Applied Information Technology And Computer Science Vol. 4 No. 2 (2023) 230-247

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

Secured Recruitment Management System with Data Retention Approach

Mashitah Mohd Tobroni[1], Isredza Rahmi A Hamid[1]*

[1]Fakulti Sains Komputer dan Teknologi Maklumat,
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2023.04.02.014
Received 27 September 2023; Accepted 07 November 2023; Available online 30 November 2023

Abstract: TAMCO Switchgear Sdn. Bhd. is an established electrical company specializing in the production of medium voltage switchgear. The company employs two primary methods for recruiting new employees which are a manual system and a third-party seeking job portal. However, these methods present several challenges. The manual system is burdensome as applicants must email their applications to the Human Resource (HR) department, while the third-party portal poses data security risks. To address these issues, we proposed the development of a secured recruitment management system with data retention capabilities. This system aims to serve as an employment management platform for the HR department. By incorporating automated filtering mechanisms based on position requirements, the HR department can efficiently manage job applications and identify potential candidates. Furthermore, personal data stored in the database will be deleted after six months to comply with data retention guidelines. The project will follow an iterative waterfall development model and implement password hashing, salting, and Two-Factor Authentication (2FA) through One Time Passcodes (OTP) sent via email. This project is crucial for providing a reliable and secure job recruitment platform, reducing the risk of data breaches, and enhancing TAMCO Switchgear's credibility by prioritizing data protection and building trust with potential candidates.

Keywords: Recruitment Management System, Security, Salt, Hashing, Data Retention, Two-Factor Authentication (2FA)

1. Introduction

TAMCO Switchgear Sdn. Bhd. is a leading expert in manufacturing and customization of switchgear using its advanced platform. The company has traditionally relied on conventional methods such as email applications and third-party platforms for their recruitment processes. However, the hiring process is a critical responsibility for recruiting managers and the human resource department. Moreover, solely relying on manual evaluation can lead to costly mistakes and negative impacts on team morale.

*Corresponding author: rahmi@uthm.edu.my

The traditional methods of recruitment also present security flaws and privacy concerns, including the risk of data breaches. It is crucial to continually improve the recruitment process by implementing a Recruitment Management System (RMS) to address these issues. A secure and efficient RMS is essential in today's landscape of increasing cyberattacks and data breaches. The proposed system, Secure Recruitment Management System (SRMS), aims to overcome these challenges and provide a seamless experience for both recruiters and job seekers.

The SRMS will enable recruiters to manage their recruitment processes securely and efficiently. The objective of the project is to design and develop a secured recruitment management system, and test the proposed system based on user requirement and system functionality. The system will include automation features for candidate screening, helping hiring staff identify suitable candidates for interview session based on job requirements. The scope of the project includes candidate information storage and management, interview scheduling, and recruitment process tracking. Additionally, the system will provide job seekers with a user-friendly platform to search for and apply for job openings, while tracking their application status. To enhance security, the system incorporates features such as data retention, password hashing and salting, and two-factor authentication (2FA) through One Time Passcode (OTP) sent via e-mail.

The remainder of this paper is organized as follows. Section 2 discusses related works. Next, Section 3 describes the methodology used (iterative waterfall). After that, Section 4 explains about the results of the tested system. Finally, Section 5 concludes the paper and outline future work for the system.

2. Related Works

This section discusses the concepts of recruitment management system, the encryption algorithm used in the system and comparison between similar and existing systems.

2.1 Recruitment Management System (RMS)

A recruitment management system (RMS) is a software tool that helps organizations manage the process of recruiting and hiring new employees. RMS systems typically include a range of features and functionality to support various aspects of the recruitment process, such as posting job openings, reviewing resumes and applications, scheduling interviews, and tracking the progress of candidates through the hiring process.

2.2 Data Retention

Data retention is the discipline of carefully maintaining and preserving data for a set period. It entails establishing how long data should be kept before being purged, archived, or disposed of properly. The basic goal of data retention is to keep data safe, undamaged, and accessible when required, all while complying to legal, regulatory, and organizational limits. Specific data retention periods and standards may vary depending on the kind of data and the laws and regulations in effect in different locations. Standard that needs to be obliged by Malaysian organization for personal data disposal base on Personal Data Protection Act 2010 in Malaysia is all personal data that has no longer needed in the database need to be dispose and needs to has schedule the disposal for any inactive user in the period of 24 months [1]. There are two types of data retention approaches which are secure database deletion and data archiving.

2.2.1 Secure Database Deletion

Secure database deletion involves permanently and completely erasing data from a database to prevent unauthorized access or recovery. When data is deleted, it is not immediately wiped from the underlying storage. Instead, the links to the data are usually removed, making it unreachable through normal

methods. However, the data itself might still exist in the storage until it is overwritten. Thus, overwriting data is a crucial technique to ensure effective data removal.

In addition to removing the links to the data, overwriting the data plays a vital role in secure database deletion. Overwriting implies replacing existing data with random or meaningless information, making recovering the original material extremely difficult, if not impossible [2]. This procedure involves multiple overwriting runs, using different patterns or algorithms to overwrite the data. The number of passes and specific overwrite patterns used may vary depending on the sensitivity of the data and the level of protection required [3]. By employing this approach, the chances of recovery technologies are significantly reduced, enhancing the secure database deletion process.

2.2.2 Data Archiving

Data archiving involves transferring data that is no longer actively in use to a separate storage device, where it is securely stored for long periods. This archived data often comprises older information that is still important to the organization or must be retained for future reference or compliance with legislation. However, there are some techniques to safeguarding of the data during the archiving process where all the archived data must be encrypted or locked to ensure the confidentiality, integrity, and accessibility of the data [4]. The archival process that is taken place by the third party or it has been outsource needs to ensure that all the process comply with the Data protection and Information Standard regulation.

It is important to consider the potential degradation of data storage medium used for archiving [5]. When electronic storage mediums are chosen, procedures and systems must be put in place to ensure that the information is accessible during the retention term. This involves assuring the lifespan of the information carrier as well as the readability of formats, so that data is not lost owing to future technological improvements.

2.3 Hashing Algorithm

The hashing algorithm is also known as hash function and it is an important factor in helping humans with digital authentication, secure and reliable digital signature. There are many hashing algorithms and the most common one is Message Digest Series 5 (MD5), Security Hash Algorithm Series 1 (SHA-1), and BCrypt. Both MD5 and SHA-1 have been found to be vulnerable to collision attacks. This means that the same hash result can be generated by many inputs [6]. This flaw allows attackers to detect different passwords that result in the same hash, possibly jeopardizing password security.

In this regard, the BCrypt algorithm varies from MD5 and SHA-1. The BCrypt technique is built to withstand collision attacks and includes a unique random salt value for each password. As a result, the chances of BCrypt producing the identical hash output are exceedingly remote [7]. Thus, it is important to use BCrypt as hashing algorithm for password hashing to mitigate vulnerabilities.

