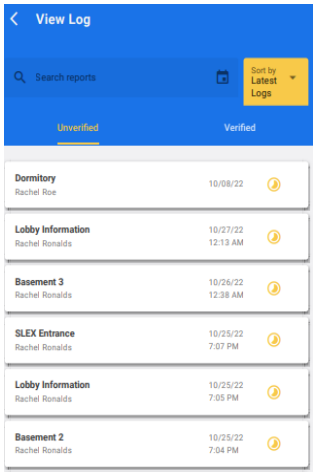

Figure V-22 View Log

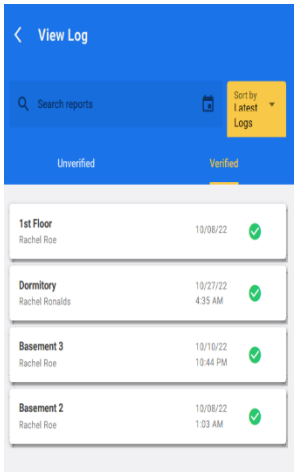

Figure V-23 Verified Patrol Log

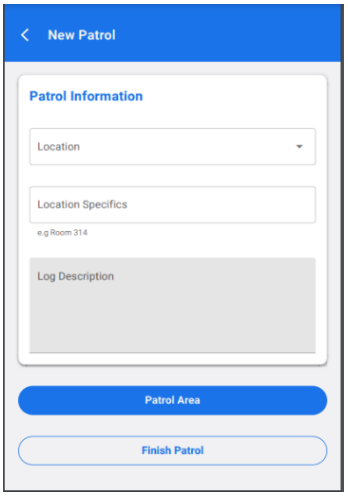

Figure V-24 New Patrol Log

5.6 Insights

All users of the SurveiRams application have an insight view. Figure V-25 is the incident analytics, such as the total number of incidents and resolved incidents, the most common departments reported to, and the most common locations where incidents happened.

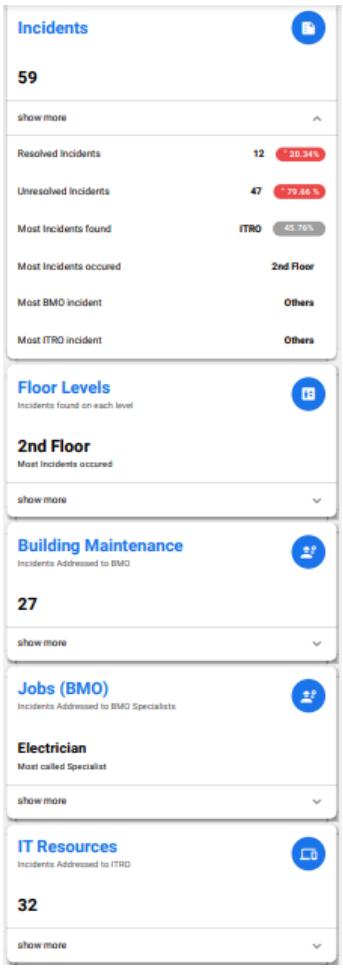

Figure V-25 View Insights

VI. Conclusions and Recommendations

SurveiRams is a mobile application intended to serve as a ticketing system for APC's security personnel, BMO and ITRO. The security personnel will use the mobile application to input their incident reports and patrol logs. BMO and ITRO will use it to view the reports directed to their respective offices and update its status.

In terms of accomplishments, the team was able to identify and resolve the pain points of the head guard, the Building Maintenance Office (BMO), Information Technology Resource Office (ITRO) and security personnel.

The researchers finalized the basic functions and developed a working prototype for each proposed feature using the user stories and meetings with the project adviser, consultants, and clients. All system data will be stored in a centralized location through Firebase. The insights feature of the system will be used to interpret and assist in the decision making of the administration

The following recommendations are made to show improvements to the proposed system:

- Integrate processes for Asia Pacific College's other departments such as the Discipline Office for the violation management system.
- Local storage input for seamless process even without internet connection
- Integrate inventory management for the Building Management Office
- Compatibility to other operating systems such as iOS
- Incorporate graphical based analytics such as Apex charts or Charts.js

VII. Appendices

7.1 Other Relevant Diagrams

In this section, all diagrams relevant to the system is shown.

7.1 1 Event Table

Table 22 Event Table

Event	System State	Response
Security Personnel logs in	User is redirected to Home Page	Home Page is displayed
Head Guard logs in		
ITRO Logs in		
BMO Logs in		
ITRO creates an account	User Management page is displayed	System stores data in the database
Security Personnel clicks on new log	Create log page is displayed	System stores data in the database; logs sent to logbook
Head Guard clicks on new log		
Security Personnel clicks on new incident report	Create incident report page is displayed	System stores data in the database; Entries sent to Incident Reports
Head Guard clicks on new incident report		
Security Personnel clicks on Incident Report button	Incident Reports page is displayed	System displays stored incident reports
Head Guard clicks on Incident Report button		
User clicks on insight	Insights page is displayed	System displays stored data
BMO updates incident report status	Incident Reports page is displayed	System stores data in the database
ITRO updates incident report status		
Head Guard authentication	User cannot proceed to home page	User input an invalid credentials
Guard authentication		
BMO authentication		
ITRO authentication		
Head Guard read incident report	Incident reports page is displayed	System displayed store data in database
Guard read incident report		
BMO read incident report		
ITRO read incident report		
Head Guard update logs	Log page is displayed	System stores updated data in the database
Head Guard read logs	Log page is displayed	System displayed store data in database
Guard read logs		
Head guard read profile	Profile page is displayed	System displayed store data in database
Guard read profile		
BMO read profile		
ITRO read profile		

