

MAASTER OF INFORMATION SYSTEMS
Capstone Project



**UNIVERSITY OF THE PHILIPPINES
OPEN UNIVERSITY**

MASTER OF INFORMATION SYSTEMS

SHERYL ANN B. VIZCARA

ACCESS CONTROL MANAGEMENT SYSTEM

Thesis Adviser:

MARI ANJELI L. CRISANTO
Faculty of Information and Communication Studies

02 June 2022

Permission of the classification of this academic work access is subject to the provisions of applicable laws, the provisions of the UP IPR policy and any contractual obligations:

Invention (I)	<input type="checkbox"/> Yes or <input checked="" type="checkbox"/> No
Publication (P)	<input type="checkbox"/> Yes or <input checked="" type="checkbox"/> No
Confidential (C)	<input type="checkbox"/> Yes or <input checked="" type="checkbox"/> No
Free (F)	<input checked="" type="checkbox"/> Yes or <input type="checkbox"/> No

Student's signature: *Sheryl Ann B. Vizcara*

Thesis adviser signature: *Mari Anjeli L. Crisanto*

University Permission Page

ACCESS CONTROL MANAGEMENT SYSTEM

“I hereby grant the University of the Philippines a non-exclusive, worldwide, royalty-free license to reproduce, publish and publicly distribute copies of this Academic Work in whatever form subject to the provisions of applicable laws, the provisions of the UP IPR policy and any contractual obligations, as well as more specific permission marking on the Title Page.”

“I specifically allow the University to:

Specifically, I grant the following rights to the University:

- a. Upload a copy of the work in the theses database of the college/school/institute/department and in any other databases available on the public internet*
- b. Publish the work in the college/school/institute/department journal, both in print and electronic or digital format and online; and*
- c. Give open access to the work, thus allowing “fair use” of the work in accordance with the provision of the Intellectual Property Code of the Philippines (Republic Act No. 8293), especially for teaching, scholarly and research purposes.*


SHERYL ANN B. VIZCARA

Signature over Student Name and Date

Acceptance Page:

This paper prepared by **SHERYL ANN B. VIZCARA** with the title: “**ACCESS CONTROL MANAGEMENT SYSTEM**” is hereby accepted by the Faculty of Information and Communication Studies, U.P. Open University, in partial fulfillment of the requirements for the degree Course.



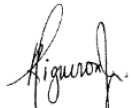
MARLANJELL L. CRISANTO

NAME

Adviser

20 September 2022

(Date)



ROBERTO B. FIGUEROA JR.

NAME

Program Chair

29 September 2022

(Date)



DIEGO SILANG S. MARANAN

Dean

Faculty of Information and Communication Studies

October 21, 2022

(Date)

Biographical Sketch

The author is a graduate of BS Applied Physics, major in Instrumentation Physics in University of the Philippines – Diliman. After her brief stint as a student researcher for two years, she has entered the government sector via the Information and Communications Technology Office of DOST, which is now Department of Information and Communications Technology (DICT). Within the span of six years, the author has been part of the Government Web Hosting Service (GWHS) and the Philippine National Public Key Infrastructure (PNPKI), where she has extensive experience on systems administration, information security, and even project management and capacity building.

The author has taken up Master of Information Systems to expand her skills towards software development, which the author has always wanted to pursue in line with her career path towards becoming a subject-matter expert in information & communications technology.

With that in mind, the author has left government service to grab opportunities and gain experience in dealing with diverse clients in line with software development in the private sector. She currently works as a ServiceNow developer for Emerson Electric Asia, ROHQ.

Acknowledgement

The author would like to thank the Data Center Management Division for giving her the opportunity to work on the project, with special thanks to Carl Francis Ayson, Mario Elmer Cunanan, and Rennald Adolf Ayalde for their valuable inputs, feedback, and support towards the development and completion of the project. She also expresses her gratitude to John Lorenz L. Recto for providing the test digital certificate used for the proof-of-concept and testing of the project.

This project would not be completed and enhanced from the original proposed concept without the feedback, recommendations, and guidance of her adviser, Mari Anjeli L. Crisanto

Dedication

This project is dedicated to:
Jerson F. Pua

TABLE OF CONTENTS

Title Page	i
University Permission Page	ii
Acceptance Page	iii
Biographical Sketch	iv
Acknowledgment	v
Dedication	vi
Table of Contents	vii
List of Figures	ix
List of Tables	x
ABSTRACT	xi
CHAPTER I: THE PROBLEM DOMAIN	1
Statement of the Problem	1
Background and Objectives of the Project	1
Significance and Scope of the Project	2
Documentation of Existence and Seriousness of the Problem	2
CHAPTER II: REVIEW OF EXISTING ALTERNATIVES	3
CHAPTER III: APPROACH TO BE TAKEN IN THIS PROJECT	6
Theoretical Framework	6
Rationale for the Framework	8
Technologies you plan to consider or use	9
CHAPTER IV: CHAPTER PLAN	11
Concept	11
Methods	15
Plan for User Testing and Project Assessment	16
CHAPTER V: RESULTS AND DISCUSSION	19
System testing results	19
Security testing results	20
Usability testing results	22
CHAPTER VI: CONCLUSIONS	27
CHAPTER VII: RECOMMENDATIONS	28

REFERENCES	29
APPENDICES	32
Deliverables and Milestones	32
Budget	32
Qualifications	33
Contributors/Collaborators	34
Resources	34
Complete Program Listing	36
Technical Reference	37
User Manual	42
Software Requirements Specifications	44

List of Figures

Figure 1 Use case diagram	11
Figure 2 Database design. Entity Relationship Diagram.	14
Figure 3 Deployment diagram of the Access Control Management System	15
Figure 4 Summary of respondents per expected role.	22
Figure 5 Visualization of SUS questionnaire scores	25

List of Tables

Table 1 Summary of system testing results	19
Table 2 Summary of initial automated scan results	20
Table 3 Summary of automated scan results after addressing alerts	21
Table 4 Summary of the SUS feedback received from the respondents	23
Table 5 Calculated scales / mean of the SUS questions	24
Table 6 Calculated score contributions of the SUS questions	25

Abstract

Access control management is an essential component of the data center security to ensure that only authorized individuals at allowed visiting times can access data center facilities. Currently, the Data Center Management Division (DCMD) is implementing a paper-based registration process for managing access. With the current process, there are challenges such as maintaining an organized and easily searchable records of the date and time persons have entered the data center. The objective of this project is to streamline the access control registration and management by digitalizing the process of requesting and approving access pass, registering data center visitor information, recording visits, and leasing access cards.

Using the Unified Software Development Process, the web-based Access Control Management System was conceptualized and constructed. In the inception phase, the requirements were gathered through correspondence and interviews with the end-user. In the elaboration phase, the requirements were refined in coordination with the end-user. The use case suite and feature set, along with the project proposal was presented to the end-user. Then, in the construction phase, with iterative implementation, the system was built using PHP and MySQL with the Laravel framework, extending the functionalities with third-party packages and solutions. Lastly, in the transition phase, the system was deployed to a test cloud server.

System functional testing was performed manually using the test case suite. The system was presented to the end-users for their feedback and usability testing. Security testing was also performed using the open-source ZAP software and Qualys SSL Labs. It is concluded that the Access Control Management System is ready for

use of the DCMD, with confidence that the functionalities satisfies the client's requirements, there is a low risk for cybersecurity attacks, and that the users will have a positive experience in using the system.

Keywords: Access Control; Laravel

Chapter I

THE PROBLEM DOMAIN

Statement of the Problem

The Data Center Management Division (DCMD) employs a paper-based process for requesting and granting access to the data center facilities. The visit logs are also currently recorded in paper. In this current setup, there are certain challenges which are common to paper-based processes such as the difficulty in searching for and sorting through records, the risk of losing important records, the higher probability of compromised information, and the physical labor involved in maintaining these paper records.

