Applied Information Technology And Computer Science Vol. 3 No. 2 (2022) 101-117
© UniversitiTun Hussein Onn Malaysia Publisher's Office

AITCS

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

Secured Forensics Reporting Web Based on Two Factor Authentication

Sanishaa Nair Sivakumaran[1], Zubaile Abdullah[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.2022.03.02.007
Received 14 September 2022; Accepted 06 October 2022; Available online 30 November 2022

Abstract: Computer forensics emerges in response to the escalation of computer and Internet crimes. The main focus in this project is on the final step of computer forensics which is the reporting stage. At the moment forensics analysts at Chiteeram Solution tend to use manual methods and third-party tools which are single authenticated to perform computer forensics investigation. Hence, the security of web reporting is less secure. This project is proposed to tighten the web reporting document based on two factor authentication which is One Time Password (OTP) via email and recaptcha at user login. These provided an extra security layer to secure user accounts. The methodolody of this project is using Waterfall Model and using PHP Codeigniter Framework. In order to test the security performance of this project, SQL injection syntax is performed to see the security strength of password whereas md5hashing.net is used to test the strength of pdf password. The application allows users to encrypt or decrypt the generated forensics report. There is also strong password management to ensure the confidentiality of the system.

Keywords: Forensics Reporting Application, Encrypt Pdf, Decrypt Pdf, Strong Password. 2 Factor Authentication

1. Introduction

Computer forensics emerges in response to the escalation of computer and Internet crimes. These crimes are increasing due to the growing dependence on computers and digital media [4]. The main goal of computer forensics is to perform a structured investigation on the occurrence of related events and the reason behind it while ensuring a well-documented chain of evidence in a formal report.

There are several steps when it comes to handling computer forensics investigation [8]. The main focus in this project is on the final step of computer forensics which is the Reporting stage [5]. Forensic investigators and companies are facing many challenges in terms of developing and generating a secure forensics report that can be submitted to court or legal officer as tamper proof evidence.

Founded in 2014 is an IT based firm and reformed in 2021 January Chiteeram solution is a small team but strongly growing, which they comprise of talents from different backgrounds working together

*Corresponding author: zubaile@uthm.edu.my
2022 UTHM Publisher. All rights reserved.

to provide services in multiple different verticals. They specialize in developing customized IT solutions, which includes both web and mobile based applications as specified by their customer preference. Besides, they recently progress having a small forensics team. They also provide a variety of other services such as Marketing consultancy, Event Management, Professional Photography and Videography Services, as well as IT Trainings [12].

Such as mentioned in the conducted interview Chiteeram solution company conducts their forensics investigation manually or using the available forensics tool on the net. However, these third-party tools such as securecube and monolith forensics are single authenticated where it does not require a second authenticated to access the system. Not only that, the company has faced tampering of data of the end product of the forensics report.

There are several objectives for this project - To design forensics documenting application with 2 factor authentication, to develop a 2 Factor authentication forensics documenting application, to test the 2 Factor authentication forensics documenting application, to generate an encrypted forensics report in pdf format file to ensure the integrity of the data. The scope of this project is admin and forensic analyst.

The proposed application allows only registered administrators and forensic analysts to encrypt or decrypt the forensics report generated. The users as mentioned are able to encrypt the forensics report (pdf) with a strong password only which contains at least 8 characters with a minimum of one upper-case character, a minimum of one lowercase character, a minimum of one number and a minimum of one symbol. Then users are only able to view the encrypted forensics report (pdf) by decrypting it with the correct password only. This is to ensure the integrity of the document is maintained.

Registered administrators can view audit trails of users whenever changes are made throughout navigating the application. For instance, the timestamp of the user encrypting the pdf is recorded. This is to ensure that no mishandling data occurs at the end of the day. Project significance is to ensure all parties adhere to the integrity and confidentiality of the application via 2 Factor authentication when login and ensure the validity of the generated report.

Strong password management in the system is to force users to use a strong password. The proposed system allows users to set their own password. The password must contain at least eight characters with a minimum of one upper-case character, a minimum of one lower-case character, a minimum of one number, and a minimum of one symbol. The combination of characters and integers to the password slows down the brute-force attack [4].

When you sign into your account, you must first verify with a username and password - this is the first phase of verification. Two-factor authentication adds a second security layer to the procedure, allowing you to validate your identity. Its goal is to make life difficult for attackers and reduce fraud risks. If you already employ basic password security precautions, two-factor authentication will make it more difficult for cyber criminals to gain access to your account because the second authentication element is tough to obtain; they would have to be much closer to you. Their chances of succeeding are substantially reduced because of this.

2. Literature Review

In this section, related literature reviews are explained including the steps in digital forensics, CIA triad consisting of confidentiality, Integrity and authentication, and comparison of the applications.

2.1 Steps in Digital forensics

The first stage implies the identification of investigation goals and required resources. The analysts also identify the evidence, the type of data they deal with, and the devices the data is stored on. Digital forensics specialists work with all kinds of electronic storage devices: hard drives, mobile phones, personal computers, tablets, and others [7].

Next, through search and seizure the team looks for proof and data on the gadgets used in the crime. Investigators grab the devices to ensure that the criminals are unable to carry out their plans. Any gadgets used during a crime scene were then meticulously seized in order to retrieve data from them.

During preservation, the evidence is stored in an isolating place to secure and preserve it from any thefts. It will stop people from buying digital devices so that any kind of proof is not meddled with.

During the examination phase, procedures for retrieving, copying, and storing evidence within appropriate databases must be in place in order to effectively investigate potential evidence. Investigators typically examine data from designated archives, using a variety of methods and approaches to analyze information. These could include utilizing analysis software to search massive archives of data for specific keywords or file types, as well as procedures for retrieving files that have been recently deleted. Investigators value data with times and dates, as well as suspicious files or programs that have been encrypted or intentionally hidden.

The inspection group will reform the chunks of evidence in this analysis phase and determine the outcome based on the proofs or evidence that result. However, discovering the support in a criminal case may take several cycles.

In the final phase, the team such as forensic analysts investigates and documents data and evidence in accordance with the court of law. This phase happens once the initial criminal investigation is down. Team members report and document data and evidence in accordance with the court of law.

2.2 Confidentiality

Confidentiality is such as Any information about a person's private life that they do not want shared with others is considered 'confidential.' This information is distinct from 'public information,' which is available to anybody. The right of research participants to not disclose certain information and to retain control over their privacy has increasingly been acknowledged inside and outside of academia and has become subject to extensive legislation [9].

Next, a pdf encrypted with password is significant [6] as stated there are few reasons that bring benefits to having a password protected document. Firstly, the password protected document remains confidential where it was intended to prevent unauthorized parties from accessing the related document. Hence, provides a secure document which is original and certainly protects original works. Hence, maintaining integrity while avoiding potential threats such as altering or tampering the document without one's permission and out of given permission.