Head Guard read insights	Insight page is displayed	System displayed store data in database
Guard read insights		
BMO read insights		
ITRO read insights		
BMO update incident report	Incident report page is displayed	System stores updated data in the database; Entries sent to resolve Incident Reports
ITRO update incident report		
ITRO update profile	profile page is displayed	System stores updated data in the database

7.1.2 Activity Diagram

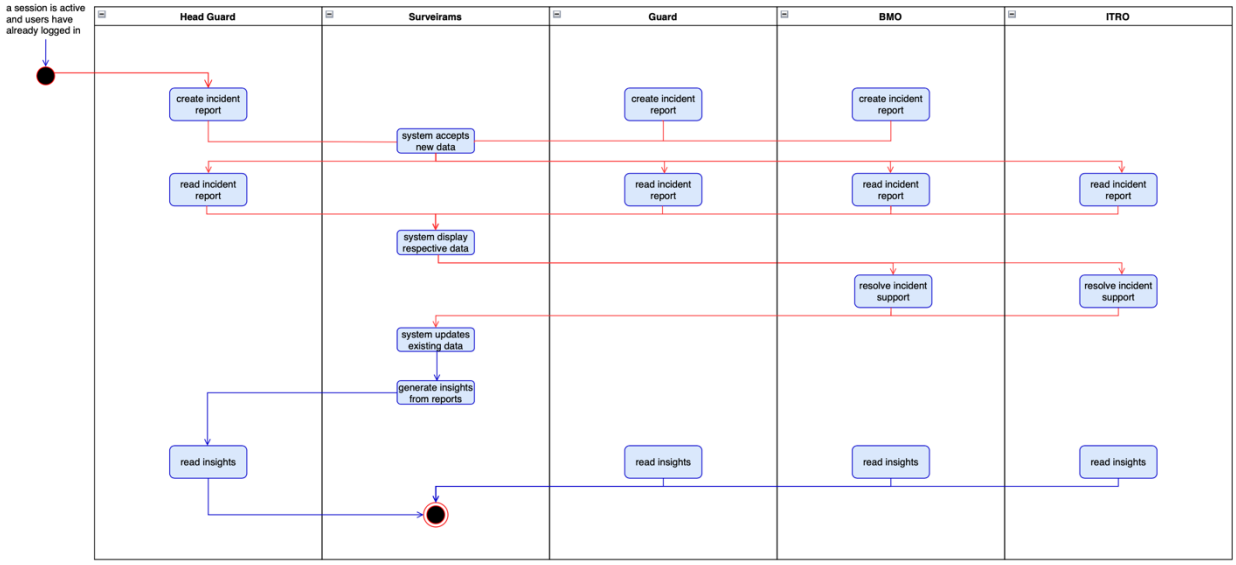

Figure VII-1 Manage Incident Report and Insights Activity

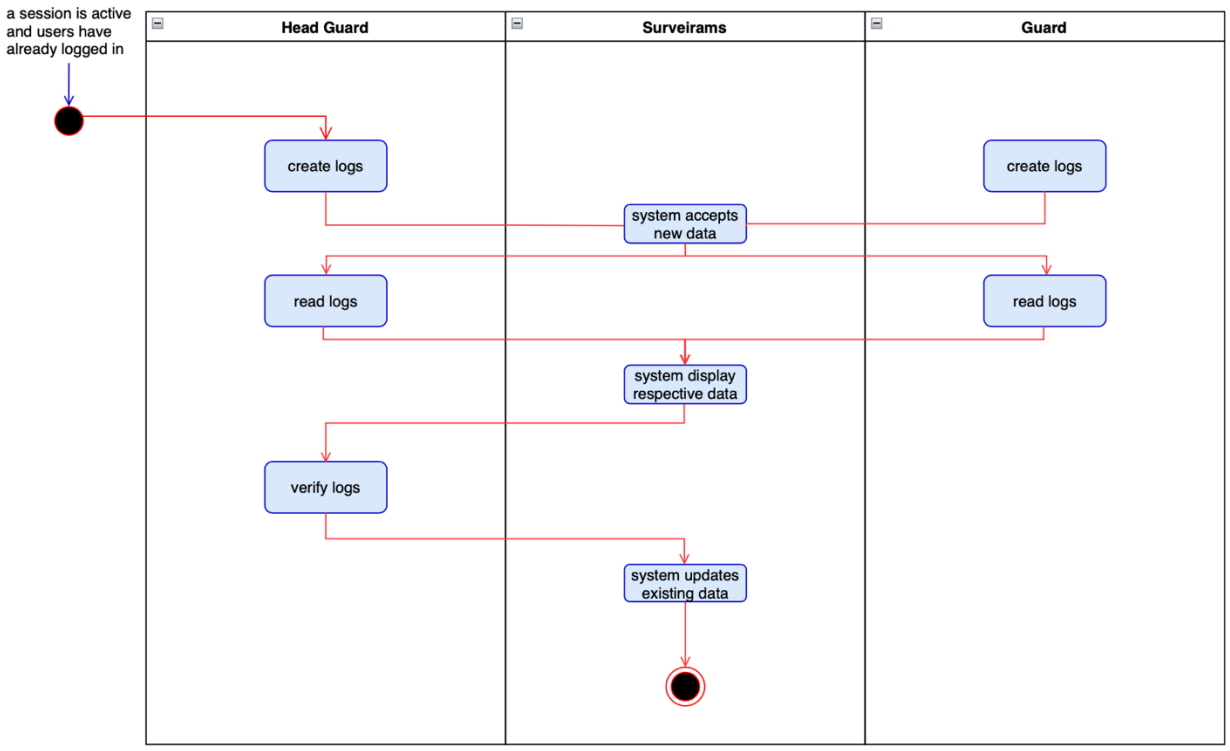

Figure VII-2 Manage Logs Activity

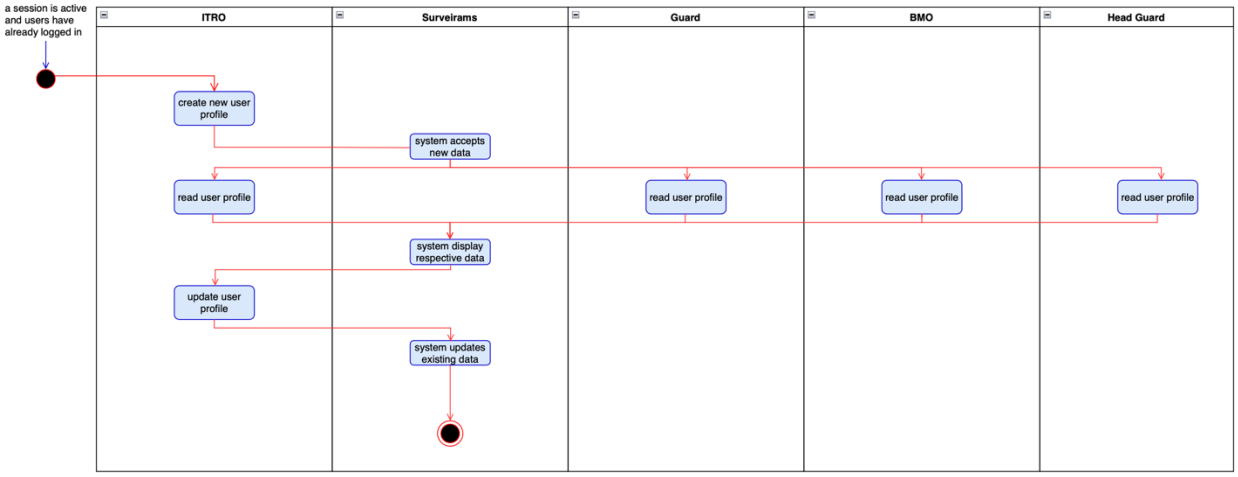

Figure VII-3 Manage User Activity

7.1.3 Class Diagram

7.1.4 Sequence Diagram

7.1.5 State Transition Diagram

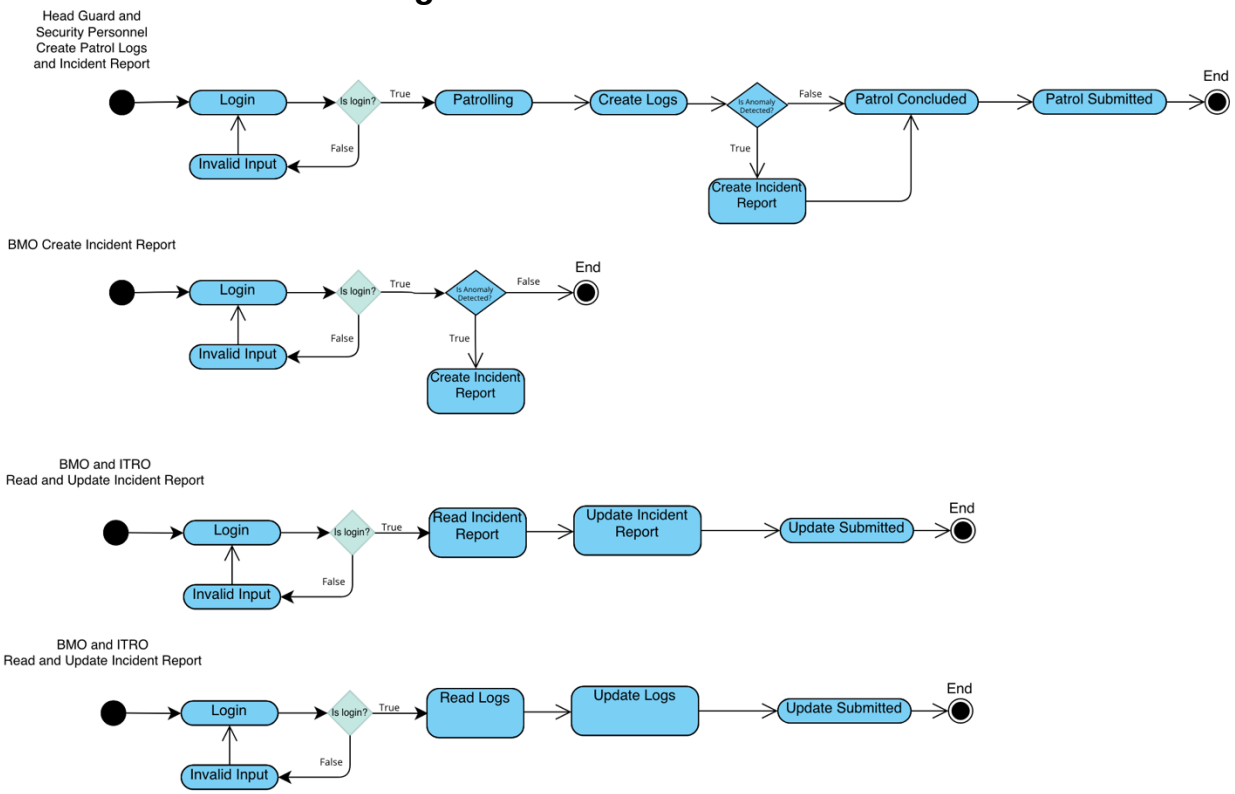

Figure VII-4 State Transition Diagram

7.1.6 Package Diagram

7.1.7 Component Diagram

7.1.8 Functional Decomposition Diagram

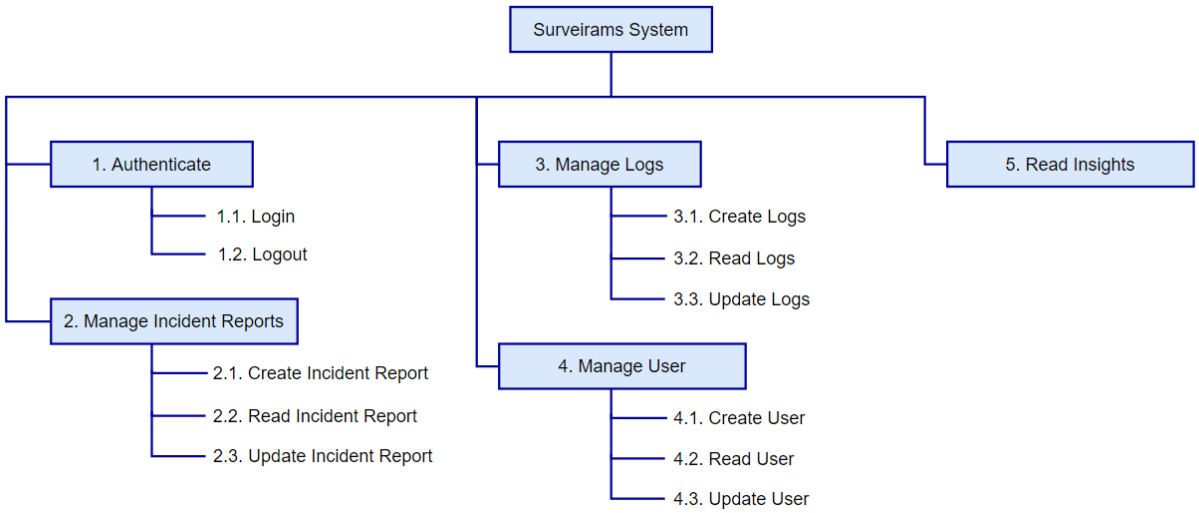

Figure VII-5 Functional Decomposition Diagram

7.1.9 Data Flow Diagram

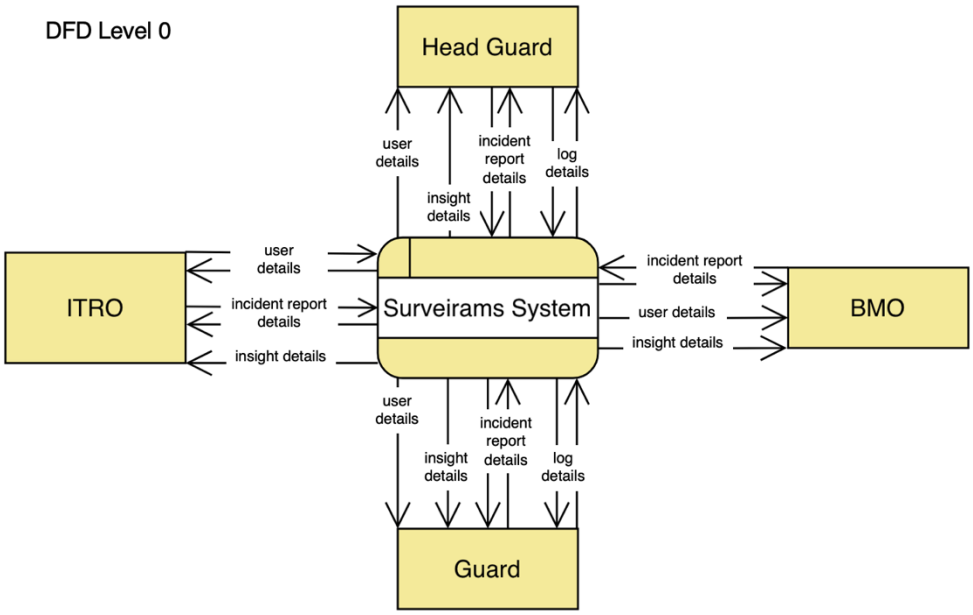