Background and Objectives of the Project

Access control is an important aspect of information security. In a data center where critical infrastructure and sensitive information are usually situated, both physical and logical access controls must be properly implemented. One of the first steps to enforce access control is to manage who can enter the data center and when. It is also necessary to maintain an updated access list.

To improve their access control system, the DCMD saw the need to digitalize and enhance their access control management, specifically, their access control registration database. The objective of this project is to design and develop a working web-based information system that satisfies the functional requirements of DCMD with respect to the granting and controlling access to the data center. Ultimately, the goal is to streamline the existing registration process and improve the physical security of the data center facilities by having a better control over access management.

Significance and Scope of the Project

The web-based Access Control Registration System shall allow the computerized registration of visitors and company information, recording of visits, and the leasing of access cards. The information system shall also enable DCMD to keep and review the audit trail of the visits to the data center. These features will help DCMD to streamline their access registration process and will make it easier for DCMD to monitor visits to the data center. The privileged access to the information system database will also ensure that any confidential or sensitive information will not be easily accessed by anyone, allowing for better information security. The information system will also cover the computerization of request and approval of data center access that incorporates the use of digital signatures, in consideration of one of the hurdles in going into a paperless system, which is the issue of affixing valid signatures. Outside the scope of this project is the configuration of access card privileges which shall be handled by the Access Control System currently in place.

Documentation of Existence and Seriousness of the Problem

In 2020, DCMD has started implementing a newly installed Access Control System that allows the use of access cards, i.e., RFID cards, to authorize entry and exit in the data center. Currently, only the DCMD personnel and privileged co-locators are assigned with named access cards, i.e., the access card is registered under the name of the personnel/co-locator to whom the access card is leased. For other visitors, DCMD intends to lease unnamed access cards upon entry and have the access card returned by the end of the visit. However, the software for the Access Control System

they are currently using doesn't have a separate database / records for access cards that fits the card leasing scheme they intend to implement. The software is expecting the cards to be already assigned to someone prior to use. The problem with this process is the need to register and deregister the visitor each visit if they intend to implement the per-visit leasing of the access cards. To make the lease and return of cards flexible, the DCMD expects a separate database / audit trail for the access card which lists to whom it was leased and what date and time it was used to access the data center.

Moreover, the software for the Access Control System is still currently off-limits to the guards who are at the front-desk of the data center and who monitor the access to the main door. For the meantime, they are still implementing the paper-based visitor logbook system. This requires the visitor to write in the visitor logbook the following information: date of visit, name, signature, company, id presented, purpose of visit, time in and later on, time out.

Chapter II

REVIEW OF EXISTING ALTERNATIVES

The current and recently installed Access Control System already had the essential features needed for enabling physical and logical security when it comes to access control. A software also comes in package with the Access Control System which can be used to register information about the cardholder, who is then assigned with an access card. As mentioned in the previous section, DCMD intends to lease unnamed access cards upon entry and have the access card returned by the end of the visit. However, DCMD is still formulating their policy on the proper leasing and/or distribution of access cards. For the meantime, they are only distributing named access cards to authorized cardholders, i.e., authorized DCMD personnel, data center guards, and privileged co-locators. Other visitors can enter the data center with the use of the data center guard's access card, that is, once the visitor with approve access pass has already written on the visitors' logbook, the data center guard will open the main door for the visitor. Once the visitor is already inside the mantrap, the DCMD personnel can allow entry to the data center facilities through the data center control/monitoring room when the visitor presses the call button.

It would be possible to implement the desired process, i.e., per visit leasing of access cards, as stated in the user requirements, using the existing software of the Access Control System. This will be done using the Temporary Cards Store feature of the software. The Temporary Cards Store can support up to 500 access cards that can be handed over to guests / temporary cardholders. Upon clicking the 'hand over' button, the Guest dialog box will show up and the system user will be prompted to

enter the guest and visit information. An expiration date can also be entered for the temporary card. Then, when the visit ends or upon return of the access card, the system user can click the 'take back' button. Unlike the regular Cards List though, the guest will not have a visitor's profile. Moreover, the visits are not logged in a way such that you can view the leasing history of the cards.

It is also necessary to mention that since the application used is a prepackaged software and cannot be customized, there are features needed by the client that are not included in the software. The software is built and optimized for configuring and managing the access control itself, e.g., door and access card configuration, and not the registration and recording of visits.

Yet, the proposed information system will not replace the existing software but instead, it will enhance it by providing more features for the access control registration, management, and monitoring. The web information system to be developed shall be designed to work alongside but not integrated with the software for the Access Control System. For this project, the information system data flow shall be consistent with the current manual and paper-based based process as much as possible unless some deviations are necessary for the improvement of the process as per user requirements.

Chapter III

APPROACH TO BE TAKEN IN THIS PROJECT

Theoretical Framework

The Access Control Management System follows the client-server computing model, specifically, web information system. The client-server model is a widely used distributed computing architecture and is suitable for many applications. It is the dominant computing model used by web applications. It has two major components: the client and the server. The client is the user's local system which could be the user's computer or a device used to access the application or data. The server is the 'remote' system which hosts the application and data accessed by the user/s. These two components communicate using a protocol through a network connection, such as the Internet. In the client-server model, the client issues a request to the server, then after processing the request, the server returns a response. This framework is made possible with the use of TCP/IP in the transport and internet layer, and HTTP in the application layer.

Security of the information system is controlled via authentication mechanisms with role-based access control (RBAC), firewall policies / security groups, and Transport Layer Security (TLS) protocols with the use of secure sockets layer (SSL) certificates. RBAC is a method of regulating access to information over a network or in an information system such that users can only access information as required by their role while restricted access to other information. Access per system user is intended to be further controlled with the use of authentication mechanisms, starting with username and passwords. Furthermore, data privacy and information security

between client to server communications over the Internet shall be ensured by employing TLS encryption with the use of TLS/SSL certificates, enabling HTTPS. An X.509v3 digital certificate follows the international industry standard for Public Key Infrastructure (PKI) certificates defined by the International Telecommunications Union. It is used by TLS/SSL certificates for the HTTPS protocol and also by digital signatures accepted by most applications. For the network security controls, the information system shall take advantage of the security group feature of the cloud environment to be used in testing and deployment. A security group acts as a virtual firewall wherein rules can be applied to control inbound and outbound traffic to the virtual server. Alternatively, if the client chooses to deploy the information system within their existing network infrastructure, firewall policies similar to those applied in cloud security groups may be implemented.

In attempt to fully implement a paperless Access Control Management System, the information system is intended to allow the generation and affixing of digital signatures on the Data Center access pass retrievable from the system. Similarly, x.509v3 certificates shall be used for the generating the digital signatures. These digital signatures generated using x.509v3 certificates are expected to be verifiable and accepted by current document readers and signing applications available in the market. Moreover, since the digital signatures assure integrity, authentication, and non-repudiation, they are also recognized as functional equivalents of written signatures as per the existing Philippine laws and issuances on electronic signatures.

Rationale for the Framework

The client-server computing model, specifically, web information system, is planned to be used because the information system is expected to be accessed by more than one system user. It will allow the information to be accessed by several authorized DCMD personnel or registration officers regardless of the operating system of the user's device. The centralized database will also ensure that the registration data is updated and synchronized across the network whenever one system user enters new information or introduces changes.

The web information system is also easier to develop and maintain as compared to other deployment models. The client doesn't have specific user requirements when it comes to the software compatibility with hardware / workstations. Moreover, the existing software for the Access Control System implemented by DCMD is an application program that can only be installed in a computer/server running a Windows operating system. Since the pre-packaged application is not an open-source software that can easily be customized, software integration was not an option. On another note, even though several information systems intended for access control management already exists in the market, there are only specific features that the client has identified in the user requirements. Using a prototype will only add complexity to the project output.