2.3 Authentication

Authentication is a process that encompasses processes that allow systems to determine if a user is who they say they are. Two factor authentication is basically a validation method that uses two methods of authentication to create a system with security features that are current with technology advancements. The verification account website is compared to two factor authentication procedures such as producing a six-digit random number (OTP), applying photo verification, and using the verification account website. Third parties or hackers will have a hard time obtaining users' personal information if they employ two authentication factors, preventing identity theft [10].

Password management is a set of guidelines and practices that users follow while storing and managing passwords. For maximum password security and to prevent unauthorized access, password

management is crucial. At least eight characters, including one capital letter, one lowercase letter, one small letter, one numeric character, and one unique symbol, make up a good password.

CAPTCHA is a form of visual verification and identification that uses a challenging Artificial Intelligence (AI) issue to discriminate between humans and bots. CAPTCHA is primarily used to combat auto-bots and click fraud during account registration. Its application may also be used to verify a group of persons who have similar knowledge or skills. For the proposed application, math captcha is used [11].

2.4 Comparison of Existing System

The review of the existing system is crucial to analyze the similarities and differences of the system. The goal of this review is to determine weaknesses and flaws of the existing application and improve the build of the proposed application. A comparison of two forensic reporting applications is made. Monolith forensics and Securecube are the two related applications. The differences between the proposed application and the existing applications are shown in a comparison in Table 1. Both the existing monolith forensics and securecube are tool based. Only pro version of monolith forensics possess login, however the free version of monolith forensics and securecube does not possess login.

Table 1: Comparison of existing and proposed forensics reporting applications

	Monolith forensics	Securecube	Proposed application
Type of integration	Tool Based	Tool Based	Web Based
Login	Pro version (yes) Free version (no)	No	Yes
Login attempt	-	-	Yes
Password requirement	-	-	Yes
Secure report generation (Password)	No	Yes	Yes
Reporting module	Pro version (pdf) Free version (csv, word)	Licensed version	Yes
Audit trail	Pro version (pdf)	Licensed version	Yes

3. Methodology

Waterfall model is the method used in developing the proposed application. There are five phases in the waterfall model. The first phase is the analysis phase. The second phase is the design phase. The third phase is the implementation phase. The fourth phase is the testing phase. The final phase is maintenance. However due to some time constraints maintenance will not be implemented in this project [1].

3.1 Waterfall Analysis Phase

The waterfall analysis phase includes the activity of planning and requirement analysis [2]. The planning activity is to design a few interview questions and perform an interview with the director of chiteeram solution company. The interview question is designed to understand how the forensics team are running their work. To know the ones who are especially responsible in reporting the activity. To understand and know how the forensic team handles the forensics process. This information is collected to be analyzed at the analysis phase.

As shown in Table 2, user management module, user profile module, audit log management module, report generation module and login module are displayed as functional requirements of the system. Table 3 shows the nonfunctional requirements are listed as operational where the system is only

available with internet connection, then in terms of usability where the system is minimalistic and user friendly. Finally in terms of security aspects proposed such as OTP via email and encryption or decryption of pdf format forensics report.

Table 2: Functional requirement Analysis

Module	Functional requirement
User management	Admin only should register the users Admin only should be able to edit or update profile of users
User Profile	Users should be able to edit their own profile Users should be able to change their password
Audit log management	Admin will get to view the log generated by computer with the related timestamps and other information stored
Report generation	Users should be able to generate a forensics report (pdf) with password
Login page	Users uses email to login the account for forensics reporting application

Table 3: Non-Functional requirement Analysis

Requirement	Actual result
Operational	System only available when there is internet connection
Usabilility	The system is minimalistic and user friendly The system has fast adaptability to its functions
Security	Users may access the system by input correct Recaptcha and the correct OTP (One-Time-Password) that is sent to user via email User may encrypt forensics report (pdf) with a complex password. User may decrypt the forensics report (pdf) with correct password.

The requirement analysis activity is to analyze the collected information from the director of the company. The first requirement of the application is to allow the admin and forensic analyst to perform reporting of any sort of computer forensic cases. The second project requirement is to ensure both admin and forensic analyst to encrypt the report generated with a strong password. The third project requirement is to ensure both admin and forensic analyst to decrypt the forensics report (pdf) with only the correct password to be able to view the specific report. Final project requirement is to ensure admin be able to view and record audit trails when any changes made such as timestamp of the time a forensics report (pdf) is encrypted or decrypted.

Figure 1 shows the system architecture design of the proposed application that users such as forensic analyst and admin able to perform respective activities. As the system is a web-based application, the user needs an internet connection to use it. New admin and forensic analyst need to be added by registered admin. After the 2-factor authentication such as captcha and OTP via email is successful at login, admin may manage other admin, forensic analyst, view and edit user profile, view recorded audit trail, view audit log of report. Then both admin and forensic analyst may generate a report based on computer forensic cases that occur, encrypt the generated report with a complex password, and decrypt the encrypted report with only the correct password.

