UTHM

Universiti Tun Hussein Onn Malaysia

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

COMPUTER RENTAL SYSTEM

CONTENT

1.0 INTRODUCTION

2.0 SYSTEM DESIGN

3.0 IMPLEMENTATION

4.0 CONCLUSION

1.0 INTRODUCTION

1.1 Project Background

The Computer Rental Management System is a comprehensive software solution designed to streamline and optimize the process of renting and managing computer equipment. In today's dynamic business environment, where technology is a critical component of operations, the efficient handling of computer rentals is essential. Computer Rental Management System offers a user-friendly interface that allows businesses to effortlessly track and manage their computer rental inventory, schedule rentals, monitor equipment status, and generate insightful reports. By providing real-time visibility into rental activities, Computer Rental Management System enables organizations to enhance resource utilization, minimize downtime, and ultimately improve operational efficiency. This report explores the key features, benefits, and implementation considerations of the Computer Rental Management System, shedding light on its potential to revolutionize the way businesses handle their computer rental operations.

However, companies must spend money on both legal defense and breach remediation because of multiple instances of security breaches. In order to stop outside attacks, which are covered by the licensing agreement for RM 17,000, the manager intends to install a Network Intrusion Detection System (NIDS). But first, he must persuade the board to approve funding for this option. He believes that simply setting up NIDS, he can stop 95% of the attacks. He examines the breach and observes the pattern for those three years, when the attack happens ten times a year around the holiday season.

ALE = ARO x SLE

ALE = 10 x (17, 000 x 0.95)

ALE = 10 x 16150

ALE = RM 161, 500

1.2 Problem Statement

1.2.1 Less systematic and Operational inefficiency

Sinaro relies on manual, paper-based systems for tasks such as booking, inventory management, and maintenance tracking. This results in delays, errors, and an overall disjointed process that hampers the efficiency of computer rental operations. The lack of an automated system leads to operational inefficiencies throughout the computer rental lifecycle. From reservation to tracking and return processes, the current manual procedures are prone to errors, hindering the timely and accurate execution of tasks.

1.2.2 Ineffective management

Sinaro struggles with effective management of computer inventory and maintenance schedules. Without a centralized system, the organization faces challenges in keeping track of available computer units, leading to overstocking or shortages, and inconsistent maintenance schedules, causing increased downtime.

1.2.3 Suboptimal user experience

Clients and internal staff at Sinaro experience a suboptimal user experience due to the manual nature of current processes. This includes cumbersome reservation procedures, inaccurate tracking of rental status, and delays in the delivery and return of rented computers.

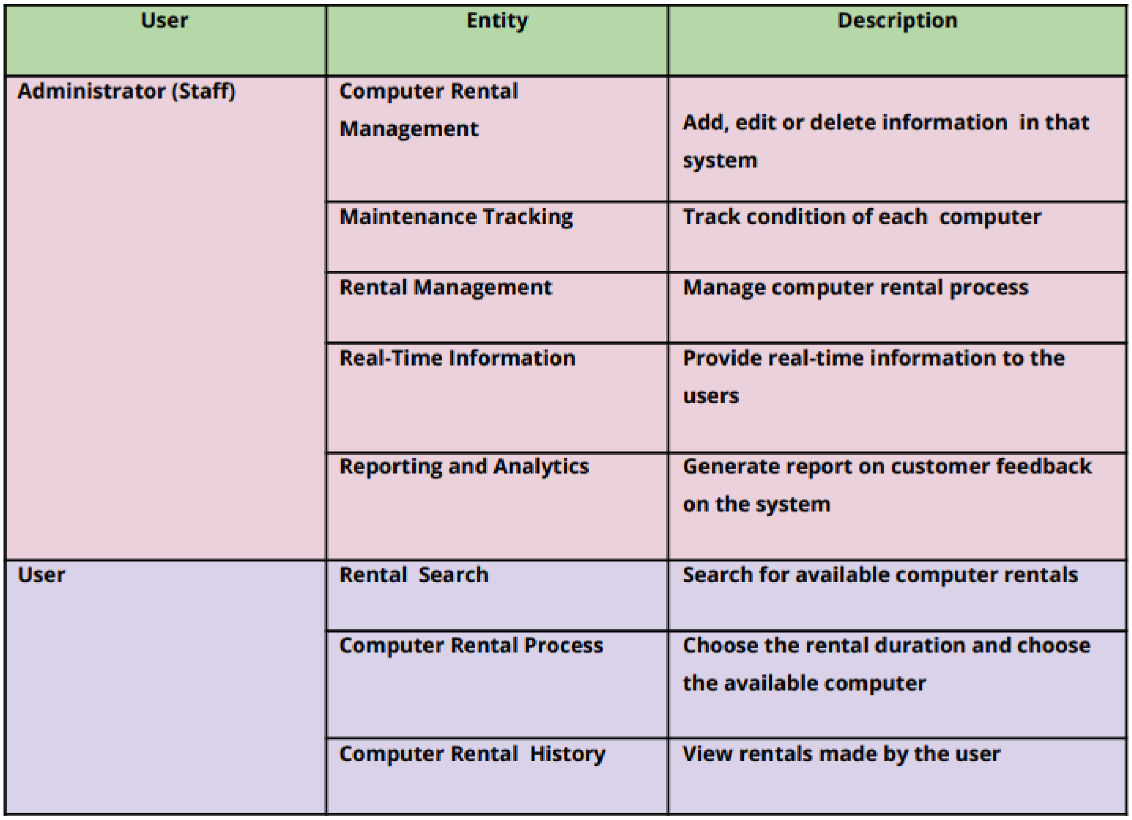
1.3 Project Objectives

i) To design a Computer Rental System for Sinaro with automation for reservation management and maintenance scheduling to reduce manual workload and minimize errors.

ii) To develop a Computer Rental System for Sinaro that prioritizes the security of customer data by implementing encryption.

iii) To test the Computer Rental System for Sinaro until efficient and secure.

1.4 Project Scope

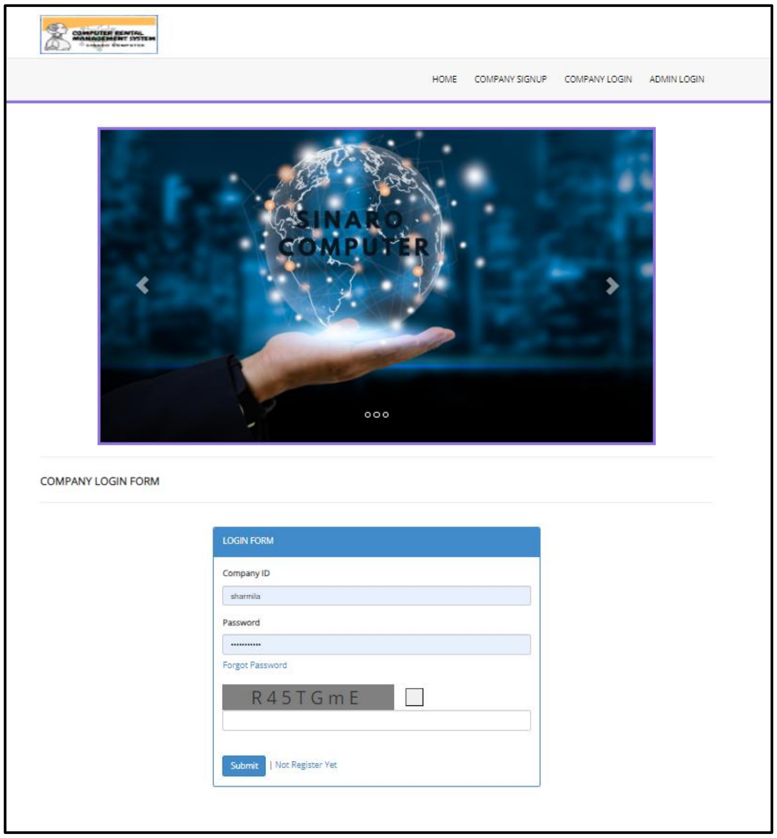


User	Entity	Description
Administrator (Staff)	Computer Rental Management	Add, edit or delete information in that system
	Maintenance Tracking	Track condition of each computer
	Rental Management	Manage computer rental process
	Real-Time Information	Provide real-time information to the users
	Reporting and Analytics	Generate report on customer feedback on the system
User	Rental Search	Search for available computer rentals
	Computer Rental Process	Choose the rental duration and choose the available computer
	Computer Rental History	View rentals made by the user

2.0 SYSTEM DESIGN

2.1 Home Page

There are three sections on the home page. The first is for customers to do registration. The second is Admin's login page. The last is the customer's login page.