Technologies you plan to consider or use

The web information system is implemented using the following technologies:

1. *Cloud computing.* Cloud computing services, specifically, Infrastructure as a service (IaaS), are used during the development and testing phases, to save cost on hardware requirements.
2. *Linux.* The server is hosted in a Linux-based operating system. Amazon EC2, which comes with the AWS subscription is used for the testing environment.
3. *Apache.* The Apache HTTP Server (httpd) is a free and open-source cross-platform web server. It is widely used and has strong community support. For most operating systems, it is already available in a software bundle along with other essential web application software such as PHP and MySQL.
4. *PHP.* PHP: Hypertext Preprocessor is a widely-known web scripting language that is free and open-source. It makes use of HTML, CSS, and Javascript, among others.
5. *MariaDB/MySQL.* MySQL is an open-source relational database management platform. It is usually used along with Apache and PHP. For this project, only the MySQL Community Edition is used.
6. *Laravel.* This PHP-based web application framework is used to jumpstart the development process. It already has the necessary web application and configuration files organized in an easily understandable directory and file-naming system. It is also easy to extend the functionalities with a variety of packages available to the developer.
7. *Spatie Laravel-permission package.* This package allows the developer to manage user permissions and roles which enables Role Based Access Control (RBAC) functionality.

8. *Laravel Excel package*. This package is utilized in the reports generation feature of the information system. It allows creation and export of CSV and Excel files.

9. *FullCalendar JS*. This Javascript package allows calendar displays in PHP. This is used for the requested calendar feature of the information system.

10. *Laravel DomPDF package*. This package provides a wrapper for DomPDF, which is used to generate PDF files. This package is needed for access requests PDF generation.

11. *SetaPDF FPDF and TCPDF package*. The package allows the import of existing PDF files and affixing of digital signatures that use x.509v3 certificate.

12. *X.509 Digital Certificates*. SSL/TLS certificates shall be used to secure communications between the client browser and web server. The same type of certificate is also used for the affixing of digital signatures in the submitted, endorsed, and/or approved access requests.

Chapter IV

CHAPTER PLAN

Concept

The Access Control Management System is a web information system. The key features will only be accessible to authorized users and specific guests (Immediate Head of the Client who will be sent the Access Request endorsement email). The use cases for the authorized roles are summarized in the use case diagram in Figure 1.

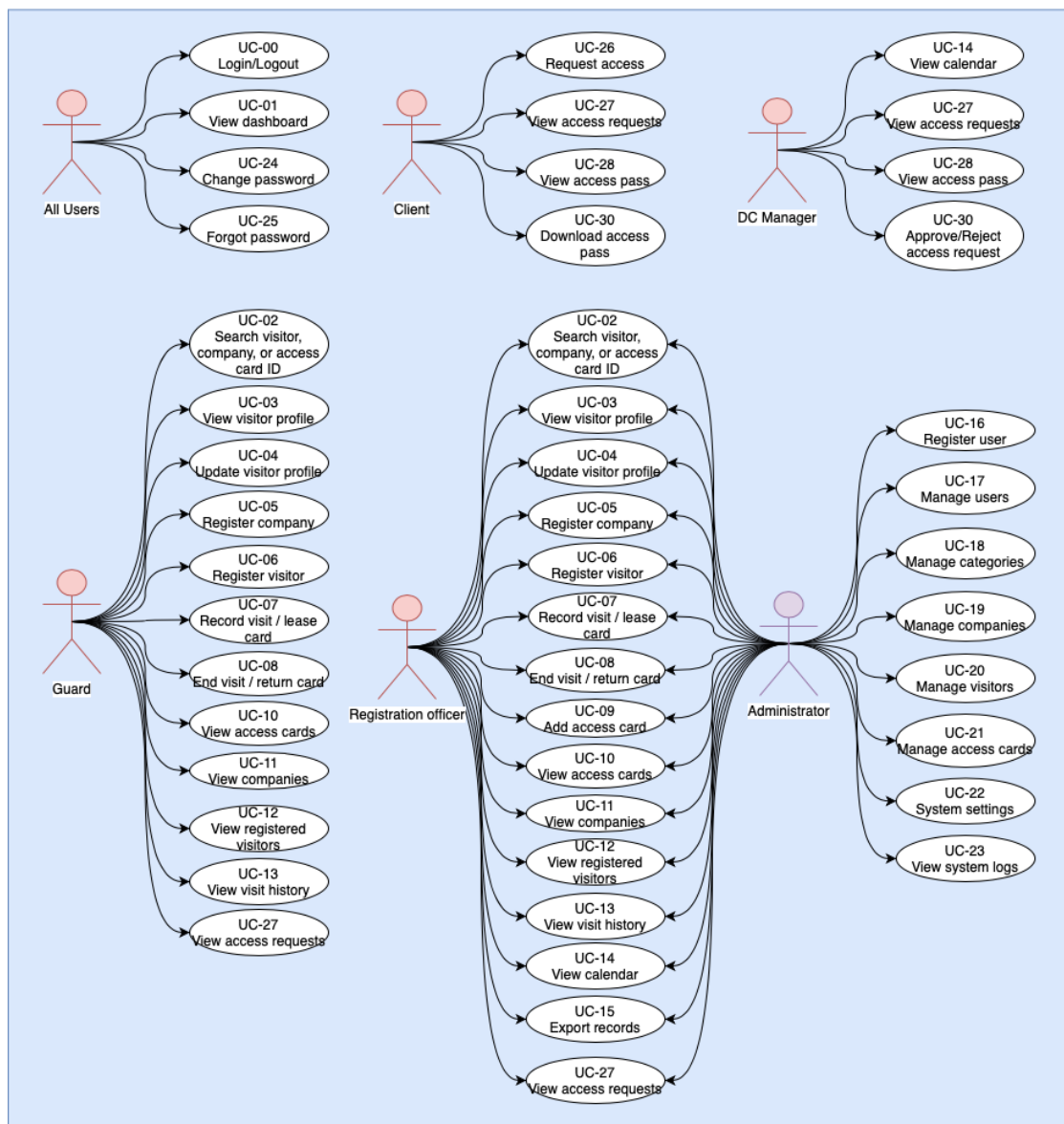


Figure 1. Use case diagram

The Access Control Management System have the following pre-configured user roles:

1. *Administrator*. This user role shall be assigned to the designated system administrator/s.
2. *Registration Officer*. This user role shall be assigned to DCMD staff authorized to access their existing Access Control System and corresponding access cards.
3. *Client*. This user role shall be assigned to co-locators/ authorized representatives of the co-locators.
4. *DC Manager*. This user role shall be assigned to DCMD personnel/officers who can approve access requests.
5. *Guard*. This user role shall be assigned to the security personnel detailed in the Data Center.

All users need to login first before they can access their respective dashboards. The system features available to the user will depend on the assigned role and is limited to the registration of visitors, companies, access cards, & current visits, the leasing & returning of access cards, and accessing reports. The Client can create and submit access requests through the Client dashboard. The DC Manager can approve view & approve access requests via the DC Manager dashboard. The DC Manager can also view the visit history.

The information system have the following key features:

1. *User authentication (login and logout).* The information system data and features should only be accessed by authorized and registered system users. Thus, user authentication through login and logout features are implemented.
2. *User registration and management.* The system users shall be added through the user registration feature. The user registration is only available to the Administrator role. The system also allows the management of user information & access.
3. *Access card registration and management.* Users with role/s Administrator and Registration Officer can register access cards that can be leased to visitors. Moreover, the administrator should be able to manage the access cards list.
4. *Visitor registration.* Users should be to record visitor information into the system for a faster transaction in the available next visit and more importantly, for audit trail purposes.
5. *Company registration.* Users should to be able to record company information, assign a color code, and categorize them.
6. *Access pass request and approval.* Companies via their registered user with Client role should be able to request for data center access pass and the Data Center manager should be able to approve or reject the request.
7. *Visits recording.* Users should be able to record the date and time when the visitor enters and exits the data center.
8. *Leasing of cards.* Users should also be able to record the leasing and returning of access cards upon the recording of visit start and end time.
9. *Calendar.* As per user requirements, the current visits must be viewable through a calendar feature.