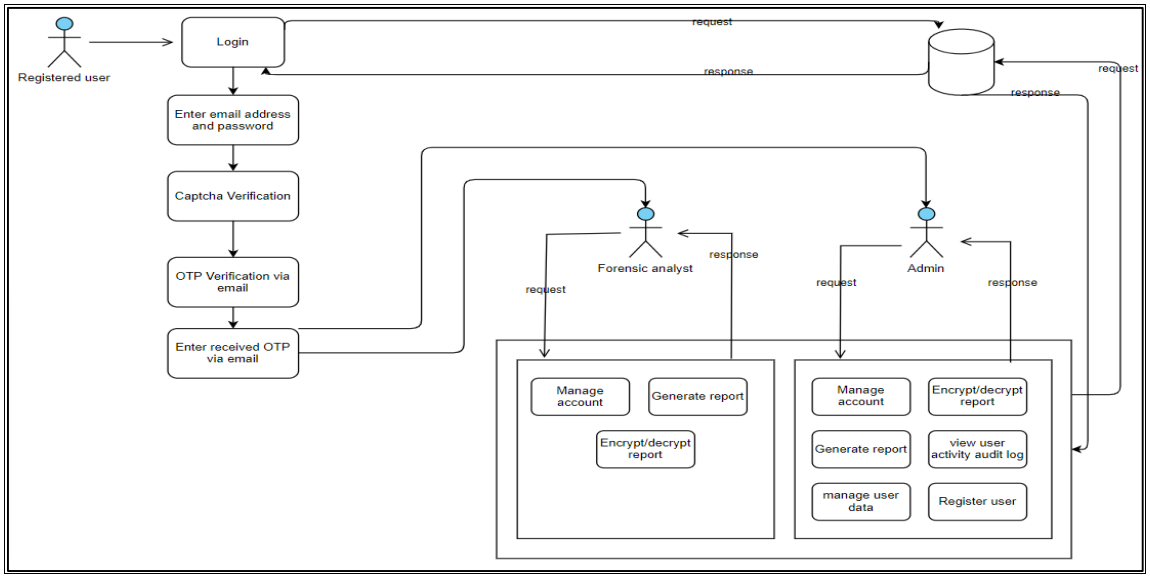

Figure 1: System architecture design of proposed application

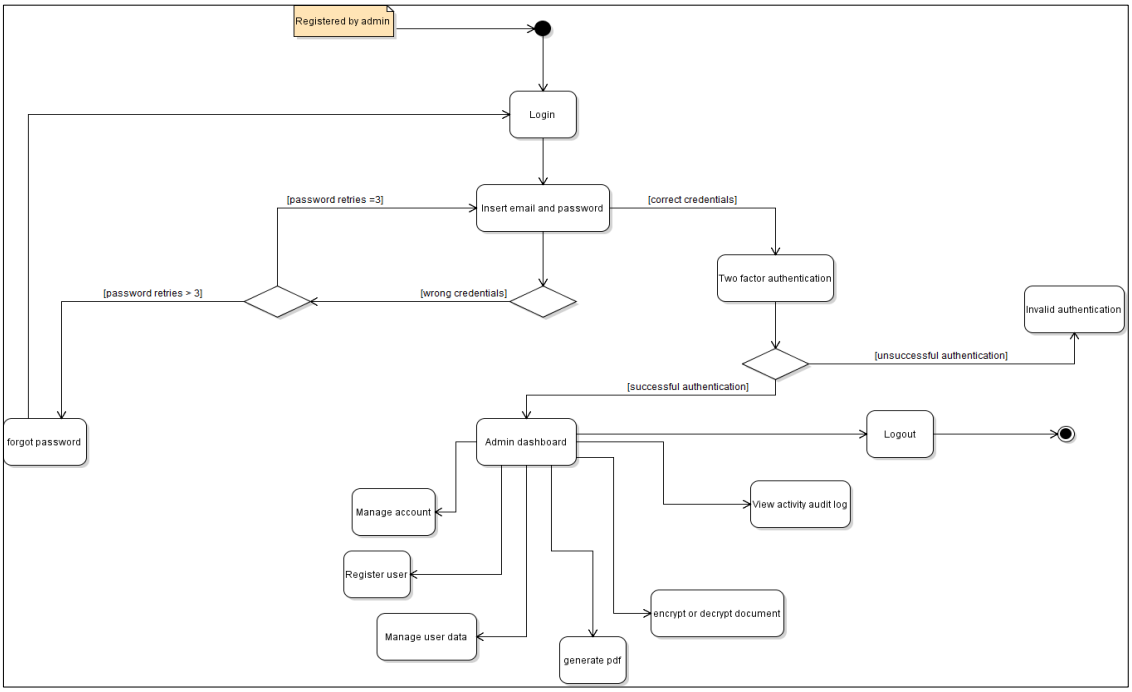

Figure 2: Activity diagram for admin

Figure 2 shows the activity diagram for admin. The activity starts by admin logging in to the application. Admin log in to the application with email and password with a maximum login attempt of three. Then, the admin needs to reset the password after reaching the maximum number of the login attempt. After successful login with correct credentials and successful authentication, the admin is prompted with a dashboard where admin is given options to perform all the operations of forensic analysts. Admins additionally can register forensic analysts to the application. Besides, admin can manage user data. Not only that, admin can also view audit logs on the application. The activity is ended when the admin logs out from the application.

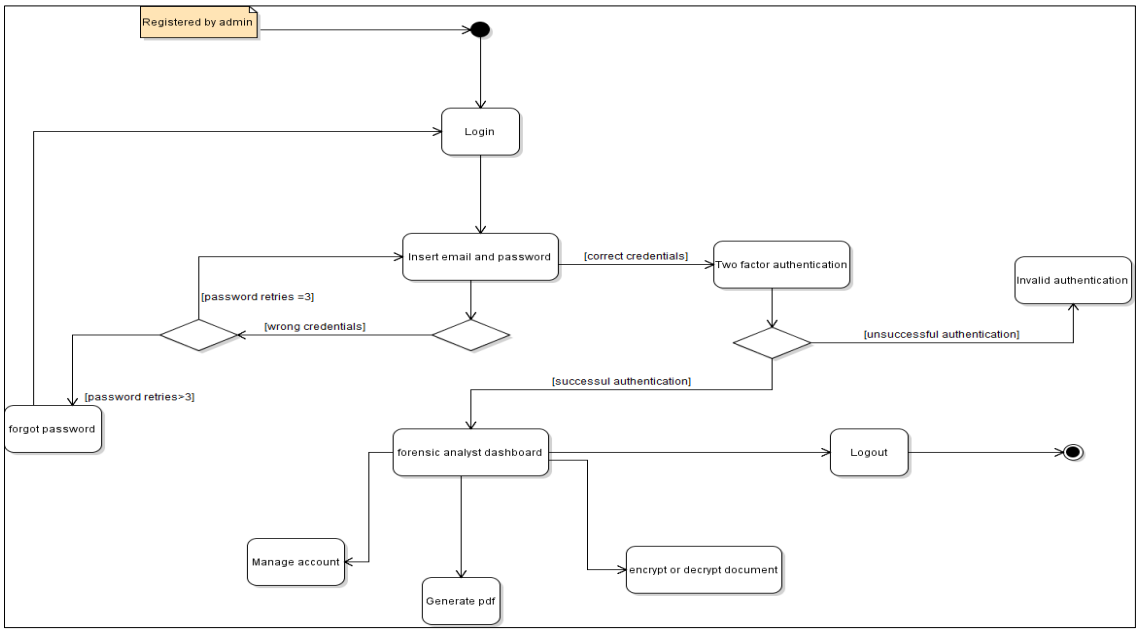

Figure 3: Activity diagram for forensic analyst

Figure 3 shows the activity diagram for forensic analysts. The activity starts by forensic analyst logging in to the application. Forensic analysts are pre-registered to the application by admins. Then, forensic analysts log in to the application with the assigned email and password with a maximum login attempt of three. The forensic analyst needs to reset the password if user forgot password. After successful login with correct credentials and successful authentication, forensic analysts are prompted with a dashboard where the forensic analysts are given options to generate forensics report (pdf) and encrypt or decrypt those forensics report (pdf). Besides, they can edit and manage their account in the settings. The activity ended when the forensic analyst logout from the application.