2.4 Two-factor Authentication (2FA)

Two-factor authentication (2FA) protects user accounts against unauthorized access [8]. When 2FA is enabled, users must verify themselves using two distinct forms of credentials. This often comprises something they know, such as a password, as well as something they own, such as a mobile phone or hardware token. By combining these two factors, 2FA improves user account security and helps avoid unauthorized account breaches.

It has the same implementation as single-factor authentication but there are some added points in it. When implementing this authentication, the same username and password are used, but additionally, the user is required to get verification from their possession such as mobile device. This can be done by using several methods such as app generated-code, Short Messages Service (SMS), One Time Password (OTP) through email.

2.3 Studies on Equivalent System

This section explores the existing recruitment system that has similar functionalities to the proposed system. Three systems were analyzed, which are TAMCO Switchgear Sdn. Bhd Manual Recruitment System, Job Street Malaysia [9], and Caspio Recruitment Management Software [10].

2.3.1 TAMCO Switchgear Sdn. Bhd Manual Recruitment System

The manual recruitment system has been used at TAMCO Switchgear Sdn. Bhd. since the company's set up. The recruiting process was conducted manually including the job advertisement and interview. All applications and hiring procedures were solely handled through email. This manual approach has proven to be cumbersome for both recruiter and applicants, often prone to human error and oversight in application management. Figure 1 shows an example of a job advertisement uploaded by TAMCO Switchgear Sdn. Bhd. It shows that the applicant needs to apply for GrabJobs to apply for the job. TAMCO Switchgear chose to outsource and use a third-party platform in advertising the open job vacancy. Thus, applicants need to register and submit their details to the third-party website.

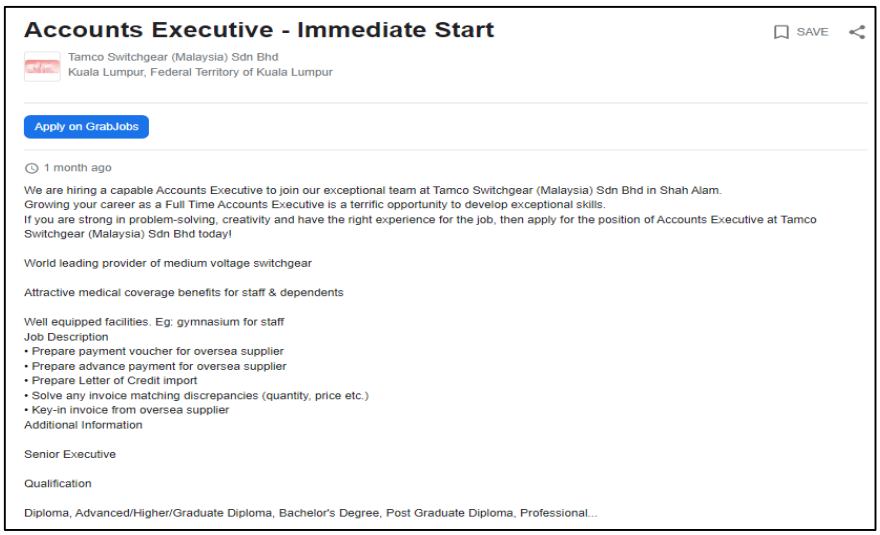

Figure 1: TAMCO job advertisement

2.3.2 Job Street Malaysia

Job Street Malaysia [9] is a prominent online employment company that serves as one of the top Asia employment marketplaces. The platform offers various features such as a job matching engine called LiNa for job seekers and a job posting platform for employers. Job seekers will find job vacancies through the job seeker module, and the employer can post advertisements and manage job applications through the employer module. Job Street Malaysia emphasizes security by implementing an account verification process during registration. It requires the user to insert password and username. The system is developed by using Web Hypertext PreProcessor (PHP) language. However, user do not have control over the data management of their stored data within the Job Street Malaysia database, as it is fully controlled by the platform. Figure 2 shows the homepage interface of JobStreet Malaysia.

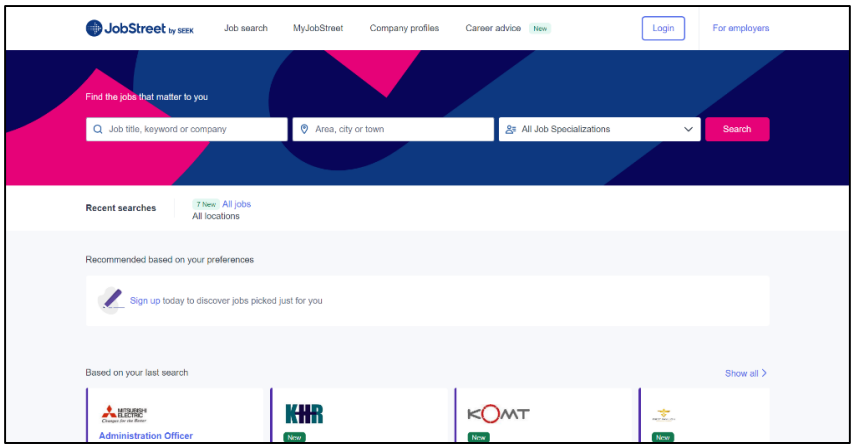

Figure 2: Homepage of JobStreet Malaysia [9]

2.3.2 Caspio Recruitment Management Software

Caspio Recruitment Management Software [10] provides several features including job online posting on a website, creation and updating of job positions, and automated email notifications at each stage of the job interview process. The system offers centralized online database applications where the data will be stored on an online server. However, the system has limited access to the database and lacks encryption for sensitive data. The system is not secure as there is no implementation of two-factor authentication (2FA). Another concern is that the data of disqualified applicants stored in the centralized online database are not deleted after the hiring process is done. Figure 3 shows the interface of Caspio Recruitment Management Software for public viewing.

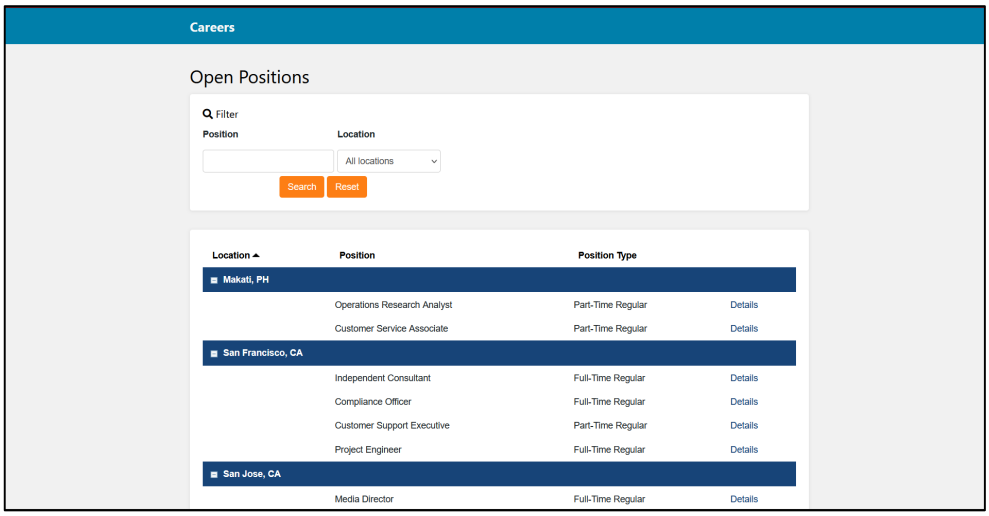

Figure 3: Public view of job advertisement in Caspio Recruitment Management Software [10]