10. Reports generation. It must be possible to view and export reports in CSV format.

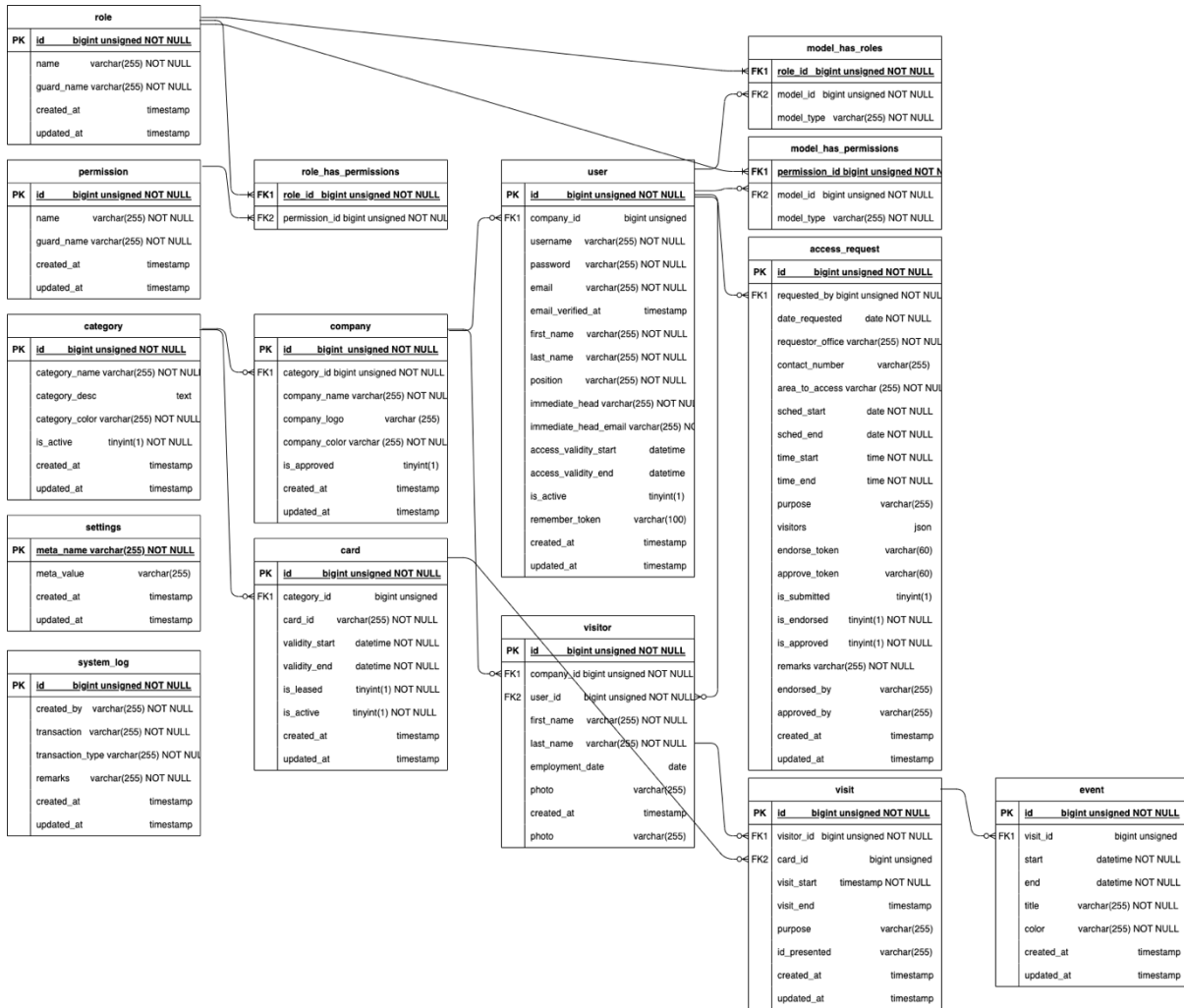


Figure 2. Database design. Entity Relationship Diagram.

The Access Control Management System is accessible via web browsers, and is described by the deployment diagram as shown in Figure 1. During the development and testing phases, the information system is hosted in a cloud VM. It is currently hosted via a LAMP stack running on an open-source Linux operating system. The database is on the same server as the web application. To secure communications between the client and server, server security is hardened by implementing firewall

policies / security groups rules, and HTTPS protocol is implemented using a free, auto-renewed SSL certificate, i.e., Let's Encrypt, installed via certbot. Firewall policies shall be configured to allow only traffic to HTTPS and SSH. The web information system is accessible and renders properly in major browsers, i.e., Chrome, Firefox, Safari and tested to be working even in mobile browsers.

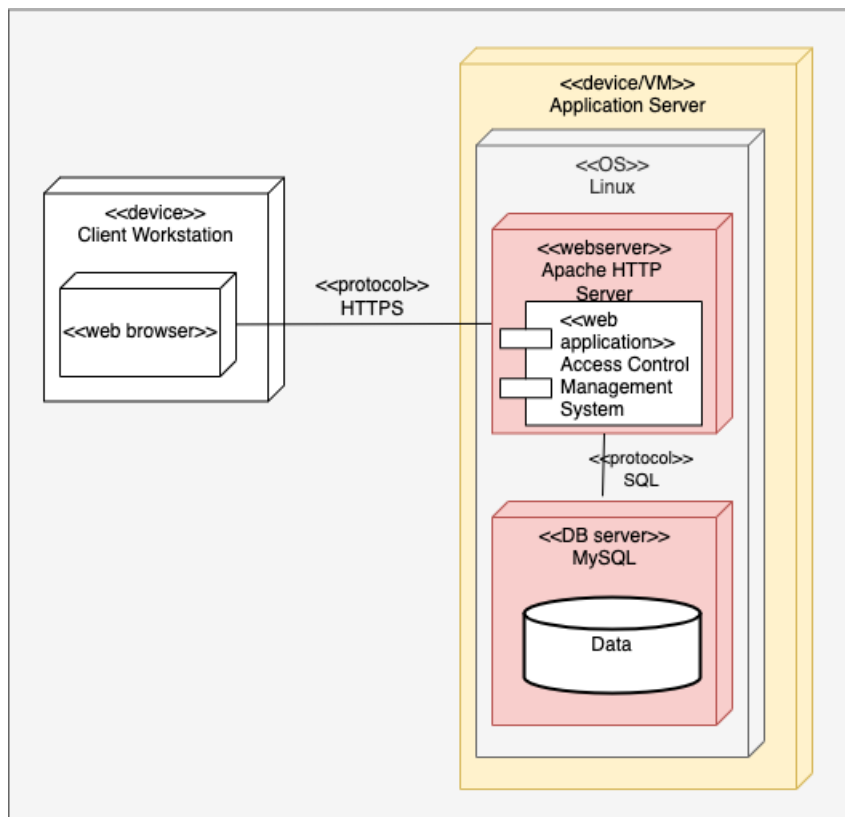


Figure 3. Deployment diagram of the Access Control Management System

Methods

The initial software development life-cycle (SDLC) methodology planned to be followed was the waterfall method, assuming that the user requirements are already clearly defined at the beginning. The initial methodology had been carried out as follows:

1. *Planning* - includes the statement of the problem, identification of solution strategy, setting of timeline, and cost estimation.
2. *Requirements analysis* - outputs shall be narrative descriptions, the Software Requirements Specification (SRS) document, data flow diagrams, and data dictionary.
3. *Software design* - data, architectural, procedural, and interface design. The technology to be used, such as programming language and database platform, shall also be identified.
4. *Software implementation* - coding and deployment.
5. *Software testing* - software testing and optimization. This will involve incorporation of the user feedback to the user interface and functionality.
6. *Documentation* - polishing of SDLC documentation and creation of end-user manuals.