3.2 Waterfall Design Phase

In this waterfall design phase, a scheme design will be created and the user interface of the forensics reporting application will be designed. The scheme design will be created by referring to the UML class diagram created in the analysis phases.

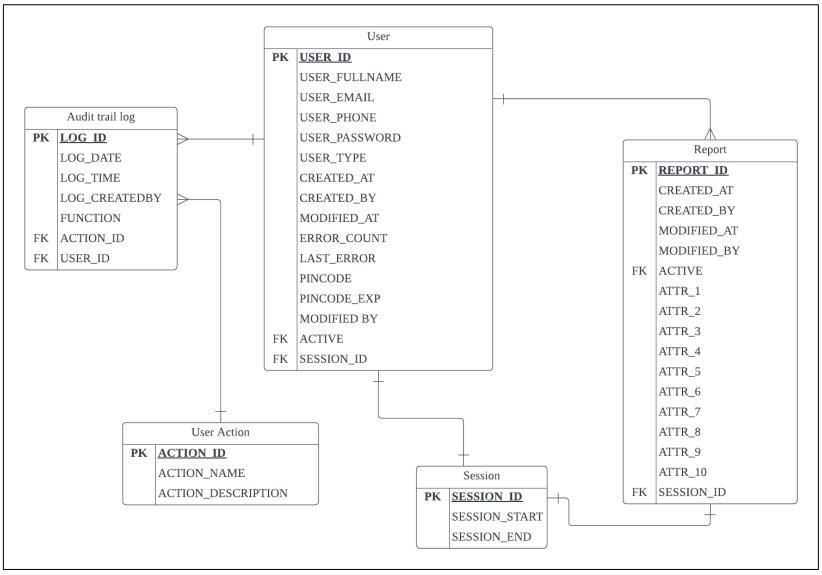

Figure 4: Scheme design

Figure 4 shows the schema diagram of the proposed application. There are five entities in the application which are 'User', 'Session', 'User Action', Report, 'Audit Log'. The test plan also designs in this phase. A test plan is designed to test the forensics reporting process such as to test the email verification, report management, report generation, report encryption, report decryption, user management from admin, register of users from admin, test the login and register input validation.

3.3 Implementation and Testing

In this implementation phase, the design is coded. The design of classes, database tables and user interface are implemented. All the classes and database tables are linked together to make sure that functions well. Besides that, the user interface is linked to classes. The PHP programming language (PHP framework codeignitor) is used.

In the testing phase, the designed test plan ensures that the proposed system functions as expected. The test plan contains two categories. First is to test the system functionality. Second is to test the security requirement. If an error happens, the debugging process is taken to ensure that the system functions well [2].

Table 4: Test plan for authentication model

No	Description	Expected result	Actual result
1	Register - Input registered email	Message appear: email is already registered	Pass
2	Verify code - Input wrong verification code (login)	Message appear: Invalid verification code	Pass
3	Verify code - Input expired verification code (login)	Message appear: Invalid verification code	Pass
4	Verify code - input correct verification code	Redirect to home page	Pass
5.	ReCAPTCHA - Input wrong captcha (login)	Message appear: Invalid captcha	Pass
6.	ReCAPTCHA - every login new Mathcaptcha (login)	New captcha calculation given	Pass

As shown in table 4 which is the testing plan result for the authentication model. Overall, if a user did not verify via 2 factor authentication such as OTP via email and reCAPTCHA, an error message will be prompted to ensure that the user does not skip the step. Hence, after inputting correct verification code users will be redirected to the home page based on either admin or forensic analyst.

Table 5: Test plan for report activity module

No	Description	Expected result	Actual result
1	Empty validation when creating report	Message appear: fill in the blank place	Pass
2	Decrypt pdf - input wrong password	Unable to view report	Pass
3.	Encrypt pdf - empty input	Message appear: Please fill in the empty spaces	Pass
4.	Only accepts pdf to upload	Pdf format report only should be accepted	Pass

As shown in Table 5 which is the testing plan result for the report activity model. Overall, if the user leaves blank when creating a report, an error message will be shown to ensure the user fills in the required details. Next, when a user uploads a report, it should only be in the form of a pdf, as the system does not allow other document formats.

Table 6: Security checklist for proposed system

No	Check list	Actual result
1	Only able to login with correct reCAPTCHA (mathcaptcha)	Pass
2	Only able to login with correct OTP verification	Pass
3	Only able to reset password with reset link and OTP via email	Pass
4	Only be able to encrypt generated forensics report with strong password	Pass
5	Only be able to decrypt encrypted forensics report with correct password	Pass
6	Admin only be able to register user with strong password only	Pass

As shown in Table 6 which is the security check list for proposed system, users should only be able to login with correct reCAPTCHA, with correct OTP verification, reset password with reset link and OTP sent via email, encrypt generated forensics report with only strong password, decrypt encrypted forensics report with correct password only, and finally register user with strong password only. Due to the limitation of time, maintenance step is not going to implement in this project.

4. Results and Discussion

In this section, the result of 2 factor authentication and encrypt/decrypt pdf implementation will be shown, test plan result and security test plan.

4.1 ReCAPTCHA (Mathcaptcha)

Figure 5 shows the code segment for captcha validation. In this project the type of captcha is used is math captcha. Hence,Math.random is used where a random math calculation is generated every time a user refreshes the page. The math captcha here is the addition of 2 numbers. Users are required to input the right answer of the math captcha or else an error is prompted as shown in figure 6.

```
$().ready(function() {
    x = Math.floor(Math.random() * 100);
    y = Math.floor(Math.random() * 100);
    $('label#captcha').text(x + " + " + y + " = ");
    correct = x + y;

    $("#myform").submit(function(e) {
        e.preventDefault();

        // $(".alert").addClass("d-none");
        // $("#alert_processing").removeClass("d-none");

        do_login();
    });

    $("#mypincodeform").submit(function(e) {
        e.preventDefault();
        do_verify();
    });
});

const do_login = async () => {
    $("#alert_processing").removeClass("d-none");
    let formData = new FormData();
    let ans = $("[name='captcha']").val();
    if (ans != correct){
        $("#alert_error_captcha").removeClass("d-none");
    $("#alert_processing").addClass("d-none");
        return;
    }
```

Figure 5: Code segment of math captcha (Recaptcha at login)