COMPANY LOGIN FORM

LOGIN FORM

Company ID: sharmila

Password: •••••••••••

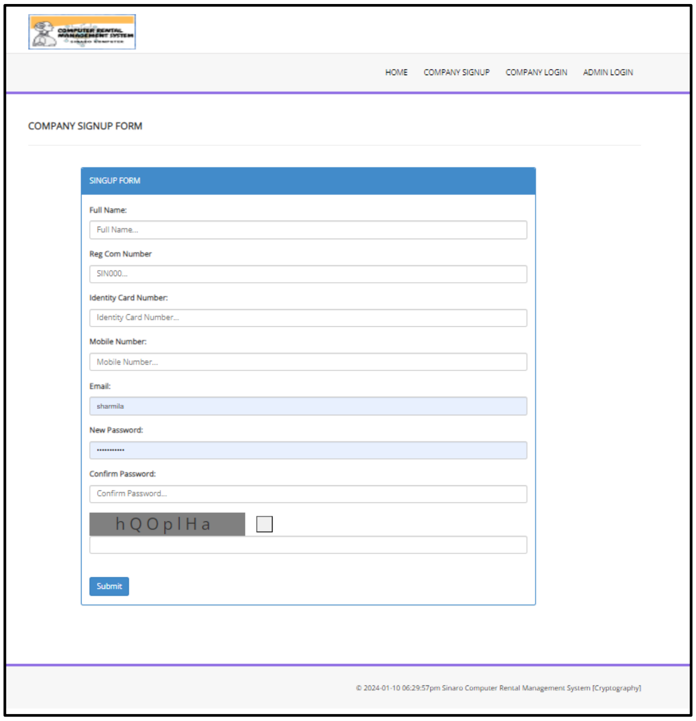
Forgot Password

R45TGmE □

Figure 1:Home Page

2.1.1 Customer's Registration Page

Below picture shows the view of Customers Registration Page. The page contains slide bar and login form. Slide bar shows the picture of other pages. The login form consists username, password and Recaptcha for verification. There's a submit button to save the data. Unregistered customers may click "NOT REGISTER YET" will proceed to customers signup form.



COMPANY SIGNUP FORM

SINGUP FORM

Full Name: Full Name...

Reg Com Number SIN000...

Identity Card Number: Identity Card Number...

Mobile Number: Mobile Number...

Email: sharmila

New Password: ••••••••••••

Confirm Password: Confirm Password...

h Q O p l H a □

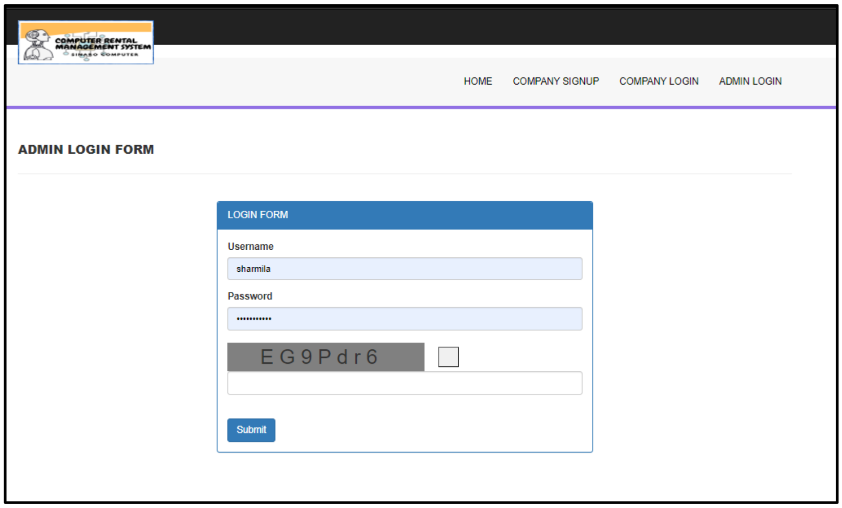
Submit

© 2024-01-10 06:29:57pm Sinaro Computer Rental Management System [Cryptography]

Figure 2: Customer's Registration Page Interface

2.1.2 Admin's Login Page

The picture below indicates Admin's Login Page. In this page, admin able to login using username and password. Recaptcha is provided for verification. A submit button to continue the process.



ADMIN LOGIN FORM

LOGIN FORM

Username sharmila

Password •••••••••••

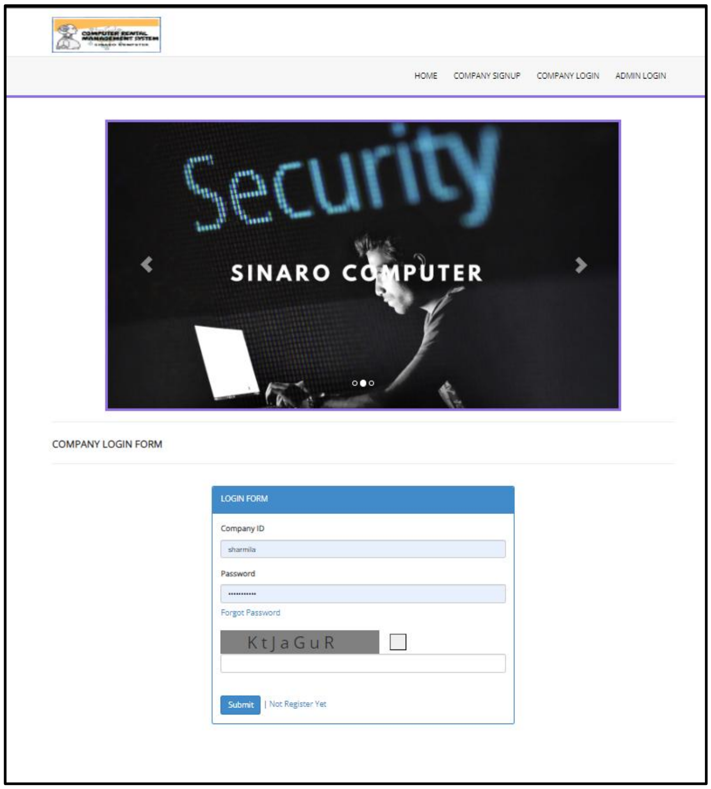
E G 9 P d r 6 □

Submit

Figure 3: Admin's Login Page Interface

2.1.3 Customer's Login Page

Below signifies the customer's signup form. Customer should enter full name, Reg Com Number, id card number, mobile number, and email address. Password and confirm password to identity the customer with security. Recaptcha is needed for the verification and submit button to save the entered data.



COMPANY LOGIN FORM

LOGIN FORM

Company ID

sharmila

Password

•••••••••••

Forgot Password

KtJaGuR □

Submit | Not Register Yet

Figure 4: Customer's Login Page

2.2 Admin Site

2.2.1 Dashboard

The page below expresses the dashboard of an Admin's site. The admin will arrive at their dashboard interface, as is depicted in Figure Admin's Dashboard below, after logging into the system. There are numerous functions available for them to implement their task here.

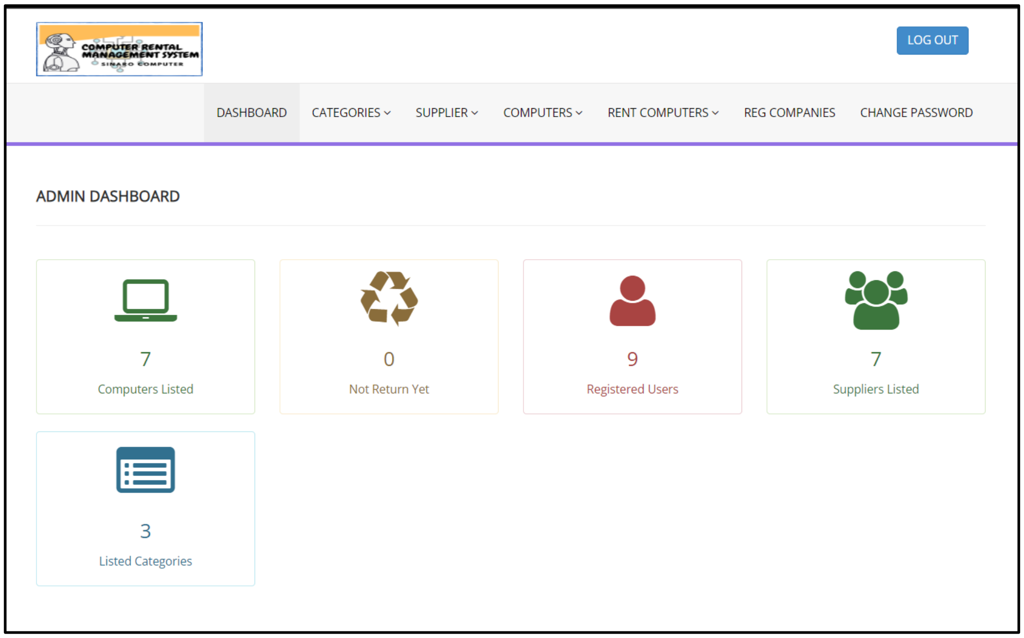
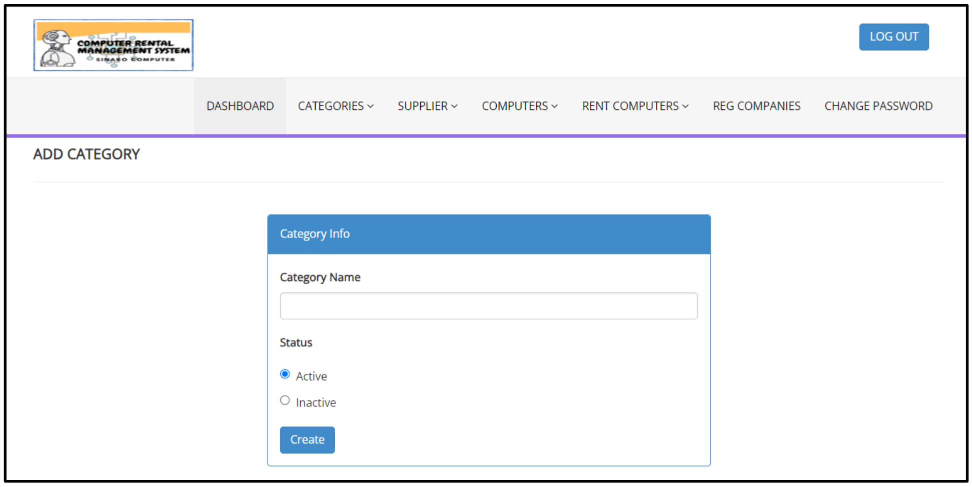