However, the SDLC has been shifted to Unified Process methodology to accommodate for enhancements in the web information system resulting from subsequent communications with the end-user.

Plan for User Testing and Project Assessment

The test plan was prepared to identify objectives of the system testing, system components to be tested, type of testing to be performed, and the resources necessary for the tests to be executed.

Objectives

The system testing should help:

- Determine if the functionality meets the user specifications;

- Ensure that the key features & functions are working as intended;
- Identify errors and bugs for fixing before it is deployed for use;
- Identify security risks and vulnerabilities and provide fix before go-live; and
- Ensure ease-of-use and accessibility of the features.

Scope and Responsibilities

The test cases are available in Appendix C. It focuses on the key features and functions of the Access Control Management System as specified in the user requirements. It was executed manually by the developer prior to security testing. Security testing was performed to check for web vulnerabilities and was also performed by the developer using security tools. Usability testing was done with participation from the client and selected users. The usability criteria used is based on John Brooke's System Usability Scale (SUS) and is provided in Appendix C.

Test Completeness

The system testing is deemed completed once all test cases are executed and all identified errors or bugs are fixed. Proposed improvements that will arise from the system testing and not error-related will not be covered and shall be included instead in future release.

Test Environment and Resources

The test environment used should be a cloud-based hosting facility with the following minimum requirements:

- Runs a Linux-based operating system
- Connected to the internet with public IP

- With network security capabilities, firewall policy setup / security group

Chapter V

RESULTS AND DISCUSSION

System testing results

A functional testing of the system was performed by the developer. The test cases and results are attached in Appendix C. The goal is to test all key features as specified by the client, to verify that these are working as intended, to check for bugs and errors and fix these. With that, the functional testing should have a 100% pass rate. Each test case was performed as indicated in the steps. When minor bugs and errors were identified, these were fixed and the test case was performed again. The test case should be passed before proceeding to the next test case. Eventually, the system functional testing was completed with 100% pass rate.

Table 1. Summary of system testing results

Key feature	Test cases	PASSED	Remarks
User authentication	4	100%	
User registration and management (including role and permission management)	12	100%	fixed validation & restrictions when editing records
Access card registration and management (including category management)	14	100%	
Visitor registration	7	100%	
Company registration	7	100%	
Access pass request and approval	6	100%	fixed error when endorsing access request (& user is not authenticated)
Visits recording / Leasing of cards	2	100%	fixed rendering of dates in visit history
Calendar	1	100%	fixed calendar title formatting

Reports generation	5	100%	fixed DB query for the date range
Other features	3	100%	Tested search & change password feature

Security testing results

Once deployed in the testing server, the system was subjected to security testing using OWASP ZAP 2.11.1. The application checks for common web vulnerabilities present in the system.

In the initial automated scan, OWASP ZAP flagged a total of 69 alerts. These are summarized in the table below. Please see Appendix C for the detailed report.

Table 2. Summary of initial automated scan results

Alert type	Risk	Count
X-Frame-Options Header Not Set	Medium	6
Cookie No HttpOnly Flag	Low	8
Cookie Without Secure Flag	Low	14
Incomplete or No Cache-control Header Set	Low	6
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	9
Timestamp Disclosure - Unix	Low	4
X-Content-Type-Options Header Missing	Low	11
Information Disclosure - Suspicious Comments	Informational	11
Total		69

These were addressed according to risk type. In Laravel, the alerts related to HTTP Header were fixed by updating the Apache configuration files (httpd.conf and httpd-le-ssl.conf) and adding the following lines inside the VirtualHost tags for ports 80 and 443:

Header set X-Frame-Options "SAMEORIGIN"

Header set X-Content-Type-Options "nosniff"

Header Set Cache-Control "no-store, no-cache, must-revalidate, post-check=0, pre-check=0"

For the "X-Powered-By" alert, this was fixed by updating the php.ini file of the server and setting:

```
expose_php = Off
```

For the Cookie Without Secure Flag alert, this was fixed by updating the .env file in Laravel

```
SESSION_SECURE_COOKIE=true
```

The Cookie No HttpOnly Flag was attempted to be fixed by setting SESSION_HTTP_ONLY=true in the .env file. At the same time, the default config of Laravel session.php is "http_only" = true. However, the alert still persists.

Table 3. Summary of automated scan results after addressing alerts

Alert type	Risk	Count	Notes	New Count
X-Frame-Options Header Not Set	Medium	6	Fixed	0
Cookie No HttpOnly Flag	Low	8	Acknowledged	8
Cookie Without Secure Flag	Low	14	Fixed	0
Incomplete or No Cache-control Header Set	Low	6	Fixed	0
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	9	Fixed	0
Timestamp Disclosure - Unix	Low	4	Acknowledged	4
X-Content-Type-Options Header Missing	Low	11	Fixed	0

Information Disclosure - Suspicious Comments	Informational	11	Acknowledged	11
Total		69		23

Out of the 23 remaining alerts, 15 come from the public app.js file that is used by Laravel. Each of the alerts (timestamp and comments) were investigated. It was confirmed that these disclosed information will not pose serious risks to the system. Thus, these are acknowledged for the meantime, while checking for better alternatives in using the javascript files without being flagged by web assessment tools.

Usability testing results

Respondents of the usability testing are composed of users that will be taking the roles of Data Center manager (DC manager), registration officer, guard, and client.

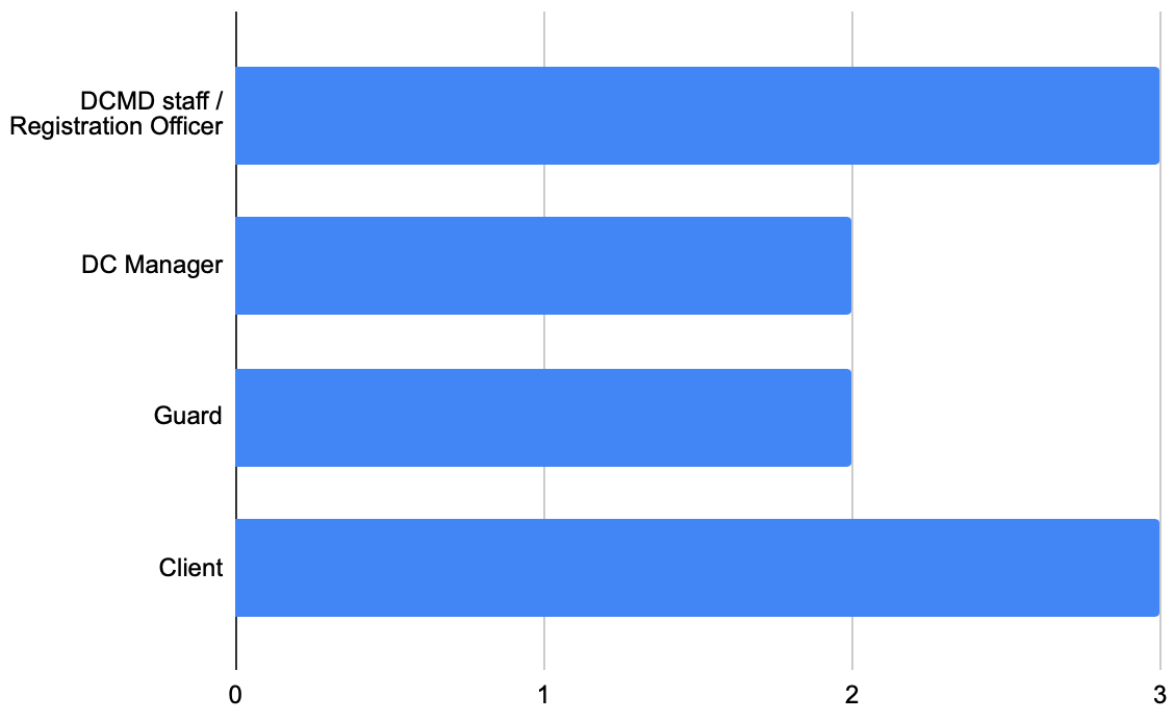


Figure 4. Summary of respondents per expected role.