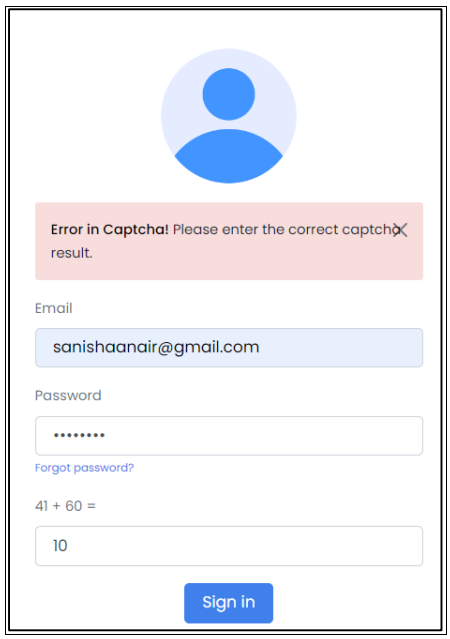

Figure 6: Interface of mathcaptcha at login page

4.2 Login OTP Verification

Figure 7 shows the API call of OTP validation. Function verify () is used with SESSION_USER_VERIFIED as true. Besides the declaration of $pincode is used. Hence, users are required to enter the pin code sent via registered email. If users enter the wrong pin code error is prompted. If user enter pincode after 5 minutes error will also be prompted. The interface of OTP validation is shown in Figure 8.

```php
public function verify()
{
    $email = $_SESSION['SESSION_USER_EMAIL'];
    $pincode = $this->input->post('pincode');

    $output = array('success' => false);

    $user = $this->model_db->verify_pincode($email, $pincode);
    if (!empty($user)) {
        $output = array(
            'success' => true,
            'id' => $user[0]->id,
            'email' => $user[0]->email,
            'fullname' => $user[0]->fullname
        );

        $this->session->set_userdata('SESSION_USER_ID', $user[0]->id);
        $this->session->set_userdata('SESSION_USER_EMAIL', $user[0]->email);
        $this->session->set_userdata('SESSION_USER_FULLNAME', $user[0]->fullname);
        $this->session->set_userdata('SESSION_USER_USERTYPE', $user[0]->usertype);
        $this->session->set_userdata('SESSION_USER_VERIFIED', true);
    }

    return $this->output
        ->set_content_type('application/json')
        ->set_status_header(200)
        ->set_output(json_encode($output));
}
```

Figure 7: Code segment of API call OTP validation

Figure 8: Interface of OTP validation

4.3 Reset Link and OTP Verification

Figure 9 shows the code segment of reset password link via email where the constant of get_reset_link is used. An error message will be prompted if user enters an unregistered email to get reset link. Figure 10 shows the code segment of reset password OTP validation where function reset () is used. Figure 11 shows the reset password interface. Users are required to enter the email registered to get a reset link where they will be redirected to the page as shown in Figure 12. Error message will be prompted if the user gets a reset link with not unregistered email.

```javascript
const get_reset_link = async () => {
    $("#alert_processing").removeClass("d-none");
    let formData = new FormData();
    formData.append('email', $("[name='email']").val());
    fetch('<?= base_url() ?>api/forgot', {
            method: 'POST',
            body: formData,
        })
        .then(response => response.json())
        .then(data => {
            $(".alert").addClass("d-none");

            if (data.success) {
                $("#alert_email").removeClass("d-none");
            } else {
                $("#alert_error").removeClass("d-none");
                $("#alert_processing").addClass("d-none");
            }
        })
        .catch((error) => {
            console.error('Error:', error);
        });
```

Figure 9: Code segment of reset password link via email

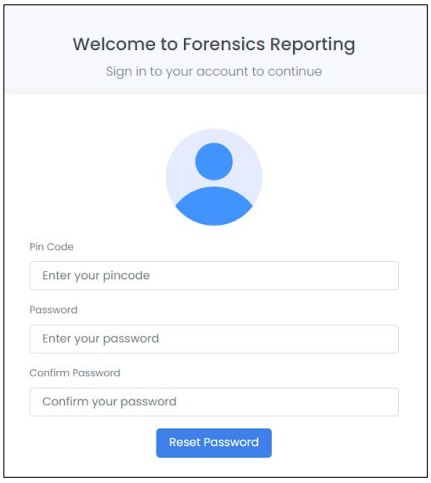

Figure 10: Interface of Reset password link via email

```php
public function reset()
{
    $email = $this->input->post('email');
    $pincode = $this->input->post('pincode');
    $password = $this->input->post('password');

    $output = array('success' => false);

    $user = $this->model_db->reset_password($email, $pincode, $password);
    if (!empty($user)) {
        $output = array(
            'success' => true,
            'id' => $user[0]->id,
            'email' => $user[0]->email,
            'fullname' => $user[0]->fullname
        );
```

Figure 11: Code segment of reset password OTP validation

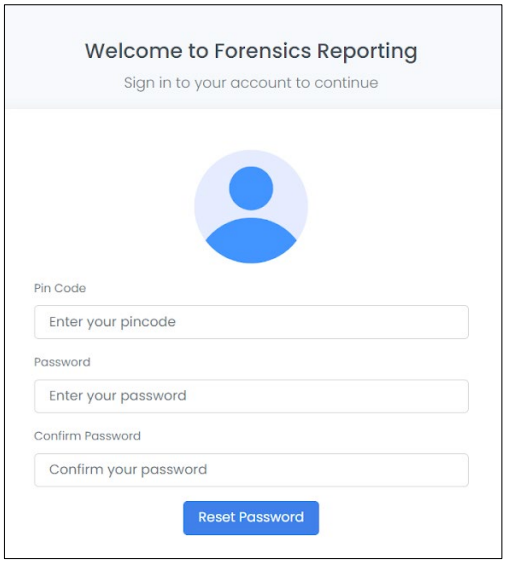

Figure 12: Interface of redirection of reset link

4.4 Encrypt forensics report (pdf)

Figure 13 shows the code segment for encrypt pdf where hash password with sha 256 is used to encrypt the forensics report. Function encrypt_file () is used.

```php
public function encrypt_file()
    {

        $this->model_db->insert_audit($_SESSION['SESSION_USER_ID'], "api/encrypt_file", json_encode($_POST));

        $config['upload_path']          = './uploads/';
        //$config['upload_path']          = 'C:\xampp\htdocs\AssetInventory\application\upload';
        $config['max_size']             = 20480;
        $config['allowed_types']        = 'pdf';

        $this->load->library('upload', $config);

        if (!$this->upload->do_upload('userfile')) {
            $error = array('error' => $this->upload->display_errors());

            print_r($error);
        } else {
            $data = $this->upload->data();

            $filedata = file_get_contents($data["full_path"]);
            $base64 = base64_encode($filedata);

            $this->load->library('encrypt');
            $hashed_password = hash('sha256', $this->input->post("password"));
            $encrypted_string = $this->encrypt->encode($base64, $hashed_password);

            // $decrypted_string = $this->encrypt->decode($encrypted_string, $this->input->post("password"));

            $output_file = $data["file_path"] . "encrypted_" . $data["file_name"];
            $ifp = fopen($output_file, 'wb');
            fwrite($ifp, base64_decode($encrypted_string));
            fclose($ifp);
```