2.4 Comparison between Existing System and Proposed System

Table 1 shows the comparison between the existing system and the proposed system. All systems, except the manual recruitment system, are web-oriented systems and have a database. Job Street Malaysia and Caspio Recruitment Management Software both have certain limitations. While they offer web-oriented platforms and databases, they have some shortcomings in terms of security features. For instance, Job Street Malaysia lacks two-factor authentication (2FA), which is an important security measure to protect user accounts. Caspio Recruitment Management Software also lacks 2FA and has limited access to the database. This limited access may restrict certain functionalities and data management capabilities.

Table 1: Comparison between current system and proposed system

	Manual Recruitment System	Job Street Malaysia	Caspio Recruitment Management Software	Secured Recruitment Management System with Data Retenetion
Web-oriented	No	Yes	Yes	Yes
Database	No	Yes (Limited Access)	Yes (Limited Access)	Yes
Two-factor authentication (2FA)	No	Yes	No	Yes (e-mail OTP)
Password hashing and salting	No	No	No	Yes (BCrypt Algorithm)
Auto-deletion of the personal data after disqualifying from the job offers	No	No	No	Yes
Candidate Screening Automation	No	No	No	Yes

In contrast, the Secure Recruitment Management System with Data Retention addresses these limitations by incorporating 2FA through email-based one-time passcodes (OTPs). It also employs password hashing and salting using the BCrypt algorithm, enhancing the security of user credentials. The proposed system further introduces the auto-deletion of personal data after an applicant is disqualified from job offers, which aligns with privacy regulations and data protection principles. Moreover, the proposed system offers the Candidate Screening Automation feature, which can streamline the screening process by automatically filtering applicants based on job requirements. This automation can significantly save time and effort for recruiters, increasing the overall efficiency of the recruitment process. Overall, the proposed system exhibits advancements and improvements over the existing systems in terms of security, data management, automation, and privacy compliance. It addresses the shortcomings identified in the related work and provides a comprehensive solution for secure and efficient recruitment processes.

3. Methodology

This section provides all the relevant details about the methodology used to develop the project.

3.1 Iterative Waterfall Model

The iterative waterfall model provides practical guidelines in developing software products. It is an improved version of the traditional waterfall model, providing better structural specifications [11]. The model divides the project into distinct phases, with each phase needing to be completed before moving on to the next. Importantly, the iterative waterfall model allows for revisiting previous phases if necessary. Figure 4 illustrates the iterative waterfall development cycle employed in this project, comprising five phases: analysis, design, implementation, testing, and maintenance.

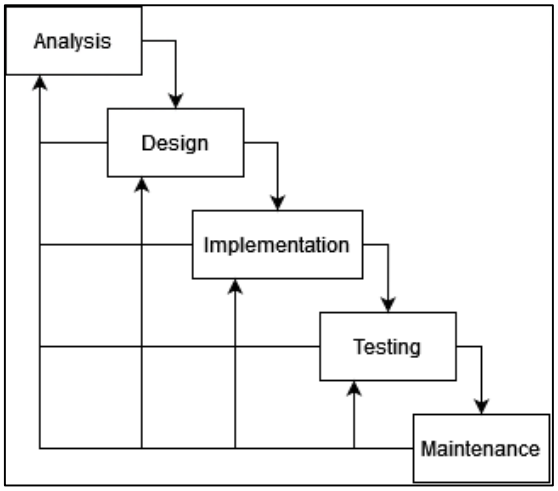

Figure 4: The iterative waterfall development cycle

3.1.1 Analysis Phase

The analysis phase is the initial stage of system development. In this phase, the important requirements for the Secured Recruitment Management System for TAMCO Switchgear Sdn. Bhd. are gathered and analyzed.

The analysis phase identifies the scope, problem statement, and objectives of the system. It identifies the challenges faced by the hiring team in filtering suitable candidates manually and overlooking applications received via email. It also acknowledges the limitations and security concerns of third-party job portals. The system will be developed as an online web-based system with three main users: admin, hiring staff, and applicants. Two-factor authentication using OTP and password hashing and salting using the Blowfish Algorithm will be implemented for enhanced security.

3.1.2 Design Phase

The design phase follows the analysis and specification process. Structured design techniques, such as flowchart, system architecture, use case diagram, data flow diagram (DFD), entity relationship diagram (ERD), and data dictionaries, are employed to design the Secure Recruitment Management System (SRMS) based on the gathered requirement and specification. The system will consist of of three main modules: admin, hiring staff, and applicant. Each of the modules will have their specific features in the system that will be discussed in section 4.0 analysis and design.

3.1.3 Implementation phase

The implementation phase of the iterative waterfall model is the third phase of the process which involves building the actual system based on the design created in the design phase. This phase will allow the developer to write code, test completed code, and integrate with other parts of the system. The software testing is conducted to ensure that all system requirements are met without errors before deployment. Hypertext Preprocessor (PHP) is used for programming, and MySql is employed for the database.

3.1.4 Testing Phase

The testing phase ensures the system meets the requirements defined in the analysis phase. Functional testing is performed to verify that the system functions as expected, while non-functional testing to ensure the system performs as expected while the non-functional testing assesses performance, security, and other requirements. Testing phases begin with preparing the test environment, executing test cases, and recording the results. After that, Test results are then analyzed, and any identified defects are fixed. The system is retested to ensure proper resolution of the defects.

3.1.5 Maintenance Phase

The maintenance phase is the final stage of the iterative waterfall model and involves providing ongoing support and maintenance to the deployed system. Issues that arise are addressed, and necessary improvements are made to meet changing user needs. The expectation is to have a continually improved and updated Secured Recruitment Management System that fulfills the evolving requirements of the users.

3.2 Hardware and Software Requirement

Table 2 shows the computer specification and software requirements for developing the system. We developed the Secured Recruitment Management System with Data Retention Approach using Hypertext Preprocessing (PHP) programming language and MyQSL as the database.

Table 2: Hardware and Software Requirement

Requirement		Specification
Hardware	Computer	Laptop: Level51 FORGE 15X RAM: 16gb Processor: 12th Generation Intel Core i7-12700H (14 Cores 20 Threads)
Software	MySql	Software used to build database and data storing.
	Web Hypertext Processor (PHP)	Programming language used to develop the system.
	Xampp v3.3.0	Web server.

4. Analysis and Design

This section briefly explains the analysis and design for the Secured Recruitment Management System with Data Retention.