Figure 5: Admin Dashboard

2.2.2 Categories

The page below indicates that admin can manage the categories of the computers . Admin is capable to create, read, update and delete the category of the computers .



ADD CATEGORY

Category Info

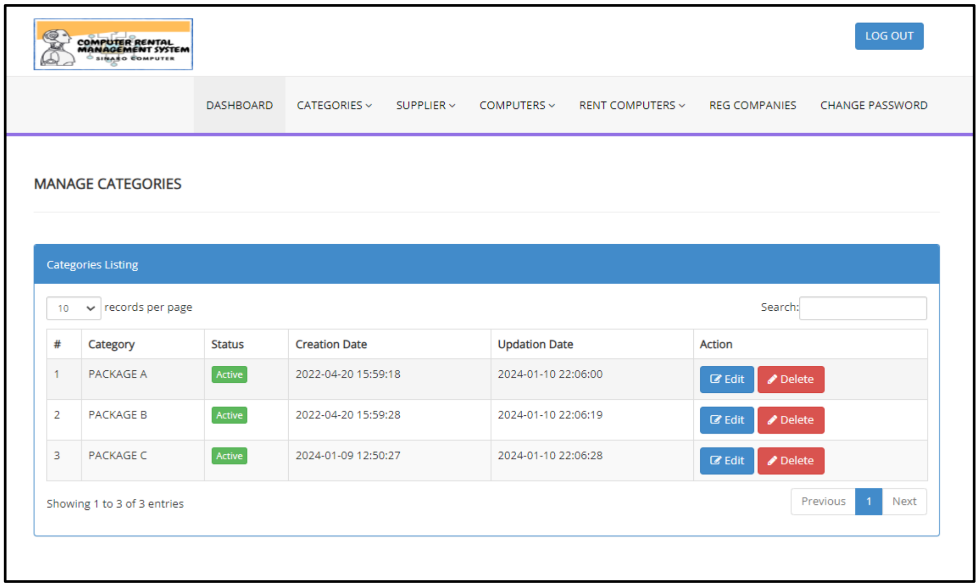
Category Name

Status

● Active

○ Inactive

Figure 6: Add Categories



MANAGE CATEGORIES

Categories Listing

10 records per page

Search:

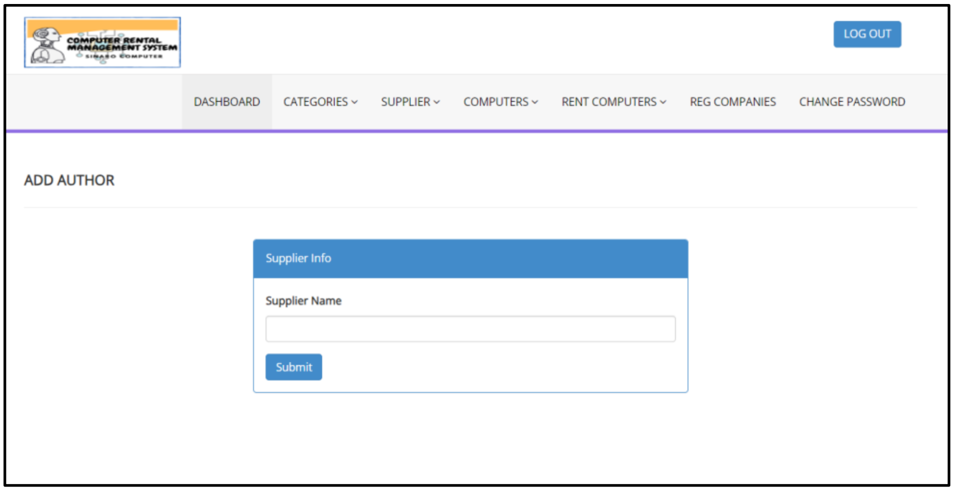
#	Category	Status	Creation Date	Updation Date	Action
1	PACKAGE A	Active	2022-04-20 15:59:18	2024-01-10 22:06:00	Edit Delete
2	PACKAGE B	Active	2022-04-20 15:59:28	2024-01-10 22:06:19	Edit Delete
3	PACKAGE C	Active	2024-01-09 12:50:27	2024-01-10 22:06:28	Edit Delete

Showing 1 to 3 of 3 entries

Figure 7: Manage Categories

2.2.3 Suppliers

This page below shows admin access permission to manage suppliers of the computers. Admins are capable to create, read, update and delete the suppliers of the computers.

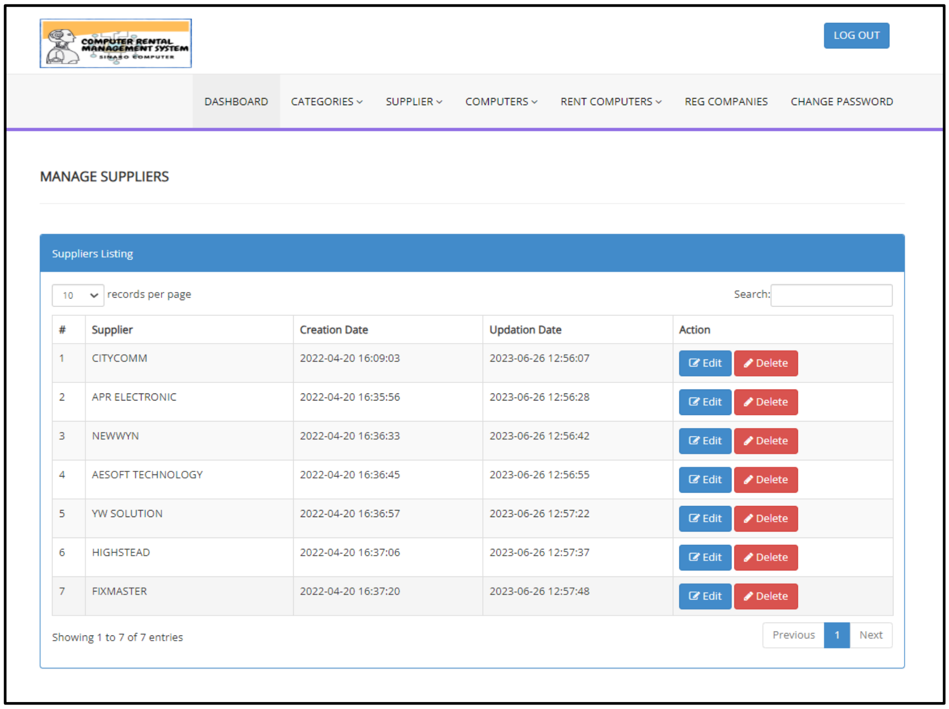


ADD AUTHOR

Supplier Info

Supplier Name

Figure 8: Add Suppliers



MANAGE SUPPLIERS

Suppliers Listing

10 records per page

Search:

