Applied Information Technology And Computer Science Vol. 4 No. 2 (2023) 175-190

AITCS

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

TCNSyst: A Kindergarten Information Management System for Tadika Cahaya Nurani with Data Anonymization

Khairunniesha Fadzil[1], Nurul Hidayah Ab Rahman[1]*

Faculty of Computer Science and Information Technology,
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2023.04.02.011
Received 02 November 2023; Accepted 06 November 2023; Available online 30 November 2023

Abstract: Digital transformation, often associated with the Industry Revolution 4.0 in the 21st-century, has been implemented by many industries including educational institutions. However, digital information systems could also pose security issues such as privacy leakage. Therefore, an information management system for Tadika Cahaya Nurani with data anonymization is proposed to allow admin and teacher to manage students efficiently while protecting their personally identifiable information (PII). The prototyping model was used as the methodology to develop TCNSyst with five phases which are planning, analysis, design, implementation, and testing. This web-based is developed using Atom software while MySQL as the database using JavaScript, PHP, CSS, and HTML. Overall, TCNSyst has been successfully developed with a login module, manage user module, manage profile module, register user module, manage timetable module, manage subject/class module, manage fee module and attendance module. Generalization technique was applied to address data and income data, while masking out technique was applied to e-mail addresses, phone number and identity card (IC) number data to minimize the risk of data privacy breach.

Keywords: Data Anonymization, Data masking, Generalization, Privacy

1. Introduction

Recently, COVID-19's mandatory lockdown has accelerated digital transformation in the education sector. The need for online management systems has increased at many schools, including Tadika Cahaya Nurani in Mantin, Negeri Sembilan. The management of Tadika Cahaya Nurani uses manual document filling, and it consumes administration time. Also, it increases human errors and data insecurity, especially during registration day. Due to COVID-19, they had been struggling to manage their students remotely in 2020.

However, digital information systems can also pose security risks if insecure databases are applied to web-based systems. Since it is more vulnerable to cyberattacks like privacy leakage, it can cause direct and indirect loss to the web system. Data leakage is a global issue, according to Palo Alto

*Corresponding author: hidayahar@uthm.edu.my

Networks CEO Vicky Ray [1]. For example, Palo Alto Networks reported that the names and proof of compromise of 2,566 organizations were posted on the dark web. In Malaysia, organizations are leaking more sensitive information, according to the United States (U.S.) company. Hence, data privacy guidelines should be considered during management system design and development.

The Personal Data Protection Act of 2010 (PDPA) is an act that provides guidelines to minimize unauthorized access, disclosure, and sharing of sensitive data from the system database [2], [3]. It came into force on 15 November 2013 with the purpose of regulating the processing of personal data in commercial transactions and there are several sectors required to register with the Commissioner's office according to the Personal Data Protection Order 2013 which includes education sector [4]. Therefore, in this study, the development of a web-based system for Tadika Cahaya Nurani Information Management System (TCNSyst) is in line with PDPA guidelines by employing data anonymization, a process of altering classified information irreversibly to protect the privacy of data subjects [5]. Generalization and data masking are two anonymization techniques that have been applied in this study. There are three objectives of TCNSyst development as follows:

1. To design TCNSyst online learning management system with data anonymization approach.
2. To develop TCNSyst online learning management system with data anonymization approach.
3. To test the TCNSyst functionality, security effectiveness by conducting user testing with three target users: admin, teacher, and parent.

The remaining of the paper is organized as follows: Section 2 discusses the literature review of the related work and existing applications. Next, the methodology used to develop the application including the analysis and design is described in Section 3, followed by section 4 that discusses the analysis results of the user acceptance test. Finally, the last section concludes the work and highlights the potential future improvement on the application.

2. Related Work

This section presents relevant study background about related terms of the proposed system, such as information management system, privacy, data anonymization and comparative study of the existing applications with the proposed method.

2.1 Information Management System

An information management system (IMS) is a computer system which is fully implemented in many industries. They store, process, and share information. A data management system also ensures data security and accessibility. For example, finance uses information management systems frequently. These systems store accounting, business, and financial data for later use. If it is needed, the data can be downloaded to generate reports or to give information to customers [6].

This system monitors and stores digital documents and paper document images. It can also track and save user versions. IMS software can also accommodate medical, financial, and other businesses. It can be used for everything from hospital records to customer data and is updated to keep up with information management trends. IMS is a complete set of software, business processes, and technological solutions for data collection, storage, and management [6].

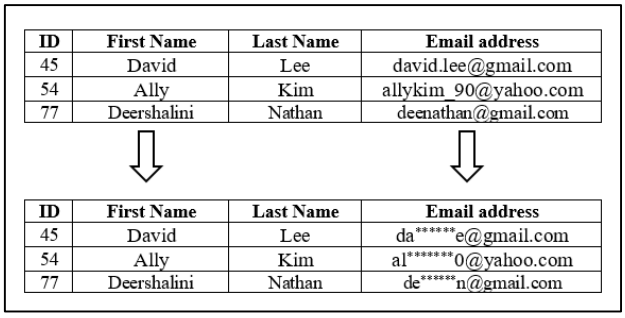
2.2 Data Anonymization

It is critical to protect Personally Identifiable Information (PII) because the trend toward data privacy is growing and alarming. One potential way to safeguard users' privacy is by making user data anonymous before publication such as removing or encoding the identifiers that connect individuals to the stored data.