Figure 13: Code segment for encryption pdf

Figure 14 shows the code segment of strong password on encrypt pdf where function checkPasswordStrength () is used. Then complexity of password requirement is a combination of number, alphabets capital or small and special characters. Besides, the length password should be above 6 or else an error is prompted.

```
let password_valid = false;

function checkPasswordStrength() {
    password_valid = false;

    var number = /([0-9])/;
    var alphabets = /([a-zA-Z])/;
    var special_characters = /([~,!,@,#,$,%,^,&,*,-,_,+,=,?,>,<])/;
    if ($('#password').val().length < 6) {
        $('#password-strength-status').removeClass();
        $('#password-strength-status').addClass('pt-2 text-danger');
        $('#password-strength-status').html("Weak (should be atleast 6 characters.)");
    } else {
        if ($('#password').val().match(number) && $('#password').val().match(alphabets) && $('#password').val().match(special_characters)) {
            $('#password-strength-status').removeClass();
            $('#password-strength-status').addClass('pt-2 text-success');
            $('#password-strength-status').html("Strong");

            password_valid = true;
        } else {
            $('#password-strength-status').removeClass();
            $('#password-strength-status').addClass('pt-2 text-warning');
            $('#password-strength-status').html("Medium (should include alphabets, numbers and special characters.)");
        }
    }
}
```

Figure 14: Code segment of strong password on encrypt pdf

4.5 Decrypt forensics report (pdf)

Figure 15 shows the code segment for decrypt pdf where decrypt file () function is used. A folder named upload is created as the upload_path where all the forensics report will be stored in.

```
public function decrypt_file()
{

    $this->model_db->insert_audit($_SESSION['SESSION_USER_ID'], "api/encrypt_file", json_encode($_POST));

    $config['upload_path']          = './uploads/';
    $config['max_size']             = 20480;
    $config['allowed_types']        = '*';

    $this->load->library('upload', $config);

    if (!$this->upload->do_upload('userfile')) {
        $error = array('error' => $this->upload->display_errors());

        print_r($error);
    } else {
        $data = $this->upload->data();

        $filedata = file_get_contents($data["full_path"]);
        $base64 = base64_encode($filedata);

        $this->load->library('encrypt');
        // $encrypted_string = $this->encrypt->encode($base64, $this->input->post("password"));

        $hashed_password = hash('sha256', $this->input->post("password"));
        $decrypted_string = $this->encrypt->decode($base64, $hashed_password);

        $output_file = $data["file_path"] . "decrypted_" . $data["file_name"];
        $ifp = fopen($output_file, 'wb');
        fwrite($ifp, base64_decode($decrypted_string));
        fclose($ifp);
```

Figure 15: Code segment of API call for decrypt file

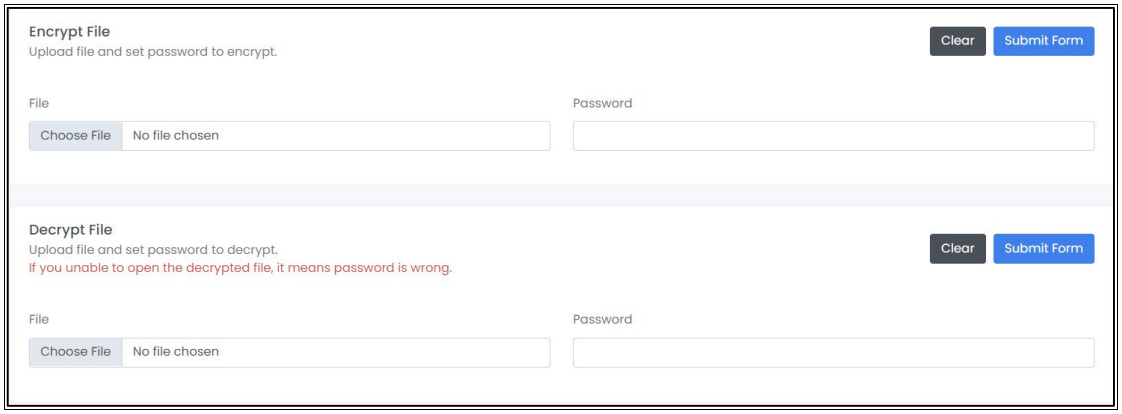

Figure 16: Interface of encrypt or decrypt forensics report

Figure 16 shows the interface of encrypt or decrypt forensics report where a user is required to upload a forensics report to encrypt and input a strong password. Then to decrypt the encrypted report, the user can only view it if input with the correct password.

4.3 Test Plan Result

Security test plan is to test whether the security feature of the developed application is functioning as expected. Table 4 shows the result of the security test plan where the actual result is all pass for the stated security checklist.

Table 7: Security test plan result

No	Checklist	Actual result
1	The user password should include at least eight characters, password one uppercase alphabet, at least lowercase alphabet, one	Pass
2	Application should be able to encrypt the user's password before storing into it the database	Pass
3	Users should be able to encrypt the pdf generated with a complex password	Pass
4	Users should be able to decrypt the pdf generated with a complex password.	Pass
5	Users should be able to decrypt the pdf generated with the correct password	Pass
6	RECAPTCHA when the user logs in.	Pass

4.4 Testing in Terms of Security

In terms of security result, two types of testing are discussed. One is SQL injection testing and the other is decrypt encrypted generated forensics report in pdf format.

(a) SQL Injection Test

SQL injection testing determines whether data may be injected into an application to cause it to run a user-controlled SQL query in the database. If an application uses user input to construct SQL queries without sufficient input validation, testers discover a SQL injection vulnerability.