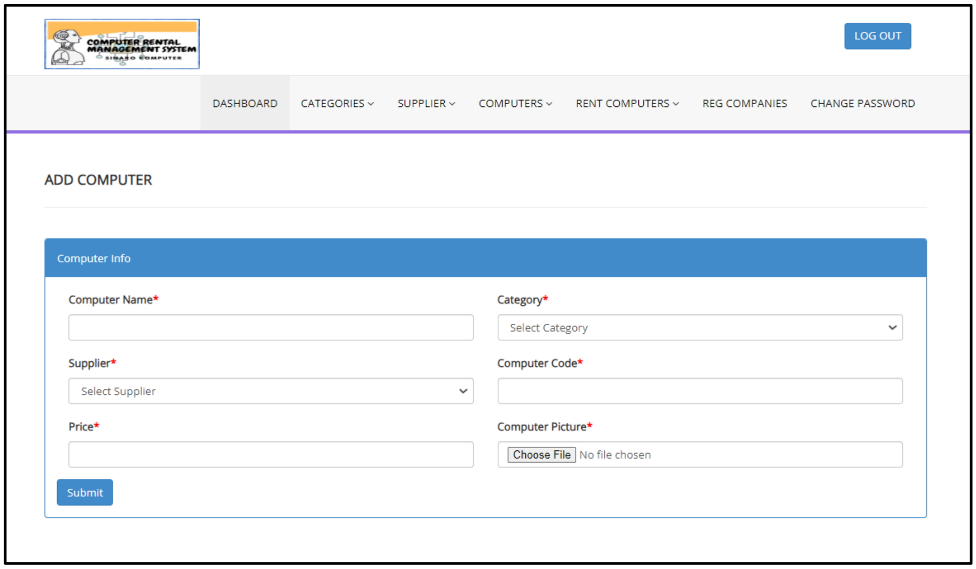
#	Supplier	Creation Date	Updation Date	Action
1	CITYCOMM	2022-04-20 16:09:03	2023-06-26 12:56:07	Edit Delete
2	APR ELECTRONIC	2022-04-20 16:35:56	2023-06-26 12:56:28	Edit Delete
3	NEWWYN	2022-04-20 16:36:33	2023-06-26 12:56:42	Edit Delete
4	AESOFT TECHNOLOGY	2022-04-20 16:36:45	2023-06-26 12:56:55	Edit Delete
5	YW SOLUTION	2022-04-20 16:36:57	2023-06-26 12:57:22	Edit Delete
6	HIGHSTEAD	2022-04-20 16:37:06	2023-06-26 12:57:37	Edit Delete
7	FIXMASTER	2022-04-20 16:37:20	2023-06-26 12:57:48	Edit Delete

Showing 1 to 7 of 7 entries

Figure 9: Manage Suppliers

2.2.4 Computers

This page below shows admins access permission to manage detail of the computers. Admin are capable to create, read, update and delete the details of each computer.



ADD COMPUTER

Computer Info

Computer Name*

Category*
Select Category

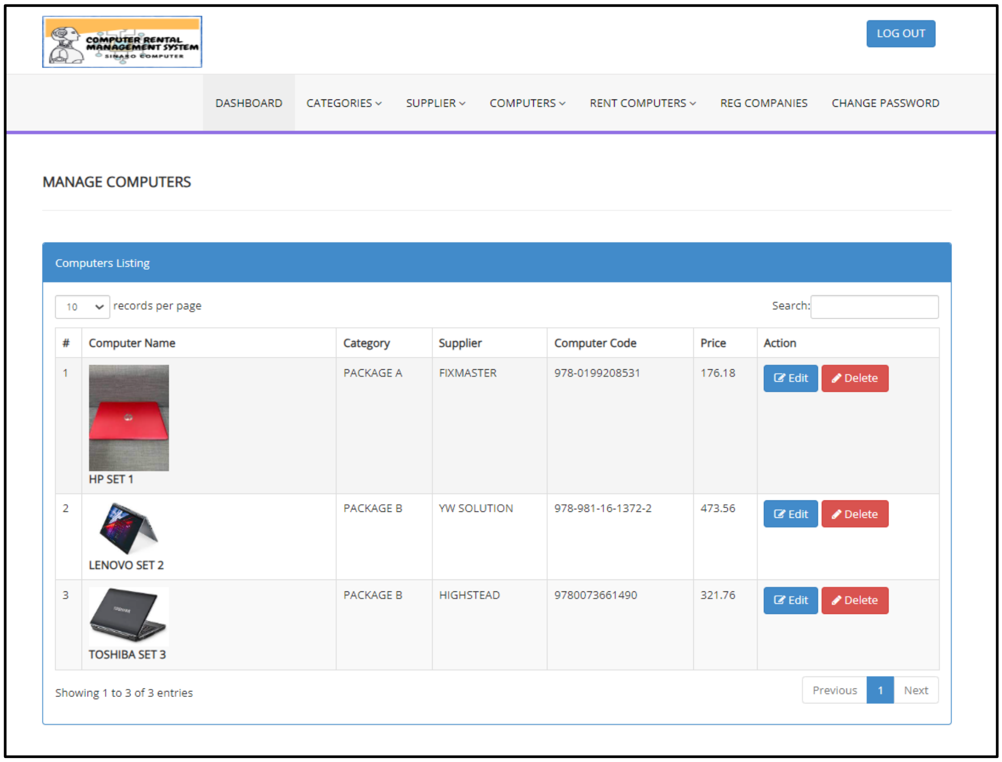
Supplier*
Select Supplier

Computer Code*

Price*

Computer Picture*
Choose File No file chosen

Figure 10: Add Computers



MANAGE COMPUTERS

Computers Listing

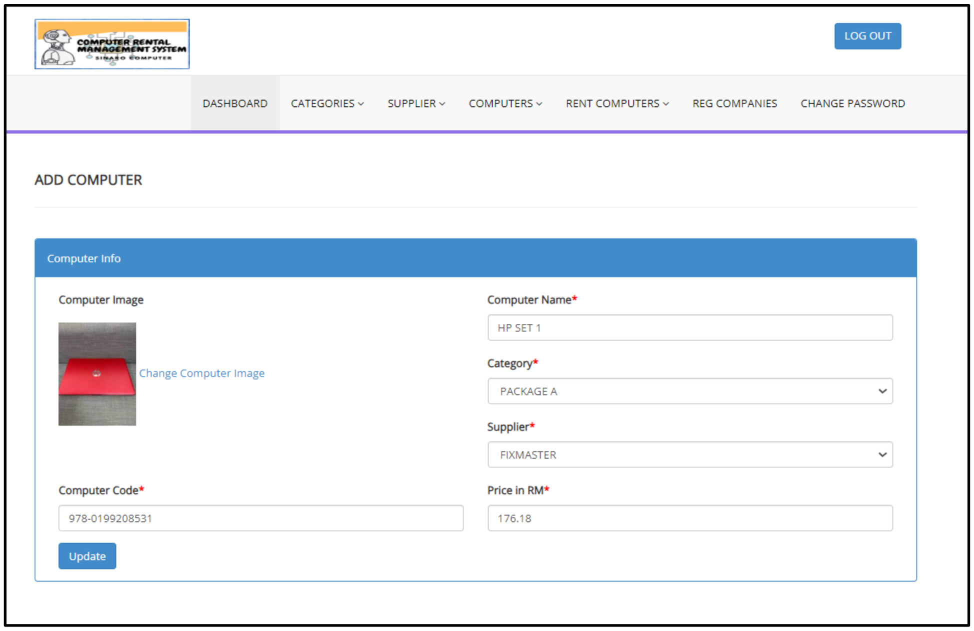
10 records per page

Search:

#	Computer Name	Category	Supplier	Computer Code	Price	Action
1	HP SET 1	PACKAGE A	FIXMASTER	978-0199208531	176.18	Edit Delete
2	LENOVO SET 2	PACKAGE B	YW SOLUTION	978-981-16-1372-2	473.56	Edit Delete
3	TOSHIBA SET 3	PACKAGE B	HIGHSTEAD	9780073661490	321.76	Edit Delete

Showing 1 to 3 of 3 entries

Figure 11: Manage Computers



ADD COMPUTER

Computer Info

Computer Image

Change Computer Image

Computer Name*: HP SET 1

Category*: PACKAGE A

Supplier*: FIXMASTER

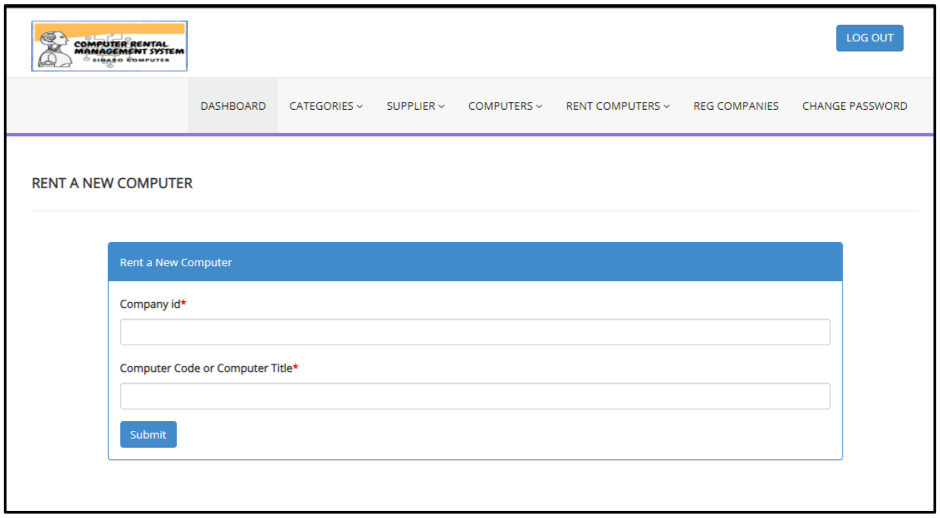
Computer Code*: 978-0199208531

Price in RM*: 176.18

Figure 12: Edit Computers Details

2.2.5 Rent Computers

This page below expresses admin access permission to manage details of rent computers. Admins are able to create, read, update and delete the record of the rent computers. The admin has permission to update the record of returned computers.