Figure VII-6 Data Flow Diagram Level 0

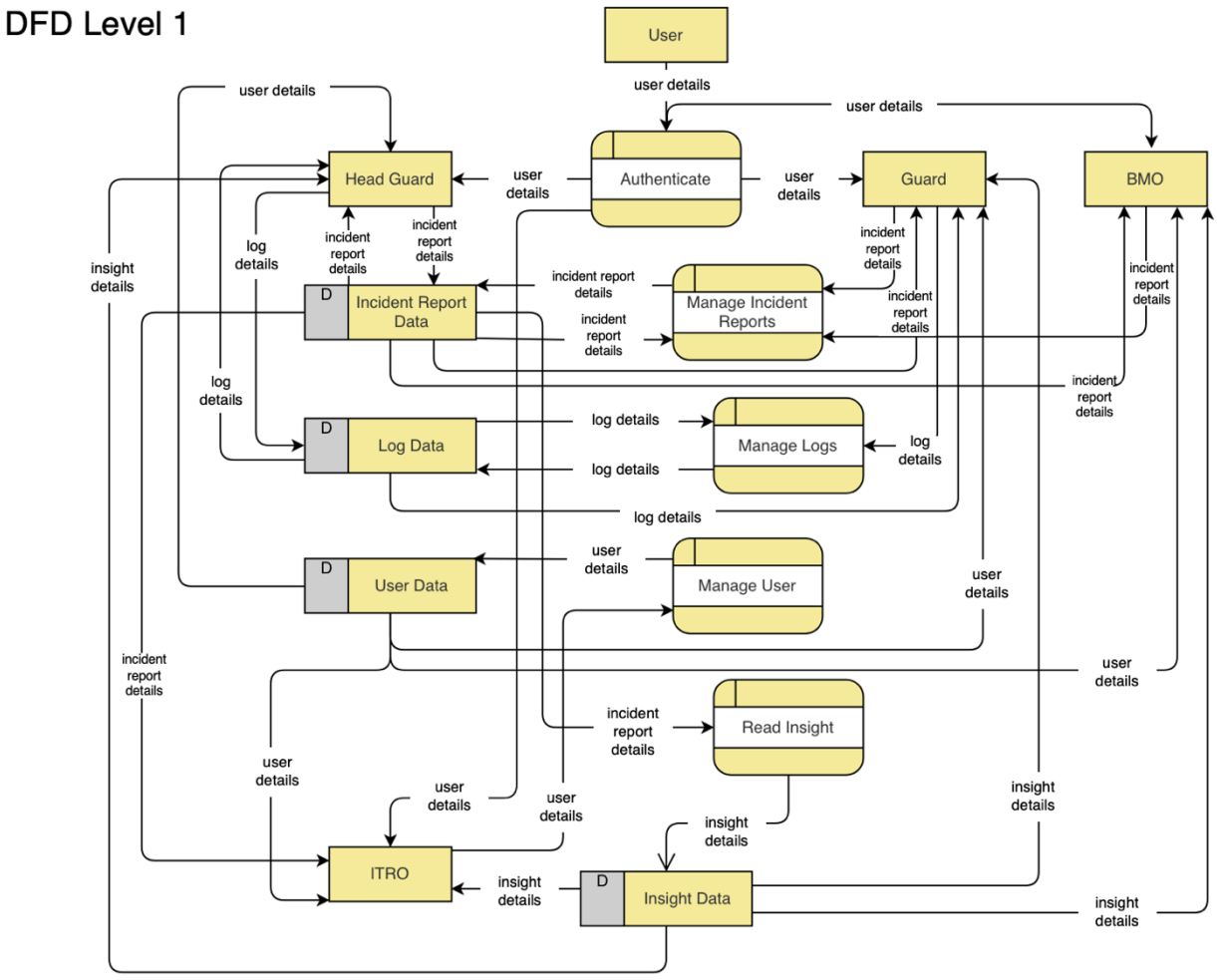

Figure VII-7 Data Flow Diagram Level 1

7.1.10 Cost Benefit Analysis

7.2 Relevant Links

7.2.1 Graphical User Interface Design

https://tinyurl.com/SurveiramsGUI

7.2.2 Source Code

https://github.com/Ciradyl/SurveiRams

7.2.3 Installation Guide

https://tinyurl.com/SurveiRamsInstallationGuide

7.2.4 User Manual

https://tinyurl.com/SurveiRamsUserManual

7.2.5 Software Requirements Specification

7.2.6 Test Documents

7.3 Team's Curriculum Vitae

7.3.1 James Aaron Heramil

James Aaron S. Heramil

+63 (915) 863 5005 | jamesheramil@outlook.com || www.linkedin.com/in/jamesheramil

PERSONAL INFORMATION

Date of Birth August 16, 2000
Home Address 308 Cyprus Bldg., Kassel Residences, E. Rodriguez Street, Brgy. Moonwalk, Parañaque City

CAREER OBJECTIVE

A Computer Science major with industry experience in cybersecurity and forensics and robotic process automation (RPA) development. Familiar with cyber security fundamentals and programming. I am looking for a cyber security analyst position where I can contribute my technical and non-technical skills.