4.1 General System Architecture

Figure 5 shows the general system architecture for the system. The system caters three main users that are applicants, hiring staff, and admin. The applicant module allows to access and view the list of open job vacancies advertised by the company. If applicants find a job listing that interests them, they can register on the platform. Applicants can bypass the job vacancy list and proceed directly to the registration process. Upon registration, applicants are required to update their profile. To make an application, they need to fill in an application form specifically on their desired position.

The system employs the Candidate Screening Automation feature to filter applicant credentials based on the job requirements. Successful applicants who meet the criteria will be shortlisted as candidates and receive interview invitations. Candidates will go through an interview session and will be evaluated and reviewed by the hiring staff. The result of the interview will be communicated through the portal system. If a candidate is deemed successful, they will be offered the job position. As per the data retention policy, the personal data of applicants or candidates who did not receive interview invitation, failed during the interview session, rejected interview invitation, or declined job offers will be deleted from the database.

The hiring staff module allows staff members to view and update their profile, access the candidate list, review the interview schedule, view the open job vacancy list, evaluate candidates, give feedback after interview, and extend job offers. On the other hand, the admin role has additional privileges, such as creating and deleting open job vacancy listings. Admin can also register, update, and delete hiring staff members.

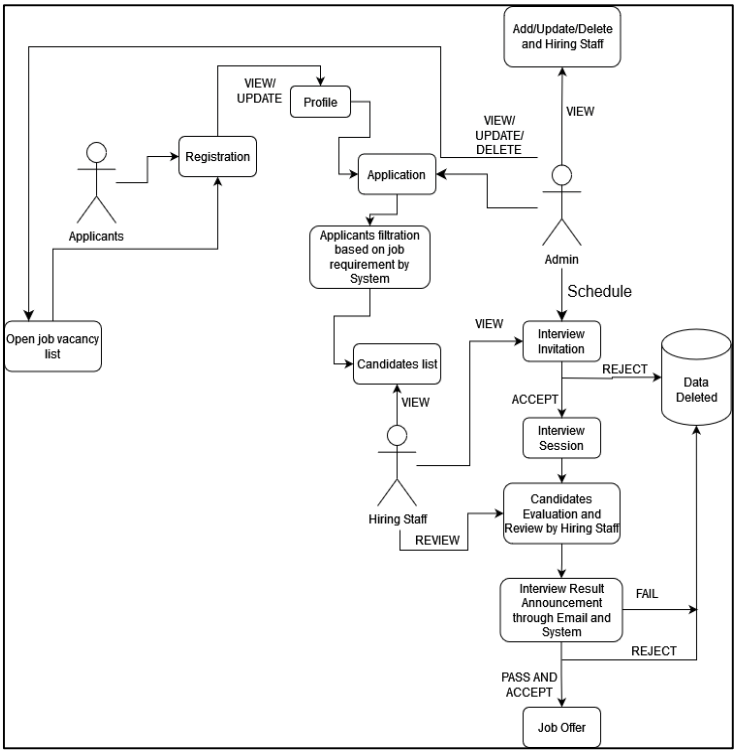

Figure 5: System architecture of the Secure Recruitment Management System for TAMCO Switchgear Sdn. Bhd.

4.1.1 Context Diagram

Context diagram is used to show the data flow among the system's users. Figure 6 shows three entities which are admin, hiring staff, and applicant. The admin entity within the system holds the authority to register hiring staff members and assign them to conduct interview sessions. The hiring staff have the privilege to view the list of shortlisted candidates. They are responsible for conducting interview sessions and providing feedback after the completion of the interview process. Applicants can update their profiles and submit job applications through the system.

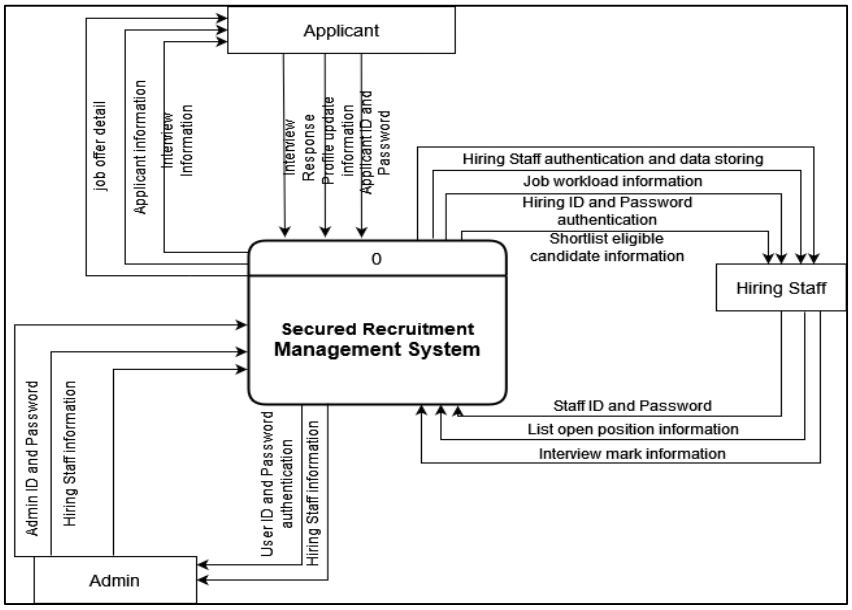

Figure 6: Context Diagram for the system

4.1.2 Data Flow Diagram

Figure 7 shows the Data Flow Diagram for the system. There are a total of nine processes, five databases, and three entities.