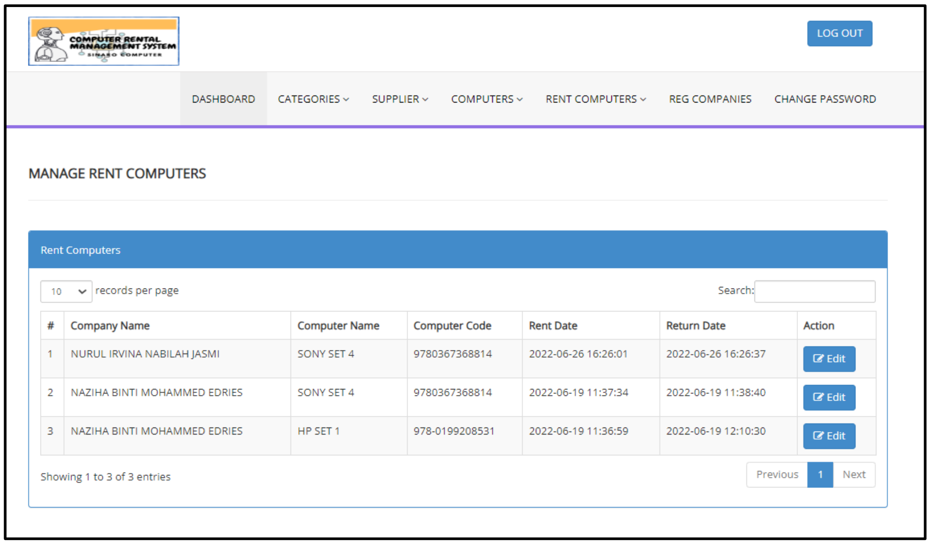
RENT A NEW COMPUTER

Rent a New Computer

Company id*

Computer Code or Computer Title*

Figure 13: Rent Computers



MANAGE RENT COMPUTERS

Rent Computers

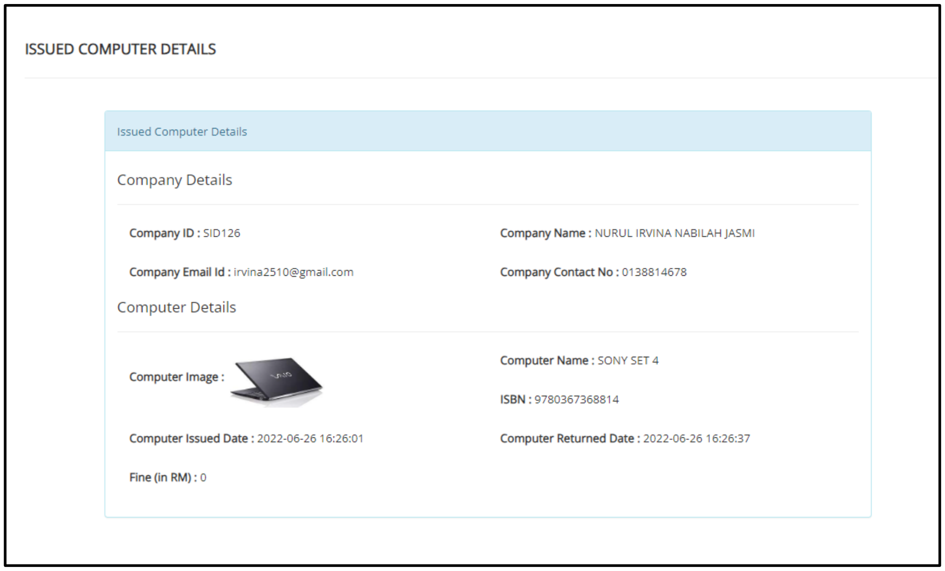
10 records per page

Search:

#	Company Name	Computer Name	Computer Code	Rent Date	Return Date	Action
1	NURUL IRVINA NABILAH JASMI	SONY SET 4	9780367368814	2022-06-26 16:26:01	2022-06-26 16:26:37	Edit
2	NAZIHA BINTI MOHAMMED EDRIES	SONY SET 4	9780367368814	2022-06-19 11:37:34	2022-06-19 11:38:40	Edit
3	NAZIHA BINTI MOHAMMED EDRIES	HP SET 1	978-0199208531	2022-06-19 11:36:59	2022-06-19 12:10:30	Edit

Showing 1 to 3 of 3 entries

Figure 14: Manage Rent Computers



ISSUED COMPUTER DETAILS

Issued Computer Details

Company Details

Company ID : SID126

Company Name : NURUL IRVINA NABILAH JASMI

Company Email Id : irvina2510@gmail.com

Company Contact No : 0138814678

Computer Details

Computer Image :

Computer Name : SONY SET 4

ISBN : 9780367368814

Computer Issued Date : 2022-06-26 16:26:01

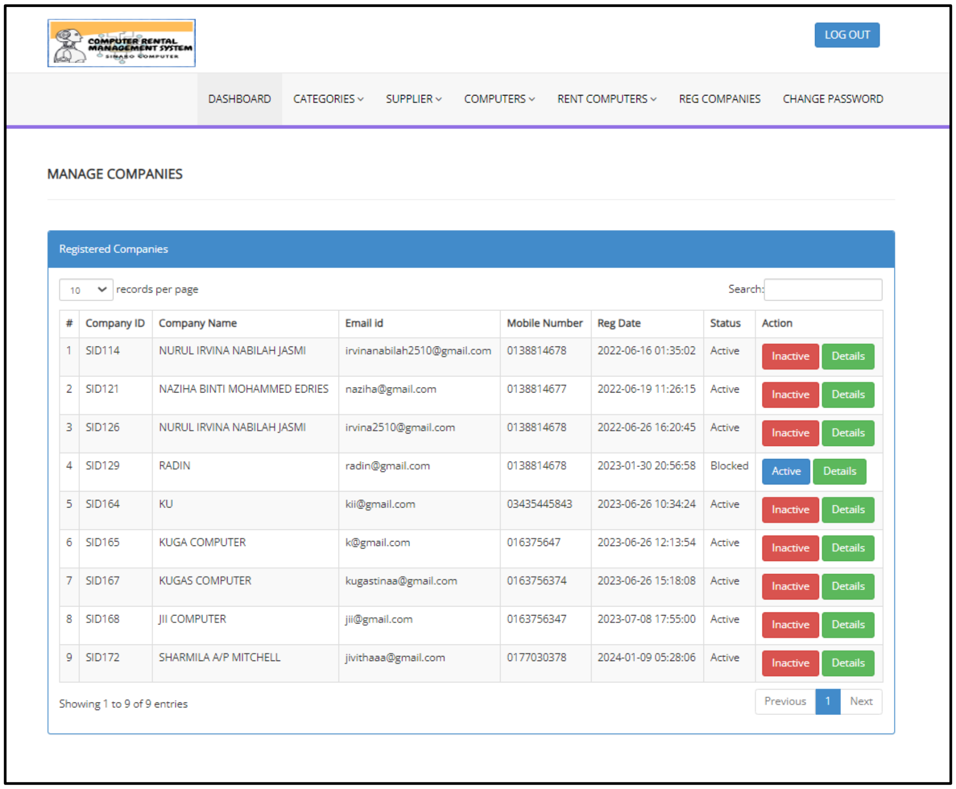
Computer Returned Date : 2022-06-26 16:26:37

Fine (in RM) : 0

Figure 15: Edit Rent Computers

2.2.6 Registered Comapanies / Customer

This page below intimate admins access permission to manage customers who have registered to the system. Admin are capable to create, read, update and delete the registered customers account. Admin can block and unblock customers to access the system. Admin are able to read the customers details and record of rented computers by customers.