SUMMARY OF SKILLS

- RPA Developer
- Cyber Security Analyst

WORK EXPERIENCE

Accenture Philippines – RPA Developer Intern
February 2019 – May 2019

- Primarily involved in migrating RPA processes from third-party tool to proprietary platform.
- Organized, tested, and monitored automated workflows to guarantee the error-free operation of business processes.
- Monitored and maintained automation post-implementation and addressed difficulties to guarantee business activities ran smoothly.

Poseidon IT Solutions – Junior Security Analyst 1
October 2021 – December 2021

- Executed activities such as vulnerability management, application development security, business continuity, networking, and risk management on information security.
- Performed incident response and computer forensics at the first level
- Assessed security controls and assessed the security posture of internal organizational controls

NovoCrew Inc. – Junior Security Analyst 1
January 2022 – June 2022

- Conducted security evaluations utilizing vulnerability testing and risk assessment
- Conducted internal and external security audits.
- Analyzed security breaches to determine their origin
- Kept the company's incident response and catastrophe recovery strategies current.
- Verified the security of third-party providers and worked with them to satisfy security standards.

EDUCATION

Asia Pacific College – BS in Computer Science majoring in Cybersecurity and Forensics June 2019 – Present (Anticipated: 2023)
Asia Pacific College (Senior High School) – STEM June 2017 – May 2019

ORGANIZATIONS

- Director of Marketing and Promotions for Junior Philippine Computer Society Asia Pacific College Chapter from 2020 to 2021.
- Vice President SOAR for Junior Philippine Computer Society Asia Pacific College Chapter from 2020 to 2022.
- President of APC Band from 2021 to 2022.
- Membership Officer for Junior Information Systems Security Association 2021 to 2022
- Member of Microsoft Student Community from 2019 to 2022.
- Apprentice in APC Speaks (Public Speaking and Debate Organization) from 2017-2018.