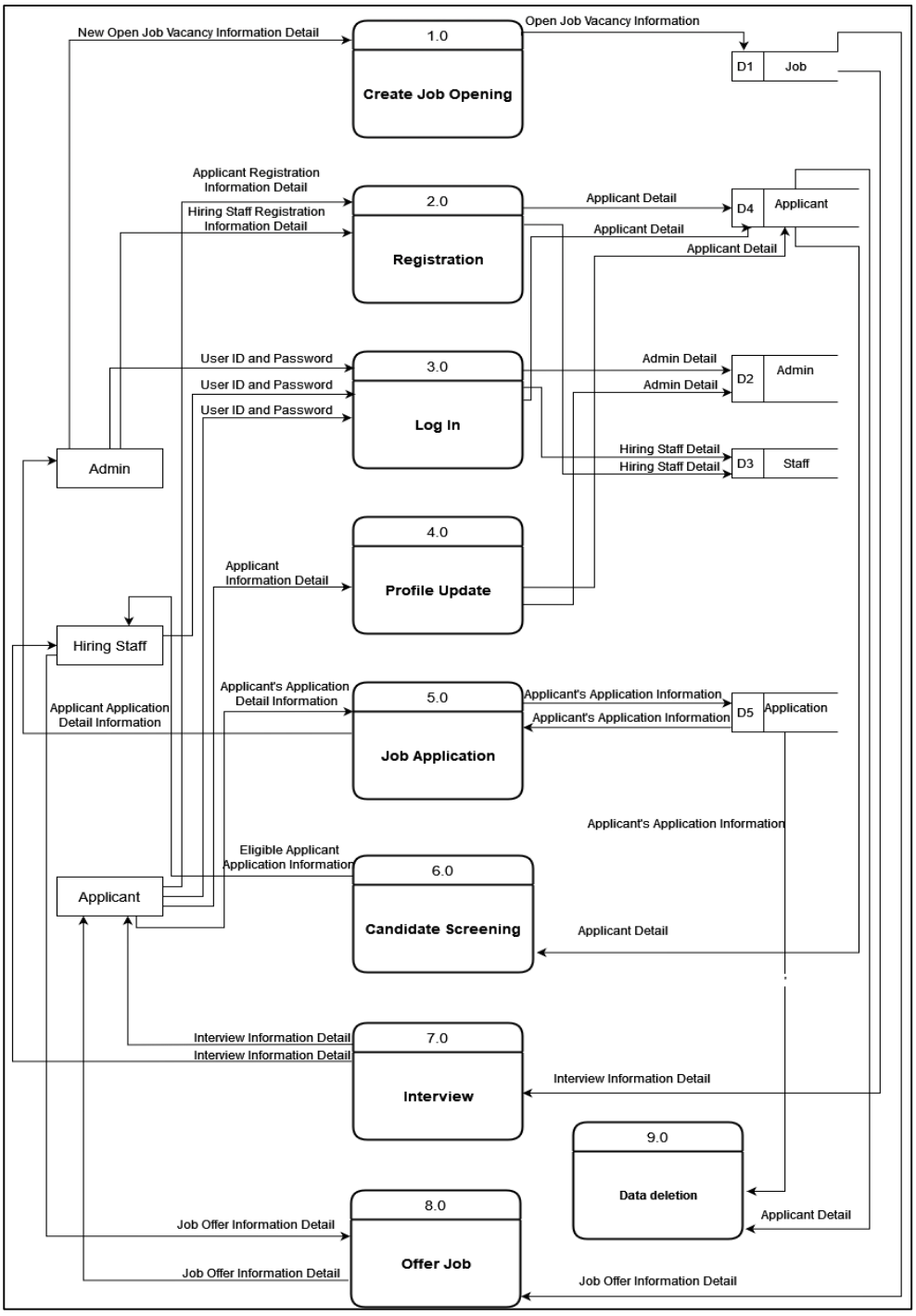

Figure 7: Data Flow Diagram (DFD) of Secure Recruitment Management System for TAMCO Switchgear Sdn. Bhd.

The first process is creating job opening where only admin can create job opening. The second process is registration where applicants can register by their own while the staff will be registered by admin. The third process is login. All users can login to their respective pages. The fourth process is only for applicants where they need to update their profile detail just before applying for the job vacancy. The fifth process is also for applicants where they can make job application. The sixth process

is candidate screening process that will automatically did by the system as it uses the filter candidate automation based on the position requirement. The seventh process is the interview. The eighth process is the job offer that will be done by the staff after they fill in the interview marks in the system. Finally, the ninth process where the data deletion that will be done to user account that has been inactive for sixth months.

4.1.3 Entity Relationship Diagram (ERD)

Figure 8 shows the entity relationship diagram (ERD) of the SRMS. This ERD is used to identify the attribute, primary key, and foreign key of the SRMS system. There are total of four entities as follows:

- Job: Stores data related to job registeration. Attributes: [job_id (Primary Key), position, department, pic, location, job_req, employment, closing, iv_date, job_desc, work_experience, cert, tech_skills, soft_skills, language, created_at, job_status]
- Application: Stores data related to job applications made by applicants. Attributes: [application_id (Primary Key), job_id (Foreign Key), applicant_id (Foreign Key), mark, cert, tech_skills, soft_skills, work_experience, language, resume, apply_status, apply_date]
- User: Stores data related to applicant user. Attributes: [userid (Primary Key), name, email (Foreign Key), ic_number, phone, password, address, sex, education, birth_date, birth_place, civil_status, created_at]
- Userole: Stores data related to user role for the system. Attributes: [email (Primary Key), name, usertype, password]

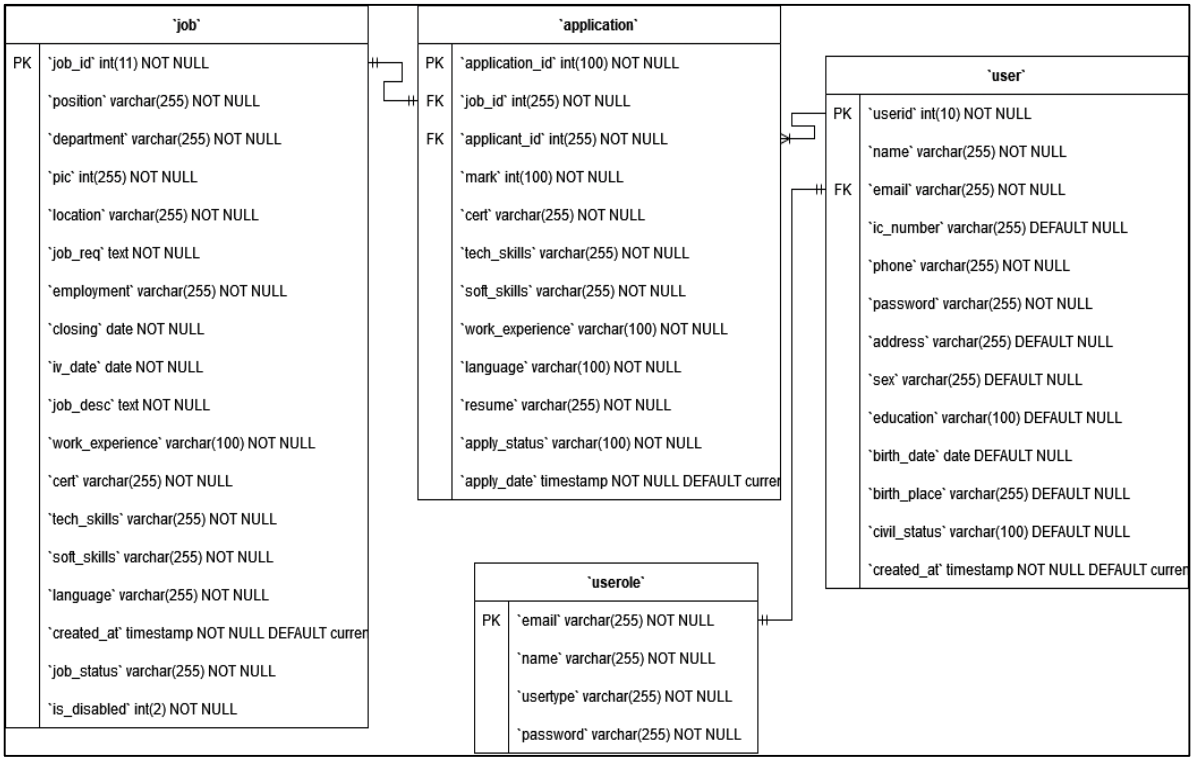

Figure 8: Entity Relationship Diagram (ERD) of Secure Recruitment Management System for TAMCO Switchgear Sdn. Bhd.