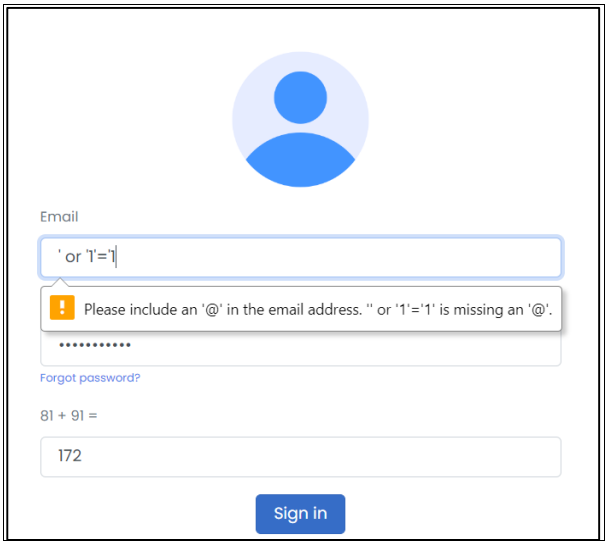

Figure 17: SQL injection attack testing

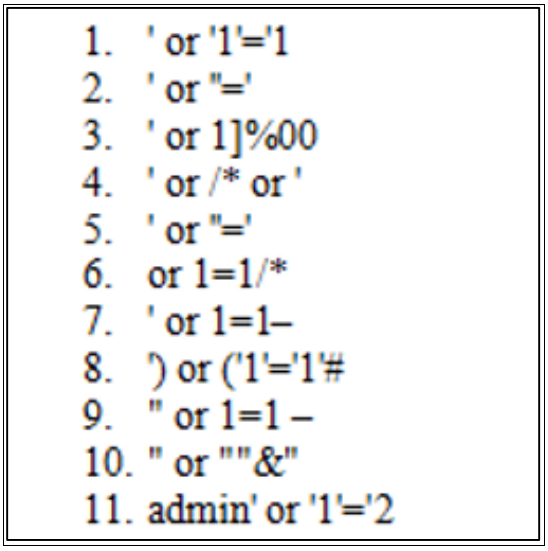

Figure 18: Login Bypass list

Figure 17 shows the sql injection testing being tested on the system. Both username and password are being input with the sql syntax. Figure 18 shows several login bypass lists to test the sql injection authentication. SQL injection syntax cheat sheet is tested. There was an error which was prompted when it was tested with the bypass info. Every time when the syntax of sql injection for instance the ' or '1'='1, it does not accept.

(b) Hashing Document

Online password cracking tool for password protected document are used to test whether the forensics report (pdf) generated can be easily cracked by hackers or not.

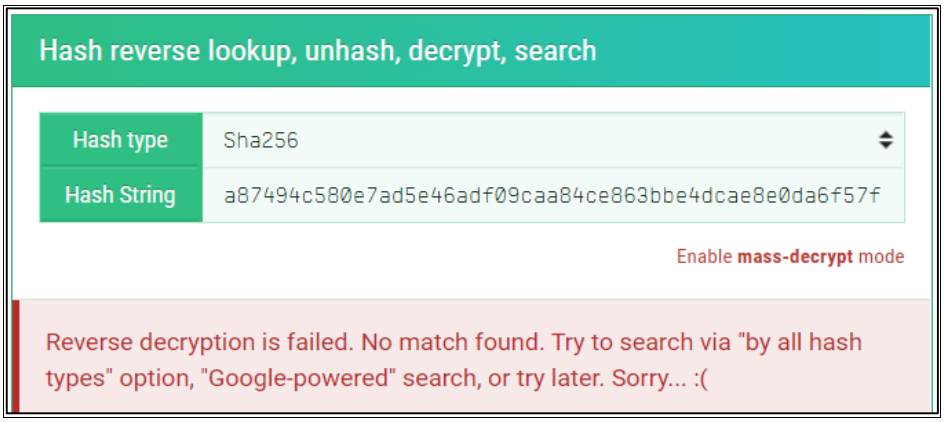

Figure 19: Result using md5hashing.net

Figure 19 shows the md5hashing.net where it is to test if the password protected forensics report (pdf) is able to crack with the online platform. As shown in the screenshot, the pdf decryption is unable to take place.

4.5 User Acceptance Results

User Acceptance Testing (UAT) is one of the last stages of the software development life cycle, and this is where User Acceptance Testing (UAT) comes in. It is carried out after the software has undergone extensive testing. End User Testing is another name for it.

Figure 20 shows the result of the system functionality testing. All users are able to use the function without error. The function of login, reset password, create, and generate report, view reporting lists, encrypt or decrypt forensics report are tested without error and able to perform well.