SEMINARS

- **DSC Loyola – Tech Everywhere:** Using Technology in Cybersecurity (October 2020)
- **ISSA Philippine Chapter – Cybersecurity Conference:** Cybersecurity in the Philippines (October 2020)

CERTIFICATES

- **Web Developer Foundations** issued by IBM Skillsbuild - (04/2021 - Present)
- **Introduction to Web Development** issued by IBM Skillsbuild - (04/2021 - Present)
- **Introduction to Packet Tracer** issued by Cisco - (03/2021 - Present)
- **Enterprise Design Thinking Practitioner** issued by IBM - (04/2021 - Present)
- **Introduction to Cybersecurity Tools & Cyber Attacks** issued by Coursera - (10/2021 - Present)
- **Cybersecurity Roles, Processes & Operating System Security** issued by Coursera – (11/2021 - Present)

TECHNICAL SKILLS

Languages and Framework Python, Java, Javascript and PHP.

Operating Systems Windows, Kali Linux, CentOS, and Ubuntu

Software Visual Studio 2019, Eclipse, Jupyter, VMware, MySQL Workbench, NMAP, Metasploit, Snort, Wireshark, Burp Suite, Microsoft Office

ACADEMIC DISTINCTIONS

- **Dean's Lister for the School Year 2020-2021:** Acquired a GPA of 3.71.

- **Dean's Lister for the School Year 2021-2022:** Acquired a GPA of 3

7.3.2 Kyle Dumbrique

Name:	**Kyle Dumbrique**
Complete Address:	2157 A2 Piy Margal, Sampaloc
	Manila City
Contact Number:	Mobile No.: (0917) 504-8849
Email Address:	ksdumbrique@student.apc.edu.ph dumbrique.kyle13@gmail.com
Website:	https://keirique.wordpress.com https://www.linkedin.com/in/kyledumbrique/

Personal Statement	I am determined, adaptable, and prepared to learn new technologies as they become available in the industry. I'd like to use my talents as a productive worker to collaborate well with teams and learn from my colleagues. The experiences I get will help me to further develop my abilities as an individual and to position myself as an indispensable asset in an innovative sector.
Education	**Asia Pacific College**, Magallanes, Makati City **B.S. in Computer Science specializing in Cyber Security and Forensics** June 2019-present
Work-Related Courses	• Computer Security • Information Security • Legal Studies (Forensics) • Network Security, Storage & Data Communication • Web Penetration Testing and Security
Academic Projects	**The Viability of the KNN Algorithm as a Network Anomaly Detection Model** • Thesis 1&2, April 2022 - Present • Project Researcher • Co-executed the prototype testing and evaluation, identifying areas for improvement to ensure the algorithm works seamlessly **SurveiRams: Guard Verification System** • August 2022 – Present • Project Manager, Quality Assurance, Scrum Master • Led overall project development, facilitated scrum by ensuring the scrum framework is followed, and ensured the client product met performance, design, reliability, and maintainability requirements. • April – November 2021

	• Project Researcher and Developer • Co-developed the application using Quasar Framework and Android Studio **RAMS Violation Management System** • April – June 2022 • Project Documentation and Researcher • Spearheaded the development of the new system, planning and organizing the project regarding managing a team of developers, establishing timelines and meeting deadlines.
Technical Skills	• Highly skilled in MS Office: Word, Excel, PowerPoint • Intermediate knowledge and skills in Networking and Cyber Security • Proficient in Linux, Nmap, Nessus, Java, Python, Windows, VMware • Basic knowledge in Wireshark, Metasploit
Certifications	• CompTIA Security+ CompTIA, August 2022 – August 2025 • Remote Work and Virtual Collaboration CertiProf, December 2021 – December 2023 • Lifelong Learning CertiProf, December 2021 – December 2023 • Microsoft Certified: Azure AI Fundamentals Microsoft, June 2021 • Scrum Foundation Professional Certificate CertiProf, May 2021 – May 2023 • Fundamentals of Vulnerability Management Cybrary, May 2021 • Enterprise Design Thinking Practitioner IBM SkillsBuild, April 2021 • Microsoft Certified: Azure Fundamentals Microsoft, March 2021 • Cybersecurity Fundamentals IBM SkillsBuild, February 2021 • Introduction to Packet Tracer Cisco Networking Academy, January 2021 • NDG Linux Unhatched Cisco Networking Academy, December 2020 • Introduction to Cyber Security Cisco Networking Academy, December 2020 • Microsoft Excel (Microsoft 365 Apps and Office 2019) Microsoft, January 2020 • Microsoft Office Specialist CertiProf, January 2020

Awards & Recognitions	• Resource Speaker, "Cyber Security in Social Media, Emails, and Personal Accounts", July 2022 • Resource Speaker, "Into the Cyverse: Exceeding Visions in the Realm of Technological Opportunities", April 2022 • Honor's List, SY 2020-2021, SY 2021-2022
Seminars & Trainings Attended	• Cyber Security Digital Summit: APAC 2022 Cyber Security Hub, July 2022 • 2021 TMIE Virtual Cybersecurity Summit for University Students Trend Micro, October 2021
Extra-Curricular Activities	• **Microsoft Learn Student Ambassador** Gold, July 2021-present Beta, December 2020-July 2021 Alpha, January 2020-December 2020 • **Junior Information Systems Security Association – Asia Pacific College Chapter** Consultant, July 2022-present President, November 2021-July 2022 Officer-in-Charge for President, August 2021-November 2021 Trainee, November 2020-August 2021 • **Microsoft Student Community – Asia Pacific College Chapter** Consultant, July 2022-Present Vice President, July 2021-July 2022 Director for Documentations, August 2020-July 2021 Trainee for Documentations Committee, August 2019-August 2020 • **Junior Philippine Computer Society – Asia Pacific College Chapter** Director for Information and Documentations, June 2019-December 2020 Assistant Director for Information and Documentations, August 2021-November 2021 Committee Member for Information and Documentations, November 2020-August 2021 Trainee for Logistics, July 2019-November 2020