4.2 Functional and Non-Functional Requirements

There are several functional requirements for TAMCO Switchgear Sdn. Bhd. that has been identified. It is based on the system user aspect such as admin, hiring staff, and applicant. The functional requirements for the Secured Recruitment Management System are explained in Table 4.

Table 4: Functional Requirement for the system

Functional Requirement	Description
Login Module	All users should be able to login to the system.
Register Module	All applicants should be able to register account in the system.
Application Module	All Applicant should be able to make an application for open job vacancy, upload resume, update cover letter and expected salary.
Open Job Vacancy Module	Only admin should be able to create, update and delete open job vacancy, and all users should be able to view the open job vacancy list.
Candidate Screening Module	The system should be able filtered out eligible candidate automatically after the application submission
Profile Module	All applicants should be able to view and update their profile in the system.
Mark Module	Hiring staff should be able to key in mark after interviewing candidates and offer job to the eligible candidate.
Log Out Module	All users should be able to log out from the system and end the session.

Non-functional requirements are needed to develop the system. The non-functional requirements for the Secured Recruitment Management System are explained in Table 5.

Table 5: Non-Functional Requirements for the system

Non-Functional Requirement	Description
Usability	The system must be a user-friendly user interface to simplify the learning process for users to use the system.
Performance	All users should be able to access the system pages from any browser and has a quick response time. The system also must support heavy traffic from user at one time.
Availability	The system must be always available every time user reached out to the system.
Security	The system must be implementing input and output validation to avoid any unnecessary login from unauthorized user, the encryption of sensitive data in the database to transform plaintext to ciphertext sensitive data and provide One Time Passcode (OTP) during the login.

4.3 User Interface Design

This section will entail more about the system user interface design. It is crucial for the development of the system for the developer to have some insight just before they start to develop the system.

Figure 9 shows the first interface that user will see when they visit the system which is the system's main page. The user can browse the open position vacancy, register, or log into the system to apply for the position. This specific page will advertise all open job vacancies that have been registered by admin for public.

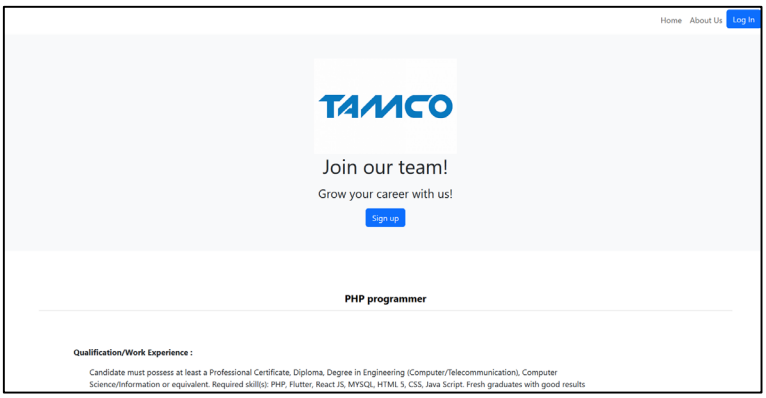

Figure 9: System main page to advertise open job vacancy

Figure 10 shows the two-factor authentication that is implemented in the system by using OTP verification page in the system. Users need to enter the six numbers of OTP received from their e-mail to log in to their account. If the verification failed, they will be redirected to the login page again for them to enter their login credential again.

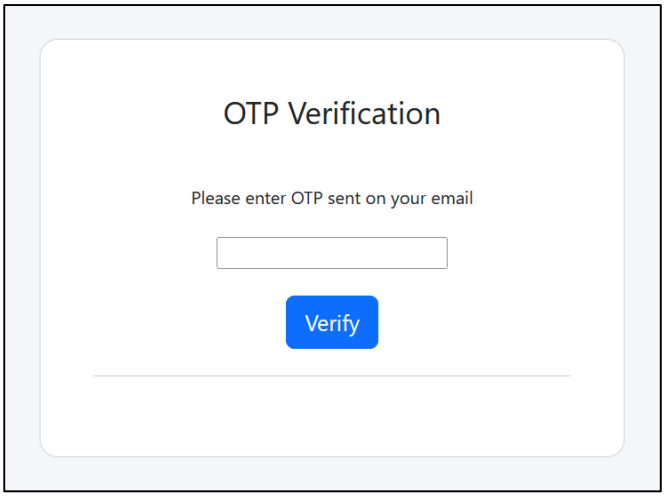

Figure 10: Two-factor Authentication using OTP email verification

Next, Figure 11 shows the application form for open position vacancies that are offered. User needs to fill up the form to apply for respective position. There are five main components for the application which are work experience, professional certification, required technical skills, required soft skills, and preferred language. These five components are crucial for the applicant to fill in as it is the main factor for the candidate automation filtration scheme.

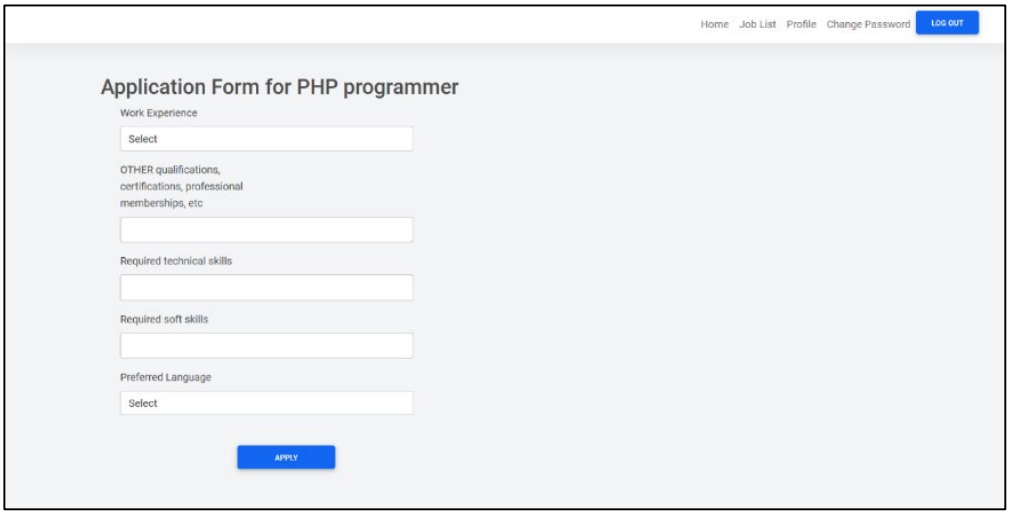

Figure 11: Application form to apply for open job vacancy

Figure 12 shows the applicant profile for applicant. This page will allow applicants to update their profile if there is anything to be updated. Applicants also need to update their account just before applying for any job as the system will only retrieve applicant personal detail from the updated profile or applicant will not allow to apply for any job in the system.