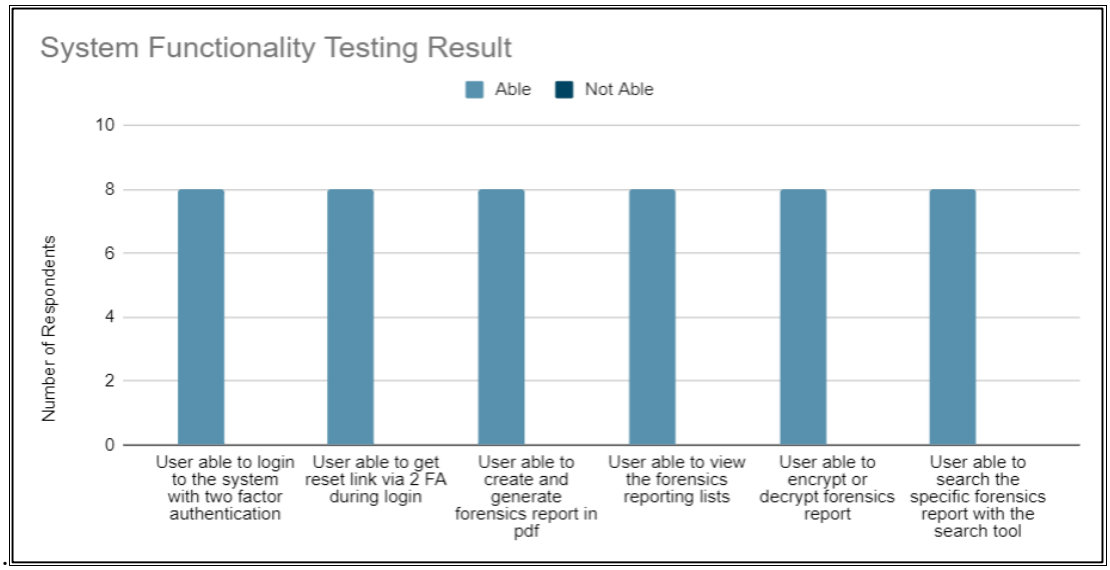

Figure 20: System functionality testing result

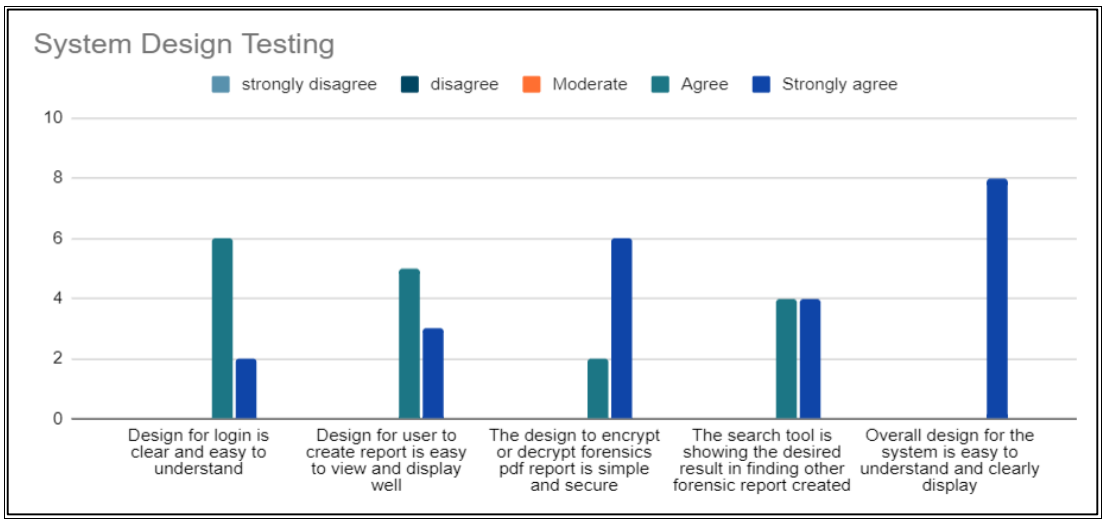

Figure 21: System functionality testing result

Figure 21 shows the result of the system design testing. Six respondents agree, and two respondents strongly agree that the design of login is clear and easy to understand. Five respondents agree, and 3 respondents strongly agree that the design to create reports is easy to view and display well. Two respondents agree and six respondents strongly agree that the design to encrypt or decrypt forensics pdf report is simple and secure. Four respondents agree while the other four respondents strongly agree that the search tool is showing the desired result in finding other forensic reports created. Finally, all eight respondents strongly agree that the overall design for the system is easy to understand and clearly display.

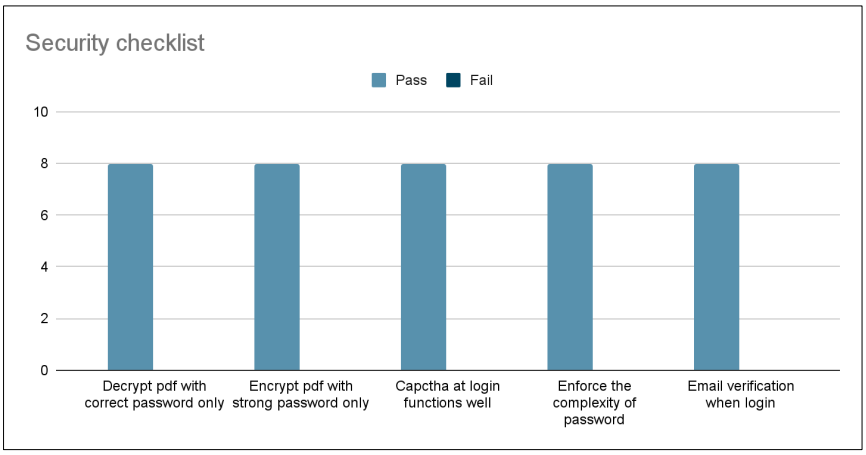

Figure 22: Security testing result

Figure 22 shows the result of the security testing result. All eight respondents answered pass for all security checklists mentioned such as decrypt pdf with correct password only, encrypt pdf with strong password only, Captcha at login functions well, email verification when login.

5. Conclusion

The forensics reporting application allows users to generate a forensics report, encrypt a forensics report with a complex password, and decrypt a forensics report with the correct password. The application has a strong password policy to force users to create a strong password. The application allows users to access the application with two-factor authentication when logging in.

The application has few advantages. The application has a strong password policy to force users to use strong complex passwords. The application has captcha to prevent bots attack. The application has restrictions on login attempts to prevent attackers from trying different passwords multiple times. The application ensures user login into the application via OTP through email registered as a 2 Factor Authentication. The application provides encryption of the generated forensics report pdf file. The application provides decryption of encrypted forensics report pdf file with correct password only.

The disadvantages of the application are as follows. The application does not have a single sign on which is that the identity data takes the form of tokens which contain identifying bits of information about the user like a user's email address or a username. Next disadvantage is the lack of Security monitoring is the automated process of collecting and analyzing indicators of potential security threats, then triaging these threats with appropriate action.

Since the web-based application does not have a single sign on for the user and lacks security monitoring. Hence, for future implementation, the application should implement single sign-on (SSO) to direct the process to access an application and implement security testing.

Acknowledgement

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

References

[1] Bassil, Y. (2012). A Simulation Model for the Waterfall Software Development Life Cycle. *ArXiv, abs/1205.6904*.

[2] Sinha, A., & Das, P. (2021). Agile methodology vs. traditional waterfall SDLC: A case study on quality assurance process in software industry. *2021 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*. https://doi.org/10.1109/iementech53263.2021.9614779

[3] Bourke, Julius & Wessely, Simon. (2008). Confidentiality. BMJ (Clinical research ed.). 336. 888-91. 10.1136/bmj.39521.357731.BE.

[4] Wen, L. (2017). Research on system design and implementation of computer forensics based on Log. *2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC)*. https://doi.org/10.1109/icctec.2017.00090.

[5] Huseinovic, A., & Mrdovic, S. (2018). Comparison of Computer Forensics Investigation Models for Cloud Environment. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. https://doi.org/10.23919/mipro.2018.8400157

[6] Binary Blogger. (2021). *Encrypted PDF: The 5 advantages of high secure files* . Binary Blogger. Retrieved April 8, 2022, from https://binaryblogger.com/2021/07/02/encrypted-pdf-the-5-advantages-of-high-secure-files/

[7] Flaglien, A. O. (2017). The digital forensics process. *Digital Forensics*, 13–49. https://doi.org/10.1002/9781119262442.ch2

[8] Pericherla, S. (2021, September 10). *Digital Forensics Life Cycle - cybersecurity tutorial for Beginners*. My Blog. Retrieved April 21, 2022, from https://www.startertutorials.com/blog/digital-forensics-life-cycle.html

[9] Carnall, D. (1999). Website of the week: Privacy and confidentiality. *BMJ*, *319*(7206), 390–390. https://doi.org/10.1136/bmj.319.7206.390a

[10] Ometov, Aleksandr & Bezzateev, Sergey & Mäkitalo, Niko & Andreev, Sergey & Mikkonen, Tommi & Koucheryavy, Yevgeni. (2018). Multi-Factor Authentication: A Survey. Cryptography. 2. 10.3390/cryptography2010001.

[11] Partha, Srini. (2017). CAPTCHA a simple CAPTCHA-like tool.. 10.13140/RG.2.2.35342.97607.

[12] *About chiteeram*. CHITEERAM SOLUTION. (2014). Retrieved July 13, 2022, from https://chiteeram.com.my/