MANAGE COMPANIES

Registered Companies

10 records per page

Search:

#	Company ID	Company Name	Email id	Mobile Number	Reg Date	Status	Action
1	SID114	NURUL IRVINA NABILAH JASMI	irvinanabilah2510@gmail.com	0138814678	2022-06-16 01:35:02	Active	Inactive Details
2	SID121	NAZIHA BINTI MOHAMMED EDRIES	naziha@gmail.com	0138814677	2022-06-19 11:26:15	Active	Inactive Details
3	SID126	NURUL IRVINA NABILAH JASMI	irvina2510@gmail.com	0138814678	2022-06-26 16:20:45	Active	Inactive Details
4	SID129	RADIN	radin@gmail.com	0138814678	2023-01-30 20:56:58	Blocked	Active Details
5	SID164	KU	kii@gmail.com	03435445843	2023-06-26 10:34:24	Active	Inactive Details
6	SID165	KUGA COMPUTER	k@gmail.com	016375647	2023-06-26 12:13:54	Active	Inactive Details
7	SID167	KUGAS COMPUTER	kugastinaa@gmail.com	0163756374	2023-06-26 15:18:08	Active	Inactive Details
8	SID168	JII COMPUTER	jii@gmail.com	0163756347	2023-07-08 17:55:00	Active	Inactive Details
9	SID172	SHARMILA A/P MITCHELL	jivithaaa@gmail.com	0177030378	2024-01-09 05:28:06	Active	Inactive Details

Showing 1 to 9 of 9 entries

Previous 1 Next

Figure 16: Registered Company List

2.2.7 Change Password

The picture shows the user change password for admin. The user should enter the current password and then the new password continuously the confirm password to change the password. Before change the password, the user should login to the system. A submit button to save the entered data. A log out button to sign off from the system

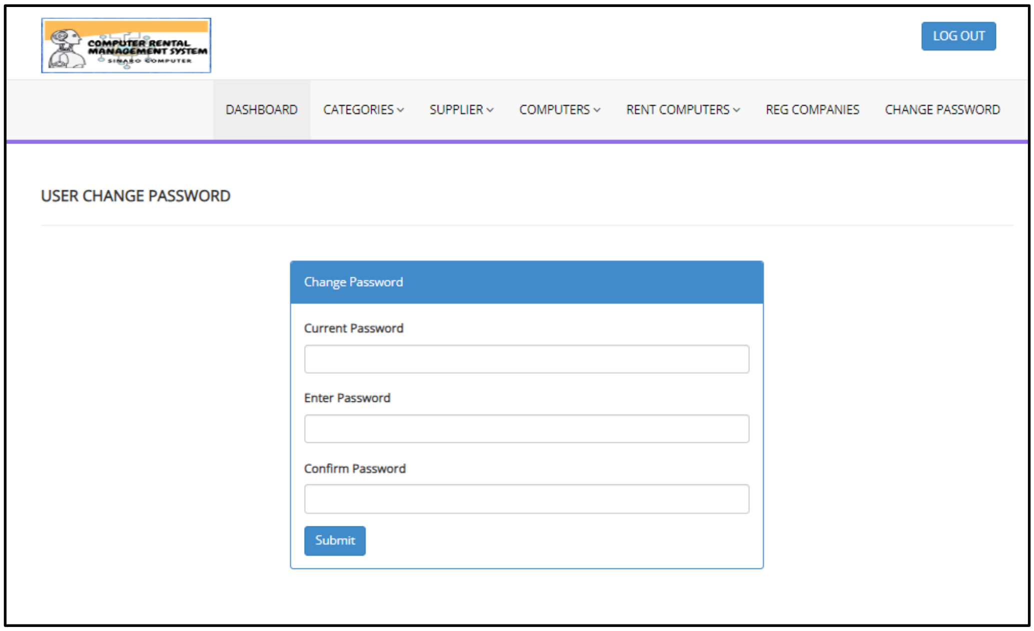


Figure 17: Change Password

2.3 Customer / Company Site

2.3.1 Dashboard

Below page intimate's the customers dashboard which was the home page of Customers Site. The logged in customers are able to view the details of listed computers, unreturned computers and issued computers. A log out button to sign off from the system.

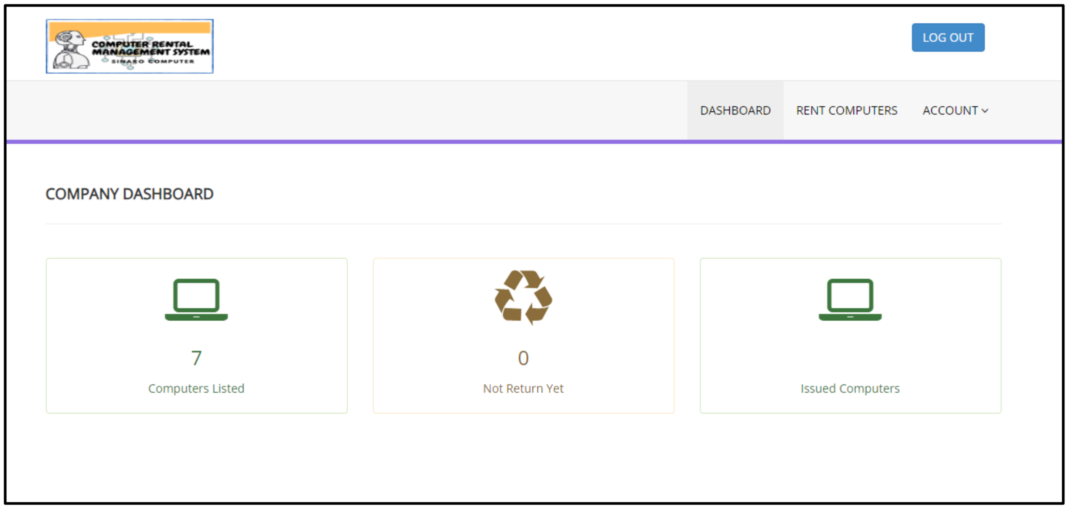
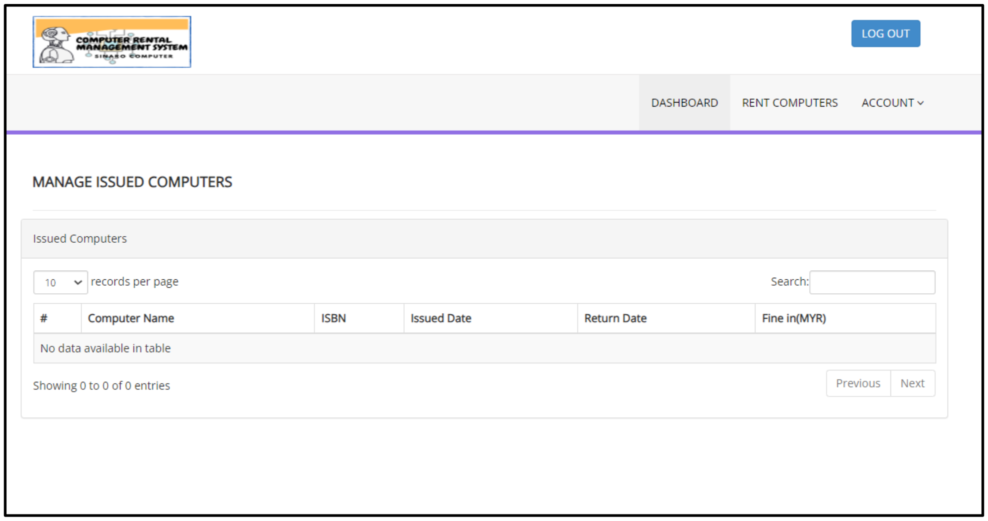


Figure 18: Customer Dashboard

2.3.2 Rent Computer List

The page below shows the rent computers list by customers. The customers are able to view the issued computer details. The previous and next button to view the computer list unless the list of computer is more than 10. A log out button to sign off from the system.



MANAGE ISSUED COMPUTERS

Issued Computers

10 records per page

Search:

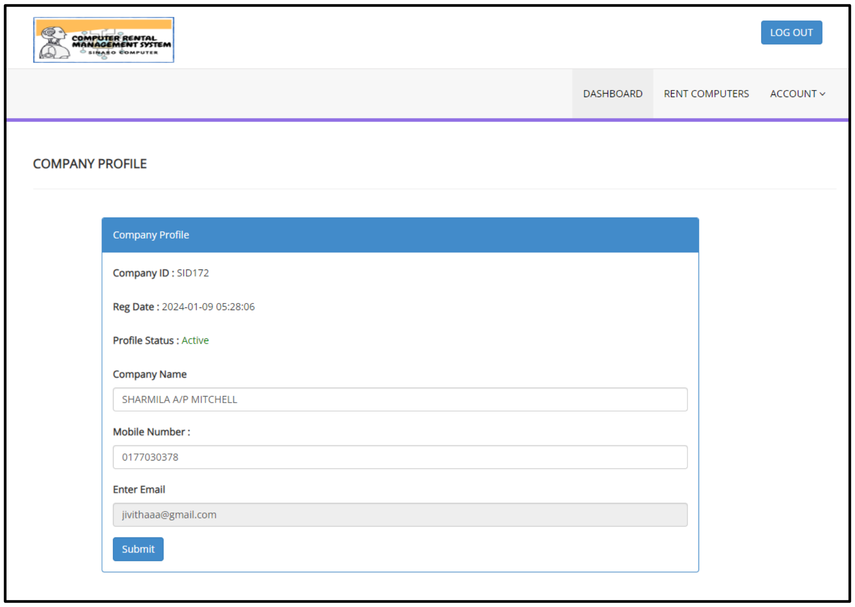
#	Computer Name	ISBN	Issued Date	Return Date	Fine in(MYR)
No data available in table					

Showing 0 to 0 of 0 entries

Figure 19: Customer Rented Computer List

2.3.3 Account Info

The page below shows the customers profile details. The details that are shown are Company ID, Registration Date, and Profile Status whether active or un active. Customer is able to edit the full name, mobile number and email address. A submit button to save the edited data in the system. A log out button to sign off from the system.