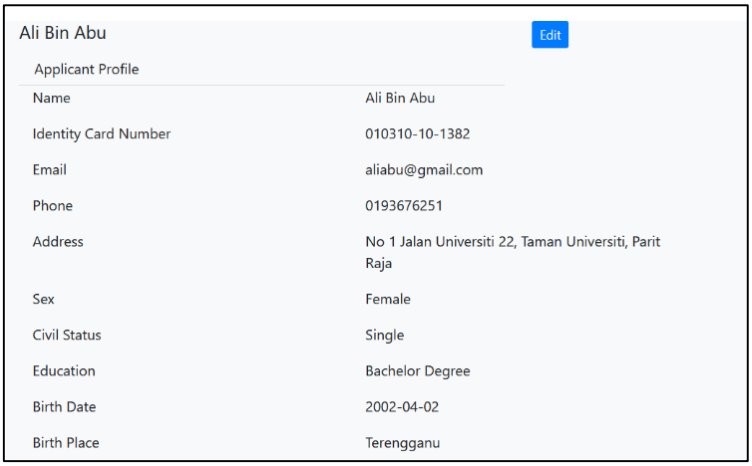

Figure 12: Applicant profile for Applicant

4. Result and Discussion

In results and discussion, the implementation and testing result of proposed system are discussed. There are three security modules included in this system which are data retention, two-factor authentication using e-mail OTP, and password hashing using Bcrypt. Each of these modules are included to lower security risk and avoid data leaks.

Data retention is the amount of time that a system can hold data. In the system, it is set to hold the data of applicant until six months of their inactive account. An account will be labeled as inactive when applicants did not make any recent applicant in the system for six months. Function deleteInactiveAccount() is use to delete any inactive ‘s account applicant. The source code to delete the inactive account is shown in Figure 13.

```php
// Function to delete inactive accounts
1 reference
function deleteInactiveAccount($userid, $email, $connection) {
    // Calculate the date six months ago
    $sixMonthsAgo = date("Y-m-d", strtotime("- 6 months"));

    // Query to select users who haven't made any recent applications
    $query = "SELECT user.userid
              FROM user
              LEFT JOIN application ON user.userid = application.applicant_id
              WHERE user.userid = $userid
              AND (application.apply_date IS NULL OR application.apply_date < '$sixMonthsAgo')";

    $result = mysqli_query($connection, $query);

    if (mysqli_num_rows($result) > 0) {
        // Account is inactive, delete the account and related records
        $deleteQuery = "DELETE user, userole, application
                        FROM user
                        LEFT JOIN userole ON user.email = userole.email
                        LEFT JOIN application ON user.userid = application.applicant_id
                        WHERE user.userid = $userid";
        mysqli_query($connection, $deleteQuery);

        return true; // Account deleted
    } else {
        return false; // Account is active
    }
}
```

Figure 13: Source code for database deletion for the inactive account

All passwords that are stored in the database for the system will be hashed using BCrypt algorithm and salted by the password_hash function pre-defined function. The source code for the password hashing and salting are shown in Figure 14. While Figure 15 shows the hashed and salted password stored in the database table userole.

```php
//encrypt the password before saving in the database
$Hashedpassword = password_hash($password_1, PASSWORD_DEFAULT);
```

Figure 14: Source code for password hashing and salting using BCrypt

email	usertype	password
baeirene@gmail.com	staff	$2y$10$lZdavYui71bvmobqBjEdc.a0lMHSeAcCbWOZcjjhg3l...
fazilahramli14@gmail.com	applicant	$2y$10$uv99osK7CYlqs4ZAVq0GKeZrmuqkbRzRhkq/tn7MPUc...
kangseulgi@gmail.com	staff	$2y$10$KB14bJOQQF8uKRFguQ27aucK8ozb8hfghUvb2EeKlZk...
mashitahmt01@gmail.com	applicant	$2y$10$3lR9NlGQ019K/QiXZeStN.7Owmtci1EZwdKsn5Ks0pl...
nrfrhz25@gmail.com	applicant	$2y$10$p3u/TA5RlHucPxvp0IldHOQFKrJkDLZheo6fZZqyLyl...
psseudogi@gmail.com	admin	$2y$10$VShNO2Lu0bqS73a8ox8kL.6K/K8YfciMOVgX4gb7PoW...
sonwendy@gmail.com	staff	$2y$10$zmHAeTnP0mvRcZ3o5feXkOOVCBq.CuM1jZDb4Ox7qjm...

Figure 15: Userole table storing the hashed and salted password

The system implemented two-factor authentication using OTP verification sent through e-mail. The OTP will be generated by using the generateOTP() function that is set to six lengths and it will use secret keys source from openssl_random_pseudo_bytes(32). The source code for the OTP generation is shown in Figure 16.

```php
// Function to generate OTP using secret key
1 reference
function generateOTP($length = 6) {
    // Generate a random secret key
    $secretKey = openssl_random_pseudo_bytes(32);

    // Generate a random OTP based on the secret key
    $otp = '';
    for ($i = 0; $i < $length; $i++) {
        $otp .= random_int(0, 9); // Generate a random digit (0-9)
    }

    return [
        'otp' => $otp,
        'secretKey' => base64_encode($secretKey)
    ];
}
```

Figure 16: Source code for generating OTP number using secret key

Candidate filtration automation mechanism is implemented in the system to help the staff filter out only eligible candidate base on position requirement. There are five main keywords for the filtration that are work experience, professional certification, required technical skills, required soft skills, and preferred language. From the five keywords, the algorithm will calculate the total weightage and return true if the total weightage is greater than 5 while it returns false if otherwise. The source code of the algorithm is shown in Figure 17 (a) and Figure 17 (b).

```php
// Find the common words between the two arrays
$commonWords1 = array_intersect($apply_cert, $req_cert);
$commonWords1 = array_map('trim', $commonWords1);

$commonWords2 = array_intersect($apply_tech_skills, $req_tech_skills);
$commonWords2 = array_map('trim', $commonWords2);

$commonWords3 = array_intersect($apply_soft_skills, $req_soft_skills);
$commonWords3 = array_map('trim', $commonWords3);
```

Figure 17 (a): Source code for the algorithm to search for common words between two keyword strings

```php
$weightage = 0;
// Part 1
if (count($commonWords1) > 1) {
    $weightage += 2;
} elseif (count($commonWords1) == 1) {
    $weightage += 1;
}

if (count($commonWords2) > 1) {
    $weightage += 2;
} elseif (count($commonWords2) == 1) {
    $weightage += 1;
}

if (count($commonWords3) > 1) {
    $weightage += 2;
} elseif (count($commonWords3) == 1) {
    $weightage += 1;
}

// Part 2
if ($apply_language == $req_language) {
    $weightage += 2;
} else {
    $weightage += 1;
}

// Part 3
if ($apply_work_experience == $req_work_experience) {
    $weightage += 2;
} else {
    $weightage += 1;
}

// Check if the total weightage is greater than 5
if ($weightage > 5) {
    return true;
}
return false;
```

Figure 17 (b): Source code for the algorithm to count the total weightage for the keywords

This section serves to use acceptance test result after the completion of the system. The user acceptance test is used to check whether the system has fulfilled all functionality of the system. A total of five users including TAMCO Switchgear HR Admin, staff and applicants have tested the system and fill in the test form. The results of the test are summarized in Figure 18 based on the response given by the user.