7.3.3 Lionel Kerwin Ejorango

Name:	**Lionel Kerwin Ejorango**
Complete Address:	2302 Tower 2 (Arnais Tower), The Beacon Towers
	Makati City
Contact Number:	Mobile No.: (0947) 114-5374
Email Address:	leejorango3@student.apc.edu.ph lioneejorango@gmail.com
Website:	https://kerkz.artstation.com/ www.linkedin.com/in/lionel-kerwin-ejorango

Personal Statement	Combining technical and creative skills in the advancing computing age is where I am. I would love to use my skills as a solution to expand and collaborate with others in addressing both the design and technical aspect of a project. The experiences I will be working on will further develop my personal growth as well as expanding my opportunities wider.
Education	**Asia Pacific College**, Magallanes, Makati City **B.S. in Computer Science specializing in Cyber Security and Forensics** June 2019-present
Work-Related Courses	• Software Development • Software Quality Management • Web Programming • UI/UX Design and Programming • Web Application and Programming Security
Academic Projects	**The Viability of the KNN Algorithm as a Network Anomaly Detection Model** • Thesis 1&2, April 2022 - Present • Project Researcher **SurveiRams: Guard Verification System** • August 2022 – Present • Front End Developer • UX wireframes and mock-ups from the design team were converted into responsive, interactive elements utilizing Quasar Framework. Developed and digitalized a mobile application for the client's current manual processes. Managed and developed within Git and GitHub for version controls. • April – November 2021

	• Front End Developer and UI/UX Designer • Created wireframes aligned to the user requirements for UI/UX and converting said designs for development using Quasar Framework. Strive to balance the application's designs' functionality and aesthetics. **RAMS Violation Management System** • April – June 2022 • UI/UX Designer • Responsible for gathering and evaluating user requirements. Creating designs and graphic user interface around the business requirements, and users' feedback.
Technical Skills	• Highly skilled in MS Office: Word, PowerPoint • Intermediate knowledge and skills in UI/UX Design: Figma; Front-end Frameworks: Vue.js, Quasar • Proficient in Programming Languages: JavaScript, Java, HTML, CSS; Adobe Suite: Photoshop, Illustrator • Basic knowledge in Programming Languages: Python; Adobe Suite: InDesign
Certifications	• Enterprise Design Thinking Practitioner IBM SkillsBuild, April 2021 • Android Development Essential Training: Design a User Interface with Java LinkedIn, October 2020 • UX Design: 1 Overview LinkedIn, September 2020 • UX Design: 2 Analyzing User Data LinkedIn, September 2020 • UX Design: 3 Creating Personas LinkedIn, September 2020 • UX Foundations: Prototyping LinkedIn, September 2020
Awards & Recognitions	• 1st Place, "APC Animation Society Art Competition: Moving Forward", April 2022 • Honor's List, SY 2020-2021, SY 2021-2022 • 1st Place, "APC SoCIT: UI Design Competition", August 2019
Seminars & Trainings Attended	• Valhalla: Visual Development Bootcamp Misha Oplev, June – September 2022
Extra-Curricular Activities	• **Junior Philippine Computer Society – Asia Pacific College Chapter** Director for Marketing and Promotions, January-April 2021 Officer for Marketing and Promotions, July 2019-December 2020 • **APC Animation Society – Asia Pacific College**

	Member, June-August 2019

7.3.4 Mariah Rocita Mirarza

Name:	**MARIAH ROCITA R. MIRARZA**
Complete Address:	3rd Street, Villamor
	Pasay City
Contact Number/s:	854-9073
	(0906) 321-2102
Email Address:	mrmirarza@student.apc.edu.ph mrmirarza@gmail.com
Website:	www.linkedin.com/in/mariahmirarza

Personal Statement	Highly motivated individual with broad knowledge and two years of prior project management, web development, and cyber security cyber security experience, bringing forth a positive attitude and the willingness and motivation to learn new programs.
Education	**Asia Pacific College**, Magallanes, Makati City **B.S Computer Science Major in Cyber Security and Forensics** June 2019-present
Work-Related Courses	• Computer Security • Information Security • Legal Studies (Forensics) • Project Management • Web Penetration Testing and Security
Academic Projects	**The Viability of the KNN Algorithm as a Network Anomaly Detection Model** • Thesis 1&2, April 2022 - Present • Project Researcher • Collaborated with colleagues to evaluate performance and gather research in addition to overseeing testing and evaluation of the algorithm. **SurveiRams: Guard Verification System** • August 2022 - Present • Project Manager, Web Developer

	• Provided leadership and executive project management, defining and delegating roles and responsibilities to ensure successful development of all initiatives. **RAMS Violation Management System** • April – June 2022 • Project Manager • Managed six team members on conceptualizing new business systems initiatives and spearheaded project documentation to ensure it adhere to standards for quality
Technical Skills	• Highly skilled in MS Office • Intermediate knowledge and skills in Web Programming and Cyber Security • Proficient in Linux, Nmap, Java, Python, Windows, VMware • Basic knowledge in Graphic Design
Certifications	• Entreprise Design Thinking Practitioner IBM SkillsBuild, April 2021 • Cybersecurity Fundamentals IBM SkillsBuild, February 2021
Awards & Recognitions	• Honor's List SY 2020-2022
Seminars & Trainings Attended	• SANS Security Awareness Summit & Training 2022 • 2021 TMIE Virtual Cybersecurity Summit for University Students Trend Micro, October 2021
Extra-Curricular Activities	Junior Philippine Computer Society – Asia Pacific College Chapter Committee Member for Membership, September 2018 – June 2019 Director for Membership, June 2019 – January 2021