Below are collective feedback of the users to the ten-item questions. The digits represent the number of users who responded with the same level of agreement.

Table 4. Summary of the SUS feedback received from the respondents

	Strongly Agree (5)	Agree (4)	Neither agree nor disagree (3)	Disagree (2)	Strongly Disagree (1)
(1) I think that I would like to use this system frequently.	2	3	5	0	0
(2) I found the system unnecessarily complex	0	0	0	6	4
(3) I thought the system was easy to use	4	6	0	0	0
(4) I think that I would need the support of a technical person to be able to use this system	0	2	1	7	0
(5) I found the various functions in this system were well integrated	0	9	1	0	0
(6) I thought there was too much inconsistency in this system	0	0	2	7	1
(7) I would imagine that most people would learn to use this system very quickly	1	8	1	0	0
(8) I found the system very cumbersome to use	0	0	0	9	1
(9) I felt very confident using the system	2	5	3	0	0
(10) I needed to learn a lot of things before I could get going with this system	0	2	1	6	1

In order to identify the scale for each question, the mean for each question was calculated. This was done by multiplying the number of respondents for each level with its rating, (i.e. strongly agree = 5 to strong disagree = 1), adding all the numbers for each question, then dividing the sums with the number of respondents (in this case there are 10 respondents).

Table 5. Calculated scales / mean of the SUS questions

	Scale
(1) I think that I would like to use this system frequently.	37 / 10 = 3.7
(2) I found the system unnecessarily complex	16 / 10 = 1.6
(3) I thought the system was easy to use	44 / 10 = 4.4
(4) I think that I would need the support of a technical person to be able to use this system	25 / 10 = 2.5
(5) I found the various functions in this system were well integrated	39 / 10 = 3.9
(6) I thought there was too much inconsistency in this system	21 / 10 = 2.1
(7) I would imagine that most people would learn to use this system very quickly	40 / 10 = 4
(8) I found the system very cumbersome to use	19 / 10 = 1.9
(9) I felt very confident using the system	39 / 10 = 3.9
(10) I needed to learn a lot of things before I could get going with this system	24 / 10 = 2.4

To compute the total score, the score contribution of each question was calculated. Given the scale of each question, an odd numbered question shall have a score contribution of its scale minus 1. Meanwhile the score contribution for even numbered questions is 5 minus its scale position.

Table 6. Calculated score contributions of the SUS questions

	Scale	Score
(1) I think that I would like to use this system frequently.	3.7	2.7
(2) I found the system unnecessarily complex	1.6	3.4
(3) I thought the system was easy to use	4.4	3.4
(4) I think that I would need the support of a technical person to be able to use this system	2.5	2.5
(5) I found the various functions in this system were well integrated	3.9	2.9
(6) I thought there was too much inconsistency in this system	2.1	2.9
(7) I would imagine that most people would learn to use this system very quickly	4	3
(8) I found the system very cumbersome to use	1.9	3.1
(9) I felt very confident using the system	3.9	2.9

(10) I needed to learn a lot of things before I could get going with this system	2.4	2.6
--	-----	-----

Adding up all the scores and multiplying this by 2.5 will give us the System Usability Scale (SUS). For the Access Management System, the SUS is 73.5.

Based on usability.gov, a SUS of 68 is considered above average and below 68 is below average. Thus, it can be said that with an SUS of 73.5, the system is effective and provides ease of use to the users. At the same time, the system has areas for improvement.

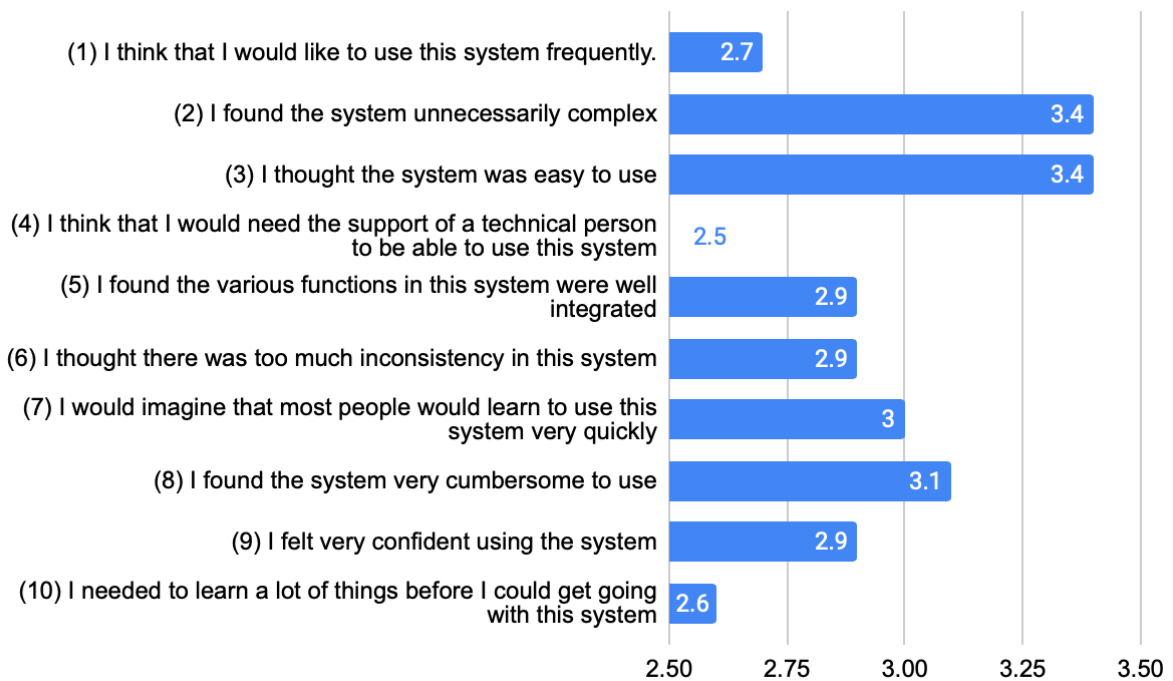


Figure 5. Visualization of SUS questionnaire scores

The individual scores are not recommended to be analyzed on their own to assess the usability of the system, yet, it is possible to gain insight from the results. From the scores, it can be seen that the three lowest scores are obtained from the ff. criteria:

- I think I would like to use this system frequently (Score = 2.7)

- I think that I would need the support of a technical person to be able to use this system (Score = 2.5)
- I needed to learn a lot of things before I could get going with this system (Score = 2.6) Although the users generally disagree that the system is unnecessarily complex (Score=3.4), the users still could have experienced difficulties resulting from the shift from paper-based system to online information systems. It is acknowledged that there should be a period allotted to user trainings and pilot implementation to help the users be familiarized to the features, use and navigation of the system. However, despite this, there is also a possibility that while the policy for the access control management is not yet in place and strictly implemented, the staff & guards may still default to using the paper-based recording / management. Parts of the effort for future works will be recommending enhancements to the system such that the users will have a higher chance of using the system over the use of paper trails.

It is also taken note that the system will only be occasionally used by clients and DC managers as their use of the system is only necessary when they will be submitting access requests / responding to access requests.

Chapter VI

CONCLUSIONS

Based on the project assessment and discussions above, it is concluded that the Access Control Management System is ready for use of the Data Center Management Division, with confidence that the functionalities satisfies the client's requirements, there is a low risk for cybersecurity attacks, and that the users will have a positive experience in using the system.