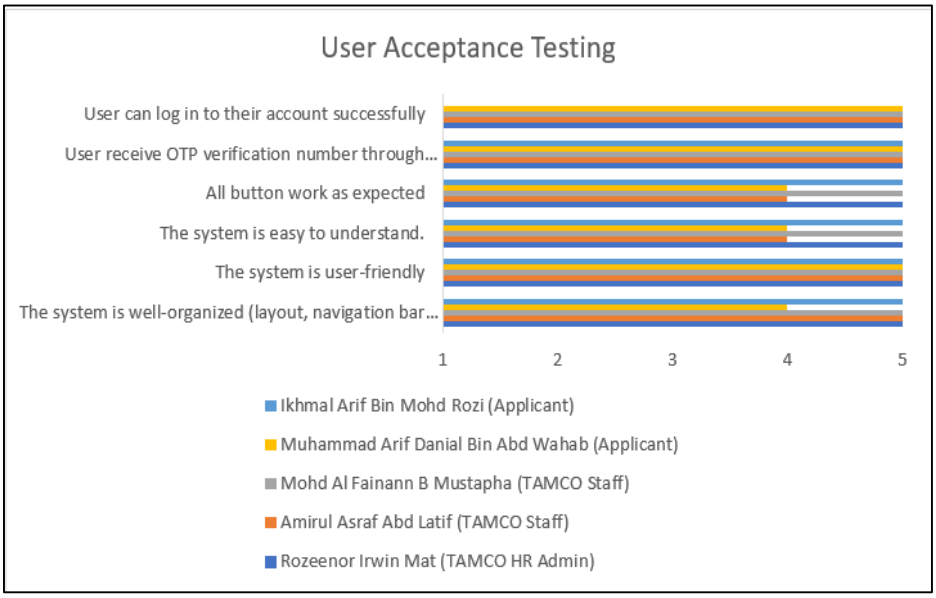

Figure 18: Applicant profile for Applicant

4.2 System Functionality Test

This section serves as both a reference for identifying errors when the test is executed and an explanation of the function's expected result. The Secured Recruitment Management System with Data Retention teste case is listed in Table 6. There are nine test cases which are sign up and log in, log in verification code OTP, staff registration, job registration, profile update, job application, candidate screening automation, data retention, interview feedback, and change and forgot password. The result of the functionality testing is all passes.

Table 6: Test Case

Test Case	Expected Result	Result
Sign Up and Log In	All users can sign in the system into different interface based on their respective role.	Pass
Log In verification code OTP	All users can receive OTP through registered e-mail.	Pass
Staff registration	Admin can register staff as person in charge for the job recruitment process.	Pass
Job registration	Admin can register open job vacancy and advertised it on company main page.	Pass
Profile update	Applicant can update profile just before applying the job.	Pass
Job application	Applicant can apply for specific job once using the same identity card number.	Pass
Test Case	Expected Result	Result
Candidate Screening Automation	The system can filter out eligible candidate and reject non eligible candidate application.	Pass
Data retention	Applicant's application data such as submitted resume will be deleted if the applicant rejected, reject the interview, and reject the job offer.	Pass
Interview feedback	Hiring can key in feedback after interviewing candidates, view feedback score, offer and hire job to the eligible candidate.	Pass

5. Conclusion and Future Works

Secured Recruitment Management System is a recruiting software project developed with the aim of providing a secure online web-based platform in managing the recruitment process for TAMCO Switchgear Sdn. Bhd. The system offers important features in the recruiting process such as posting job openings, filter candidate application, reviewing candidates after interview, and offering job. The system also offers several security features such as password hashing and salting, two-factor authentication, and data retention. It has achieved the objective for the project which is to design, develop, and test the secured recruitment management system with data retention. This system also has solved the problem that was stated before such as it helps the TAMCO staff to manage recruitment process in a very effective way and protect applicants' data from data breach. In future works, it is expected to add more features for staff giving feedback by filling in form for each candidate, interview module, and adding more security module such as Cross-Site Scripting (XSS) protection and rate limiting and brute force protection.

Acknowledgment

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support throughout the process of conducting this project.

References

[1] *Personal Data Protection Act 2010*. Malaysia, 2010, p. 52. [Online]. Available: http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act 709 - Personal Data Protection Act 2010.pdf

[2] J. Tian and T. Zhang, "Secure and effective assured deletion scheme with orderly overwriting for cloud data," *J. Supercomput.*, vol. 78, no. 7, pp. 9326–9354, 2022, doi: 10.1007/s11227-021-04297-z.

[3] J. Tian and Z. Wang, "Fine-grained assured data deletion scheme based on attribute association," *Comput. Secur.*, vol. 96, p. 101936, 2020, doi: https://doi.org/10.1016/j.cose.2020.101936.

[4] H. Mercier, M. Augier, and A. K. Lenstra, "STeP-Archival: Storage Integrity and Tamper Resistance Using Data Entanglement," *IEEE Trans. Inf. Theory*, vol. 64, no. 6, pp. 4233–4258, 2018, doi: 10.1109/TIT.2018.2825981.

[5] K. N. Rahmanto and M. Riasetiawan, "Data Preservation Process in Big Data Environment using Open Archival Information System," in *2018 4th International Conference on Science and Technology (ICST)*, 2018, pp. 1–5. doi: 10.1109/ICSTC.2018.8528669.

[6] P. P. Pittalia, "A comparative study of hash algorithms in cryptography," *Int. J. Comput. Sci. Mob. Comput.*, vol. 8, no. 6, pp. 147–152, 2019.

[7] C. Skanda, B. Srivatsa, and B. S. Premananda, "Secure Hashing using BCrypt for Cryptographic Applications," in *2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, 2022, pp. 1–5. doi: 10.1109/NKCon56289.2022.10126956.

[8] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five two-factor authentication methods," in *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*, 2019.

[9] "Jobs in Malaysia - Search Job Vacancies - Career | JobStreet.com.my." 2023. Accessed: Jan. 10, 2023. [Online]. Available: https://www.jobstreet.com.my/

[10] "Recruitment Management Software - Free App Template {$\vert$} Caspio." Jan. 2023. [Online]. Available: https://marketplace.caspio.com/details/recruiting-management

[11] P. Trivedi and A. Sharma, "A comparative study between iterative waterfall and incremental software development life cycle model for optimizing the resources using computer simulation," in *2013 2nd International Conference on Information Management in the Knowledge Economy*, 2013, pp. 188–194.