7.3.5 Shiaramae Faburada

Name:	**Shiaramae T. Faburada**
Complete Address:	14 – A Kabline st. Western Bicutan Taguig City
Contact Number/s:	(0932) 149-0237
Email Address:	stfaburada@student.apc.edu.ph shiarafaburada@gmail.com
Website:	**www.linkedin.com/in/shiaramae-faburada**

Personal Statement	Determined to work in a company or organization with an extensive opportunity that will help me to enhance my knowledge and to utilize my skills, ability, and educational background to work well to my future company.
Education	**Asia Pacific College**, Magallanes, Makati City **BSCS System Software** June 2019-present
Work-Related Courses	• Project Management • UI/UX Designer • Organizer in seminar
Academic Projects	**SurveiRams** • Mobile application, Aug. 2022 • Software Development • Documentation & UI/UX Designer **Ate Rica's Bacsilog website and Franchise order fulfilment** • Website and Mobile application, April 2021 • Website Development • Documentation & UI/UX Designer

Technical Skills	• Intermediate knowledge and skills in Programming Hypertext Markup Language (HTML), Cascading Style Sheet (CSS) • Basic Knowledge in Figma and Canva • Intermediate knowledge in MS Office: Word, PowerPoint, and basic knowledge in excel • Basic knowledge in Photoshop • Basic knowledge in MYSQL & Workbench
Awards & Recognitions	• Honor's List, SY 2019-2022
Seminars & Trainings Attended	• Cyber Security Threat Awareness for Millennials, online (Teams), June 2021 • Filipino CEO Circle, online (Zoom), February 2022 – September 2022

References

[1] "About APC," Asia Pacific College, [Online]. Available: https://www.apc.edu.ph/about-apc/. [Accessed 5 May 2021].

[2] "Facilities," Asia Pacific College, [Online]. Available: https://www.apc.edu.ph/facilities/. [Accessed 5 May 2021].

[3] A. Uzialko, "Workplace Automation is Everywhere, and It's Not Just About Robots," Business News Daily, 26 February 2019. [Online]. Available: https://www.businessnewsdaily.com/9835-automation-tech-workforce.html. [Accessed 6 May 2021].

[4] "Have you always wondered what workflow optimization is all about?," Cflow, [Online]. Available: https://www.cflowapps.com/simple-guide-for-workflow-optimization/. [Accessed 6 May 2021].

[5] K. Elingrud, "The Upside Of Automation: New Jobs, Increased Productivity And Changing Roles For Workers," Forbes, 23 October 2018. [Online]. Available: https://www.forbes.com/sites/kweilinellingrud/2018/10/23/the-upside-of-automation-new-jobs-increased-productivity-and-changing-roles-for-workers/?sh=444567097df0. [Accessed 6 May 2021].

[6] "Paychex Worx "7 Benefits of Going Paperless in Your Business"," 11 November 2015. [Online]. Available: https://www.paychex.com/articles/finance/benefits-of-going-paperless. [Accessed 22 Semptember 2022].

[7] "Citrix "What is a cloud service?"," [Online]. Available: https://www.citrix.com/en-in/solutions/digital-workspace/what-is-a-cloud-service.html. [Accessed 20 September 2022].

[8] R. Hat, "What are cloud services?," 14 March 2022. [Online]. Available: https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-services. [Accessed 20 September 2022].

[9] P. Pedamkar, "Example of Cloud Computing," [Online]. Available: https://www.educba.com/example-of-cloud-computing/. [Accessed 20 September 2022].

[10] "education.vic.gov.au," 20 June 2022. [Online]. Available: https://www2.education.vic.gov.au/pal/reporting-and-managing-school-incidents-including-emergencies/print-all#meaning-of-incident. [Accessed 19 September 2022].

[11] "Incident Reports," 13 March 2022. [Online]. Available: https://www.incidentreport.net/whatisincidentreporting/. [Accessed 19 September 2022].

[12] "Master Electricians Australia," MEA, [Online]. Available: https://masterelectricians.com.au/importance-incident-reporting-investigations. [Accessed 19 September 2022].

[13] "UCI Department of Statistics," [Online]. Available: https://www.stat.uci.edu/what-is-statistics/. [Accessed 20 September 2022].

[14] "Michigan Tech "Why is Statistics Important in Decision-Making?"," 5 April 2021. [Online]. Available: https://onlinedegrees.mtu.edu/news/why-statistics-important-decision-making. [Accessed 20 September 2022].

[15] "SysAid "What is a Ticketing System?"," [Online]. Available: https://www.sysaid.com/resources/what-is-a-ticketing-system#. [Accessed 22 September 2022].

[16] Microsoft: Azure DevOps, "What is Agile development?," 19 August 2022. [Online]. Available: https://learn.microsoft.com/en-us/devops/plan/what-is-agile-development. [Accessed 23 September 2022].

[17] H. G, "Web Server vs. Database Server," Diffzi, 21 January 2019. [Online]. Available: https://diffzi.com/web-server-vs-database-server/. [Accessed 16 June 2021].

[18] back4app, "back4app: What is the Firebase backend?," [Online]. Available: What is the Firebase backend?.

[19] Kinsta, "What Is GitHub? A Beginner’s Introduction to GitHub," 16 September 2022. [Online]. Available: https://kinsta.com/knowledgebase/what-is-github/. [Accessed 23 Septamber 2022].