COMPANY PROFILE

Company Profile

Company ID : SID172

Reg Date : 2024-01-09 05:28:06

Profile Status : Active

Company Name

SHARMILA A/P MITCHELL

Mobile Number :

0177030378

Enter Email

jivithaaa@gmail.com

Figure 20: Customer Profile Interface

2.3.4 Change Password

The picture shows the user change password for customer. The customer should enter the current password and then the new password continuously the confirm password to change the password. Before change the password, the user should login to the system. A submit button to save the entered data. A log out button to sign off from the system.

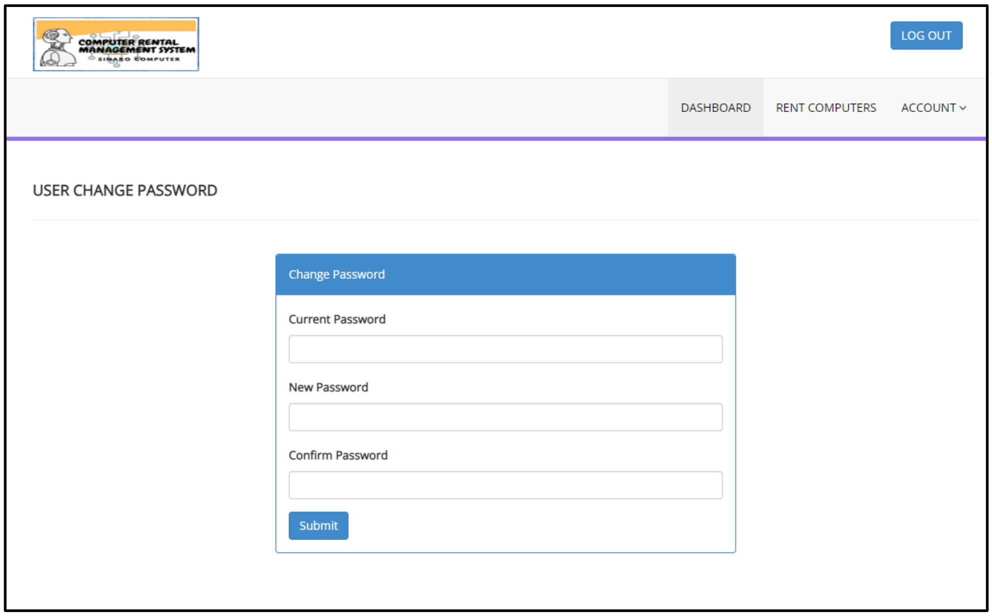


Figure 21: Customer's Change Password Interface

3.0 IMPLEMENTATION

3.1 Introduction

In this chapter, we will discuss the threat modeling for the computer rental system. In the domain of Information Security Project Management, the implementation of security measures for a computer rental system assumes paramount significance. The computer rental system, designed to facilitate the seamless renting of computing resources, inherently involves the management of sensitive data and financial transactions. Ensuring the integrity, confidentiality, and availability of this information demands a meticulous approach to security implementation. The project begins with a thorough risk assessment, identifying potential threats, vulnerabilities, and risks associated with the system. Subsequently, the development and enforcement of robust security policies and procedures become integral to the project's success.

These documents delineate acceptable system usage, access controls, and other critical security protocols. The overarching goal is to establish a secure environment that not only safeguards against cyber threats and unauthorized access but also ensures the trust and confidence of users engaging with the computer rental system. This multifaceted approach to security implementation is fundamental in addressing the unique challenges posed by the intricacies of a computer rental system within the framework of Information Security Project Management. Lastly,, we proposed a solution for our system security and operation which is by analyzing the STRIDE table.

3.2 Threat Modeling and Solution

Threat modeling is a structured approach used in cybersecurity to identify and assess potential threats, vulnerabilities, and risks in a system or application. The goal of threat modeling is to systematically analyze and understand the security posture of a system, enabling organizations to make informed decisions about security measures and prioritize mitigation efforts. There are different methodologies and frameworks for conducting threat modeling, and one commonly used framework is STRIDE table which are Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS) and Elevation of Privilege.

Table 3.1 STRIDE Table

STRIDE Category	Data	What does the attacker do?	Likelihood	Impact	Risk	Mitigation	Solution
Spoofing	User authentication data	Attempts to impersonate a legitimate user or system	Moderate	High	High	Implement strong authentication mechanisms	CAPTCHA, Email OTP, Authentication and Authorization
Tampering	Rental transaction records	Maliciously alters or manipulates rental data	Low	High	Medium	Use encryption for data integrity, implement digital signatures	Password Hashing
Repudiation	System logs	Denies involvement in malicious activities	Low	Moderate	Low	Implement robust logging and auditing mechanisms	Access Control, Session Management, Authentication and Authorization
Information Disclosure	Customer details	Gains unauthorized access to sensitive customer information	Moderate	High	High	Encrypt sensitive data, control access permissions	-
Denial of Service (DoS)	System availability	Disrupts the availability of the computer rental system	Low	High	Medium	Implement DoS detection and mitigation measures	-
Elevation of Privilege	User access rights	Gains unauthorized higher-level access rights	Low	High	Medium	Follow the principle of least privilege, strong authentication	Access Control, Session Management, Authentication and Authorization

3.3 How does the proposed solution protect?

3.3.1 CAPTCHA Security:

Protects Against: Spoofing

How it Protects: CAPTCHA helps prevent automated bots from impersonating legitimate users during authentication processes. It adds an extra layer to ensure that the entity attempting to access the system is a human and not a malicious script or program.

3.3.2 Password Hashing:

Protects Against: Tampering

How it Protects: Password hashing involves converting user passwords into a hashed form using a secure, one-way algorithm. This prevents attackers from directly manipulating or altering the stored passwords in the system. Even if an attacker gains access to the hashed passwords, reversing the process to obtain the original password should be computationally infeasible.

3.3.3 Access Control:

Protects Against: Repudiation, Elevation of Privilege

How it Protects: Access control mechanisms ensure that users have the appropriate permissions to access specific resources or perform certain actions. This helps in tracking user activities and prevents unauthorized users from denying their actions (repudiation) or gaining elevated privileges.

3.3.4 Session Management:

Protects Against: Repudiation, Elevation of Privilege

How it Protects: Effective session management ensures that user sessions are securely established, maintained, and terminated. This helps in tracking user activities and prevents unauthorized access or actions by tying each activity to a specific user session. It also helps mitigate the risk of unauthorized elevation of privileges.

3.3.5 Email OTP Verification:

Protects Against: Spoofing

How it Protects: Email One-Time Password (OTP) verification adds an extra layer of security during the authentication process. It ensures that the user trying to access the system has access to the verified email account, making it more difficult for attackers to impersonate legitimate users.

3.3.6 Authentication and Authorization:

Protects Against: Spoofing, Repudiation, Elevation of Privilege

How it Protects: Proper authentication ensures that users are who they claim to be, mitigating the risk of spoofing. Authorization mechanisms determine the level of access a user has, preventing unauthorized access and reducing the risk of both repudiation and elevation of privilege.

In summary, these proposed solutions collectively contribute to a layered security approach, addressing specific aspects of the STRIDE threats. The combination of CAPTCHA security, password hashing, access control, session management, email OTP verification, and robust authentication and authorization practices helps create a more resilient and secure computer rental system.

3.4 Implementation of the Prototype

The security implementation of a computer rental system is a paramount aspect in ensuring the integrity, confidentiality, and availability of data and services. As computer rental systems involve the management of sensitive user information, renting details, and the overall functionality of the platform, robust security measures become imperative. This introduction encompasses a multifaceted approach to safeguarding the system from potential threats, unauthorized access, and data breaches. Security implementation involves a combination of access controls, encryption, secure payment processing, regular software updates, network

measures, logging and monitoring, security awareness training, physical security considerations, incident response planning, regular security audits, privacy protection measures, and, notably. By adopting these measures, the computer rental system aims to create a secure environment that not only meets regulatory standards but also instills confidence in users, fostering a trustworthy and reliable platform for renting computing resources.