It is noted, however, that the system has areas for improvement in terms of strengthening the security of the system against future attacks, by reducing information disclosure and in terms of system usability, by ensuring that the users will be encouraged to use the system more often and with increased familiarity. The functionality of the system can also be further extended such as adding alternative authentication mechanisms and providing more flexibility.

Chapter VII

RECOMMENDATIONS

Part of the future work will be the enhancement of the dashboards, especially for the administrator and the DC manager. Charts and overview of the activities should help in monitoring the active visits and activities within the data center.

It has been established in the scope of this work that the integration with the DCMD's existing access control system will not be covered. Thus, once the pilot testing has been proven to be successful, integration to the existing access control system will be sought by exploring the database connection to the system. This will require in-depth security testing to ensure that the Access Control Management System, which is a web-based information system, will not be the gateway for attacks and unauthorized access to the access control system.

The developer will also pursue improvements to authentication and verification mechanisms and refinement of the functionalities. One particular point of interest is the allowing for the digital signing to happen by calling the private key that is stored in the client's keystore; also, to check if it would be possible to affix multiple signatures programmatically. Since this is not one of the primary requirements of the client, this could be a separate branch of research and development from the access control management system and shall focus mainly on the digital signing.

REFERENCES

3 Challenges of Paper Records. (2015).

<https://www.milnertechnologies.com/company/blog/blog/2015/07/07/3-challenges-of-paper-records>

5 Best Practices for Access Control in the Data Center. (2019).

<https://www.vxchnge.com/blog/access-control-in-data-center/>

Buyya, R., Vecchiola C., and Selvi S.T. (2013). *Principles of Parallel and Distributed Computing*. In *Mastering Cloud Computing*, Chapter 2, pp. 29-70.

Data Center Access Control. (2017). <https://www.securityinfowatch.com/access-identity/access-control/article/12335985/data-center-access-control>

Van den Bleeken, N., Hofstede, N. (2014) . *Using the W3C WebCrypto API for Document Signing*. In proceedings of W3C Workshop on Authentication, Hardware Token, and Beyond, 10-11 September 2014.

https://www.w3.org/2012/webcrypto/webcrypto-next-workshop/papers/Using_the_W3C_WebCrypto_API_for_Document_Signing.html

Ferguson, S. and Heibels, R. (2003). *The Internet and the Web. Computers for Librarians (Third Edition)*

Rouse, M. (2018). Role based access control.

<https://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC>

Duncan, R. (2001). Sans Institute. *An Overview of Different Authentication Methods and Protocols*. [https://www.sans.org/reading-](https://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-)

[room/whitepapers/authentication/overview-authentication-methods-protocols-](https://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-)

[118](#)

Chun, M. Sans Institute 2000-2002. As part of GIAC practical repository.

<https://www.giac.org/paper/gsec/594/authentication-mechanisms-best/101431>

Scarfone, K., Hoffman P. (2009). *Guidelines on Firewalls and Firewall Policy*.

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901083

Amazon Web Services, Inc. (2021). *Amazon EC2 security groups for Linux*

instances. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html>

Sphinx Access Control System User Operation Manual. KeyKing International Limited.

What Is User Acceptance Testing (UAT): A Complete Guide. (2020).

<https://www.softwaretestinghelp.com/what-is-user-acceptance-testing-uat/>

OWASP Foundation, Inc. (2021). *OWASP Web Security Testing Guide*.

<https://owasp.org/www-project-web-security-testing-guide/>

System Usability Scale (SUS)

<https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html>

Brooke, John. (1995). SUS: A quick and dirty usability scale. *Usability Eval. Ind.* 189.

Appendices

APPENDIX A

A. Deliverables and Milestones

Deliverable / Milestone	Target Date
Proposal	Jan 20, 2020
Prototype	April 30, 2021
User testing and assessment plans	April 30, 2022
User testing and project assessment results	May 20, 2022

B. Budget

The cost for this project is minimal and will only require a cloud subscription and USB storage media for storing the project output and documentation. The web information system shall be designed to use open-source development software and platforms. Estimated budget is as follows:

Resource needed	Estimated cost
Cloud subscription	2,000
Software development tools and API subscription	10,000
USB storage device	500
Other expenses (printing costs, communication/ transportation expenses, etc.)	1,000
Total	13,500

C. Qualifications

The author has knowledge and experience on developing web information systems using PHP, HTML, and CSS, including the use of available frameworks such as Bootstrap and database management platform, specifically, MySQL. The author has also gained skills and experience on deploying web information systems using cloud services, hardening security of web servers, and utilizing APIs.

As part of the coursework under the MIS program, the author has already developed and deployed at least two information systems, notable in scale of development involved are the Sell Used Books website, an online books buy & sell website, and the PHPdesk, a helpdesk portal.

With this project, the author hopes to hone her skills in project management, communication skills (via coordination with clients and collaborators), system design, system testing, and documentation. The author also expects to gain additional knowledge and experience on the development of web information systems with more complex components.

The author is a graduate of BS Applied Physics program with a major in Instrumentation. For six years, the author has worked as a computer programmer / systems administrator for the government in the field of Information and Communications Technology. She is currently working as a ServiceNow developer in the private sector.

D. Contributors / Collaborators

Participation of the client during the development and testing phases shall be sought through user inputs, e.g., data needed from existing software, clarifications on user requirements, etc., and user feedback.

Contributions from the online community and fellow students are also expected especially for relatively complex components of the information system such as the implementation of the calendar feature.

E. Resources

The development of the Access Control Management System requires the following resources:

1. *Laptop / computer.* This will serve as the workstation of the software team during all phases of the SDLC. The users / testers who will be part of UAT also need access to computers to use features of the system.
2. *Development, Testing, and Deployment Server/s.* For purposes of accessibility and flexibility, the Access Control Management System shall make use of virtual machines (VMs) offered by commercial cloud computing services during the development and testing phases. The free tier offered by cloud services can be taken advantage of. The client has the option to continue using commercial cloud services for the production / deployment of the information system. Alternatively and a more likely scenario, the information shall be hosted privately within the client's network either in an existing physical server or in a private cloud environment.

3. *Network devices (firewall, router, etc.)*. Again, instead of the physical devices, these shall be covered by the cloud computing service during the development and testing phases. More importantly, these are needed during the implementation phase. The client has existing equipment.
4. *External storage*. This will be used for storing a backup copy of the software source codes & patches, documentation, configuration files, and database backups. Prototype (including source code & configuration files) and documentation resulting from the project completion shall be stored in an encrypted USB device.

Following are identified software requirements:

1. *Workstation operating system*. Needed for the workstations of the software team and the end-user devices. Current operating system suffices.
2. *Server operating system*. Needed for deployment of the system. This should be covered by the cloud service subscription. Also, for this solution strategy, the use of open-source operating system is proposed.
3. *Software development tools*. Needed by the software team to develop and deploy the software. Resources are downloadable online and are readily available.
4. *Web server*. Needed to deploy the software, which shall be a web-based application. For this project, an open-source web server application, i.e. Apache, shall be used.
5. *Database platform*. Needed for storing information. For this solution strategy, an open-source database platform, i.e., MySQL, shall be used.
6. *Web browser*. Needed for the implementation of the software. Installers are downloadable online and are free-of-charge.