3.4.1 CAPTCHA Security :

Implementing CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is an effective security measure to protect a computer rental system. CAPTCHAs are challenges designed to distinguish between human users and automated bots, preventing malicious activities such as automated form submissions and brute-force attacks. By incorporating CAPTCHA security, especially during user authentication and form submissions, the system ensures that only human users can interact with it. CAPTCHAs commonly involve distorted characters, images, or challenges that are easy for humans to solve but difficult for automated scripts to decipher.

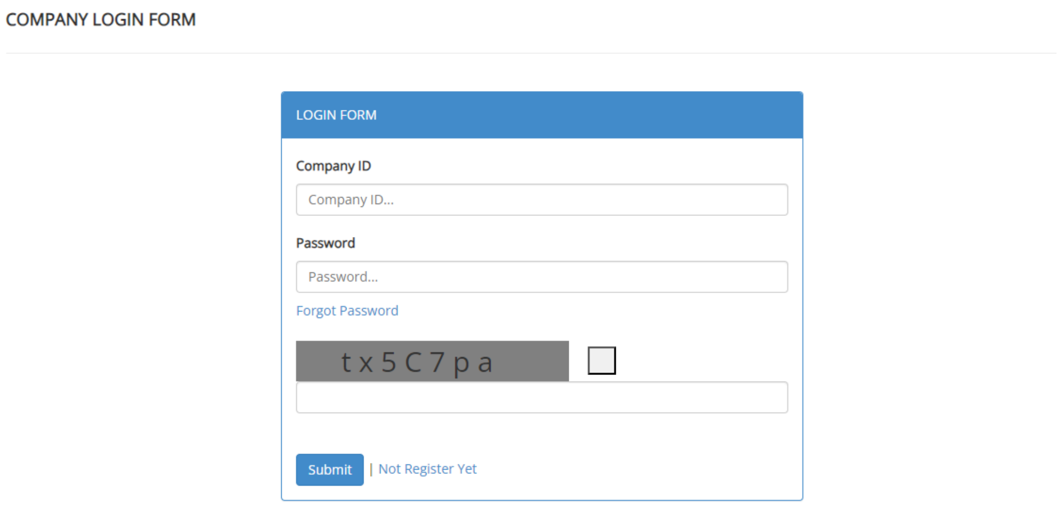
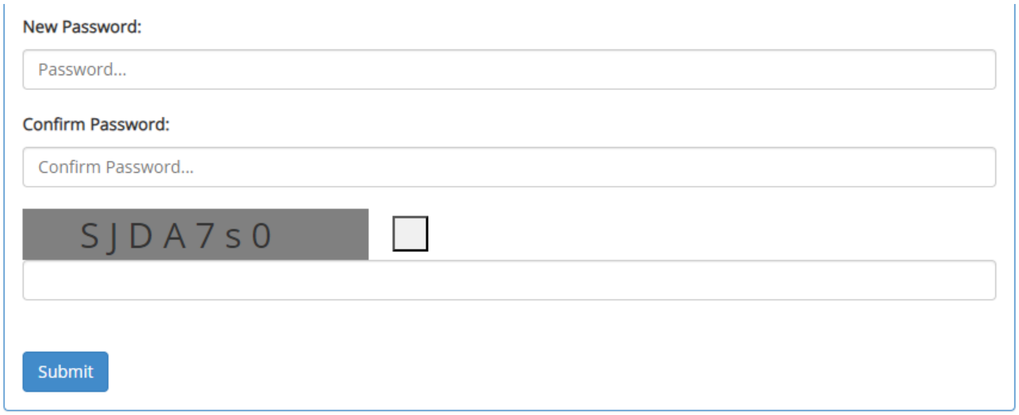


Figure 3.4.1 : CAPTCHA Security

This helps mitigate the risk of unauthorized access, fraudulent activities, and the misuse of the system's resources by automated scripts. Additionally, CAPTCHA implementation contributes to enhancing the overall security posture of the computer rental system by adding an additional layer of protection against various automated threats.

3.4.2 Password Hashing :

Password hashing is a fundamental security measure employed in the implementation of a computer rental system to enhance the protection of user credentials. Instead of storing plaintext passwords in the system's database, a secure one-way hashing algorithm is applied to transform passwords into cryptographic hash values. This irreversible process ensures that even if the database is compromised, the original passwords remain concealed. The system compares the hash of the entered password during login attempts with the stored hashed password, granting access only if there is a match. By using strong and well-established hashing algorithms like bcrypt or Argon2, the computer rental system significantly mitigates the risk of password-related vulnerabilities, such as brute-force attacks or rainbow table attacks. This proactive approach to password security contributes to the overall resilience of the system against unauthorized access and protects user accounts from potential compromise.



New Password:

Password...

Confirm Password:

Confirm Password...

SJDA7s0 □

Figure 3.4.2 : Password Hashing

3.4.3 Access Control:

Implementing robust access controls is pivotal to the security of a computer rental system. By defining and enforcing strict user permissions, only authorized individuals can access sensitive data and system functionalities. Incorporating strong authentication mechanisms, such as multi-factor authentication, adds an additional layer of security to verify user identities and prevent unauthorized access.

3.4.4 Session Management:

Session management plays a pivotal role. It involves creating and handling user sessions securely to prevent unauthorized access and safeguard user data. To achieve this, session identifiers are generated uniquely and securely, transmitted using encrypted communication protocols, and subject to appropriate timeouts. Robust logout mechanisms, protection against session fixation, and measures to mitigate cross-site scripting (XSS) vulnerabilities are implemented. Additionally, secure cookie practices, IP binding, and user-agent verification are employed to enhance session security. These measures collectively mitigate the risk of session hijacking, unauthorized access, and data compromise, contributing to an overall secure user experience within the computer rental system.

3.4.5 Strong password policy :

Enforcing a strong password policy is essential for enhancing the security of the computer rental system. This password must be entered within a specified time limit to complete the action, introducing an additional layer of security. This measure significantly heightens the difficulty for unauthorized users, especially in cases of compromised login credentials. The method proves highly effective in securing sensitive transactions and verifying the legitimacy of users. Users receive immediate email notifications for all account activities, promoting rapid responses to potential security threats. While reinforcing security measures, it is imperative to prioritize user experience and ensure the secure transmission of emails. Additionally, users should be encouraged to create complex passwords with a combination of uppercase and lowercase letters, numbers, and special characters, and to regularly update their passwords to further bolster the system's defenses against potential breaches.

3.4.6 Authentication and Authorization :

In securing the admin functionality for blocking and unblocking users in a computer rental system, it's crucial to implement strong authentication and authorization controls, ensuring that only authenticated administrators with specific roles can perform these actions. Adding a confirmation prompt and two-factor authentication for critical operations adds an extra layer of security, minimizing the risk of accidental or unauthorized changes. Keeping detailed logs, implementing role-based access control, and notifying users of account status changes contribute to a secure environment. Additionally, regular security training for administrators and periodic access reviews help maintain the integrity and confidentiality of the system, reducing the likelihood of unauthorized access or misuse of user management capabilities.

3.5 Summary

Securing a computer rental system involves a multifaceted approach to address its inherent complexities, managing sensitive data and financial transactions. Key security measures include robust access controls, encryption for data protection, secure payment processing, regular software updates, and network security. Logging and monitoring mechanisms help detect and respond to potential threats, while security awareness training ensures a vigilant user base. Physical security considerations and incident response planning are essential, and regular security audits contribute to a resilient security posture. User authentication and authorization mechanisms, such as complex passwords and multi-factor authentication, safeguard against unauthorized access. The proposed STRIDE table facilitates threat modeling, and specific security implementations, like admin user blocking/unblocking controls, require meticulous attention to authentication, audit trails, and access restrictions. Overall, this comprehensive security strategy aims to establish a trustworthy environment, mitigating risks and ensuring the confidentiality, integrity, and availability of the computer rental system.

4.0 CONCLUSION

In conclusion, the decision to outsource our cyber security needs for the computer rental system offers clear benefits in accessing specialized expertise and 24/7 monitoring capabilities to swiftly detect and respond to potential threats. This approach allows us to leverage advanced technology and expertise to fortify our defenses, filling potential gaps in our security systems and bolstering our overall resilience against cyber threats. However, the risks associated with entrusting sensitive data to an external entity necessitate careful consideration. Implementing robust Service Level Agreements (SLAs) and navigating potential limitations in flexibility or contractual discrepancies are critical factors to address. The potential costs of customization to align with outsourced systems also need thorough evaluation. Overall, a comprehensive risk-benefit analysis is imperative to determine whether outsourcing aligns with our goals of enhancing our computer rental system's security while effectively managing risks, costs, and data integrity.