APPENDIX B

Complete Program Listing

Please see link below for the complete program listing:

https://drive.google.com/drive/folders/1UPetHl8s6_MuAaSEUkN-Ac52YwVg275o?usp=sharing

APPENDIX C

Technical Reference

System Functional Testing

Please click document snapshot below to view whole document:

Release Information

Project:	ACCESS CONTROL MANAGEMENT SYSTEM
Internal Release Number:	1.0.0
Related Documents:	

Test Cases

TC-001: Login successful

Purpose:	Test the Login functionality of the web application for valid login credentials.															
Prereq:	Login Page is accessible Login Page URL															
Test Data:	The test case should be performed once for each <i>combination</i> of values. <table border="1"><thead><tr><th>User type</th><th>E-Mail Address</th><th>Password</th></tr></thead><tbody><tr><td>Administrator</td><td>superadmin@test.com</td><td>123456789</td></tr><tr><td>Registration Officer</td><td>testuser4@test.com</td><td>12345678</td></tr><tr><td>Client</td><td>testuser2@test.com</td><td>12345678</td></tr><tr><td>DC Manager</td><td>testuser6@test.com</td><td>12345678</td></tr></tbody></table>	User type	E-Mail Address	Password	Administrator	superadmin@test.com	123456789	Registration Officer	testuser4@test.com	12345678	Client	testuser2@test.com	12345678	DC Manager	testuser6@test.com	12345678
User type	E-Mail Address	Password														
Administrator	superadmin@test.com	123456789														
Registration Officer	testuser4@test.com	12345678														
Client	testuser2@test.com	12345678														
DC Manager	testuser6@test.com	12345678														
Steps:	<ol style="list-style-type: none">1. visit Login Page2. enter E-Mail Address3. enter Password4. click Login5. see Dashboard6. verify that user can login and directed to the correct dashboard															
Notes and Questions:	PASSED															

Usability Testing

Please click document snapshot below to view whole document:

Release Information

Project:	ACCESS CONTROL MANAGEMENT SYSTEM (ACMS)
Internal Release Number:	1.0.0
Related Documents:	None

Objective

This documentation aims to analyze the readiness or appropriateness of the system, Access Control Management System, for use of the Data Center Management Division staff and clients in managing access requests and leasing of access cards. To be able to do this, feedback was collected from selected users with different roles.

Usability Data Gathering

Methodology

In order to gather feedback on the usability of the system, Access Control Management System, an onsite screening and usability survey was conducted for the staff of Data Center Management Division. Some of the expected users were also requested to answer the questionnaire based on their user experience. There are a total of ten (10) respondents for the usability testing.

The questionnaire is adapted from the system usability scale “quick and dirty” reliability measuring tool developed by John Brooke. It is a ten-item attitude Likert scale to give a subjective assessment of the website’s usability. For each question, user must rate the level of satisfaction with from strongly agree to strongly disagree.


The ten-item attitude Likert scale questions

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

Security Testing Results (Initial Testing)

Please click document snapshot below to view whole document:

ZAP Scanning Report

Generated with  ZAP on Thu 19 May 2022, at 21:09:59

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=Medium, Confidence=Medium \(6\)](#)
 - [Risk=Low, Confidence=Medium \(48\)](#)
 - [Risk=Low, Confidence=Low \(4\)](#)
 - [Risk=Informational, Confidence=Low \(11\)](#)
- [Appendix](#)
 - [Alert types](#)

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- <https://acms-test.nl>
- <http://acms-test.nl>

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Security Testing Results (Re-scan)

Please click document snapshot below to view whole document:

ZAP Scanning Report

Generated with ZAP on Fri 20 May 2022, at 10:53:43

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=Low, Confidence=Medium\(8\)](#)
 - [Risk=Low, Confidence=Low\(4\)](#)
 - [Risk=Informational, Confidence=Low\(11\)](#)
- [Appendix](#)
 - [Alert types](#)

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.


Sites

The following sites were included:

- <https://acms-test.nl>

Security Testing Results (SSL Labs)

Please click document snapshot below to view whole document:

Home Projects Qualys Free Trial Contact


You are here: [Home](#) > [Project](#) > [SSL Server Test](#) > [acms-test.ml](#)

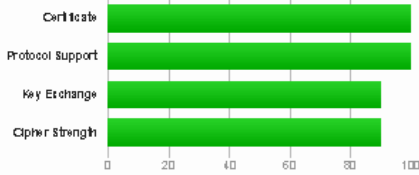
SSL Report: acms-test.ml (52.8.204.193)

Assessed on: [Thu, 19 May 2022 12:57:23 UTC](#) | [Help](#) | [Clear cache](#) [Scan Another >>](#)

Summary

Overall Rating






Category	Score
Certificate	100
Protocol Support	100
Key Exchange	90
Cipher Strength	85

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).


This site works only in browsers with SNI support.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	acms-test.ml Fingerprint (SHA256): 351785d3c7353371c55f3d5e0d95b3d4b96665333e0a077a5475470b175a Pin SHA256: 88MUDy+dlRw5D-Cy6uK9bxDATZEGowLwRR6wLSEU=
Common name(s)	acms-test.ml
Alternative names	acms-test.ml www.acms-test.ml
Serial Number	037da96fd65909e7a0c3a2ae1c57ff9cead3
Valid from	Thu, 19 May 2022 11:54:31 UTC
Valid until	Wed, 17 Aug 2022 11:54:30 UTC (expires in 2 months and 28 days)
Key	RSA 2048 bits @ 65537
Weak key (Debian)	No
Issuer	R3 AIK: hlp:W3J:encr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSF Must Staple	No
Revocation information	OCSF OCSP: hlp:W3J:encr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mobiles: Apple, Android, Java, Windows



Additional Certificates (if supplied)

Certificates provided	3 (4018 bytes)
Chain issues	None
#2	
Subject	R3 Fingerprint (SHA256): 67add1169a022a651b265f96b13cd4c2a563569d796695f72a3d7e737613d1d Pin SHA256: JQJ7bFDqnvD1TK8SumVbF: s00gogr21gT3PufK0G=

Access Control Management ... 41

APPENDIX D

User Manual

Please click snapshot of document in the following page to view the whole document.

Project:	ACCESS CONTROL MANAGEMENT SYSTEM
Internal Release Number:	1.0.0
Related Documents:	

USER MANUAL

Table of Contents

Login/Logout.....	3
How to Login and Logout.....	3
Dashboard	5
Administrator dashboard	5
Registration Officer dashboard.....	5
DC Manager dashboard	6
Guard dashboard	6
Client dashboard	7
Access Requests.....	8
How to submit new access request	8
How to edit saved request.....	9
How to submit saved request.....	10
How to cancel request.....	11
How to endorse access request	11
How to approve access request	13
How to download access request	16
Visits	17
How to record visit / lease access card	17
How to record end visit / return card	18
Visitors	20
How to register new visitor	20
How to edit visitor info.....	21
Companies	22
How to register new company.....	22
How to edit company record	23
Reports.....	24
How to generate report.....	24

APPENDIX E

Software Requirements Specifications

Please click snapshot of document in the following page to view the whole document.

Release Information

Project:	ACCESS CONTROL MANAGEMENT SYS
Internal Release Number:	3.0.0
Related worksheets:	SRS > Use case suite SRS > Feature set

Introduction

This project aims to improve the access control registration of the Data Center Management Division. By digitalizing the access control registration process, the system will allow easier administration and monitoring of access to the data center. Access control is important to regulate who can enter and exit the data center. It should also be taken into consideration when the personnel or visitor can access the data center facilities and which parts of the data center they are authorized to access. Moreover, it must be possible to keep track of the visits in case of incidents or for auditing purposes. All of these will be recorded in the access control management system.

Use Cases

User accounts are categorized based on their functional access. The administrator is responsible for maintaining the Access Control Management System. This type of user can manage registered system users, access cards, companies, and visitors. The administrator can also configure system settings and view system logs for auditing. The administrator can also remove access cards through the access cards management feature.

The registration officer controls mainly the registration of companies and visitors, leasing of access cards, recording visits, and generating reports. Registration officers can create but not delete visitor profiles, company profiles, lease and return access cards. The guard can also register visitors and their respective companies. They can also view access requests and lease cards/record visits.

The client is allowed to request data center access through the information system and also view the access pass and previous access requests.

Lastly, the data center manager can login to the system to approve pending access requests.