While maintaining the reliability of the data gathered and exchanged, data anonymization is adopted to safeguard an individual's or business's private activity. Data anonymization methods include data masking, generalization, data swapping, pseudonymization, data perturbation, and synthetic data [7].

2.2.1 Data Masking

Data masking refers to the disclosure of data with altered values (see Figure 1). The process of anonymizing data requires the creation of a database mirror and the implementation of various alteration techniques, such as character shuffling, encryption, word substitution, and character substitution [7]



ID	First Name	Last Name	Email address
45	David	Lee	david.lee@gmail.com
54	Ally	Kim	allykim_90@yahoo.com
77	Deershalini	Nathan	deenathan@gmail.com

ID	First Name	Last Name	Email address
45	David	Lee	da******e@gmail.com
54	Ally	Kim	al*******0@yahoo.com
77	Deershalini	Nathan	de******n@gmail.com

Figure 1: Example of data masking technique

Figure 1 shows character substitution where character representing a value, for instance, could be changed to a symbol such as "*" or "x.". This makes identification or reverse engineering more difficult. The method can be potentially applied to Identification Card (IC) numbers, email addresses, phone numbers, credit card numbers, and Internet Protocol (IP) addresses.

2.2.2 Generalization

Generalization helps in preventing the identification of specific individuals by reducing the level of detail in the data [7]. It is one of the techniques used to balance the need for data analysis and privacy protection. Reorganize the data into intervals or a large region with boundaries. For example, the algorithm may remove the house number from an address, but the lane name must remain.

ID	First Name	Last Name	House address	Postcode
45	David	Lee	Jalan Kinrara 1	35400
54	Ally	Kim	Jalan Bukit Saga 1	71700
77	Deershalini	Nathan	Jalan Amanah 5	81200

Figure 2: Example of generalization technique

Figure 2 illustrates an example of generalization. The purpose of this technique is to remove some of the identifiers while keeping the data as accurate as possible.

2.2.3 Data swapping

Data swapping (see Figure 3), also known as data shuffling or data permutation, reorders the attribute values of a dataset so that they no longer correspond to the original data. Altering columns (attributes) containing known values, such as a person's birthday, can have a substantial impact on anonymization [7]

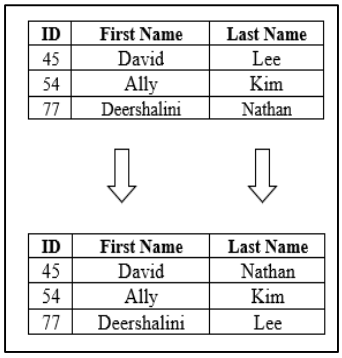


Figure 3: Example of data swapping

Figure 3 demonstrates how the data swapping method operates. The information in the "Last Name" column is randomized. However, using this technique in a small database table is extremely risky, as it will be easier for an attacker to reconstruct the original data using the "What if" scenario.

2.2.4 Pseudonymization

Pseudonymization is a technique for de-identifying data that replaces personal identifiers with fictitious or pseudonymous names as shown in Figure 4 [7].

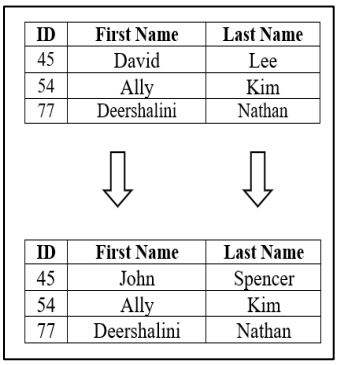


Figure 4: Example of pseudonymization technique

Figure 4 shows this technique replacing "David Lee" with "John Spencer". It preserves statistical accuracy and data privacy, allowing the use of altered data for creation, training, testing, and analysis without compromising data privacy.

2.2.5 Data perturbation

Using rounding and random noise, data perturbation produces minor modifications to the original data set [7] The values employed must correspond to the amount of disturbance employed. It is essential to choose the base that will be used to modify the original values with care. If the base is too small, the data will not be sufficiently altered to ensure anonymity. If the base is too large, the data may not be recognizable or usable.

2.2.6 Synthetic data

Synthetic data is data generated by algorithms that have no relation to actual cases. Instead of using or altering the actual information, which would compromise security and privacy, the information is used to construct fictitious datasets. This data technique employs mathematical systems based on the patterns or characteristics of the original dataset. Using statistical techniques such as linear regressions, standard deviations, and medians, it is possible to generate artificial results [7].

2.3 Study of Existing Systems

In this section, three current information management systems were examined and studied. The goal is to examine the system functionalities and security features that have been implemented. HUBmis, myTNB app and SMAPOnline are the systems that were examined.

A company called WCBS, which specializes in providing management systems to Independent and International schools worldwide, has developed a management information system called HUBmis for independent and international schools across the three core areas of (1) Admissions, (2) Management Information System (MIS), and (3) Finance [8].

Next, Tenaga Nasional Berhad (TNB) created the myTNB app to offer its customers services that are more convenient and easily accessible. By using the myTNB app, users can manage their electricity accounts and gain access to several features related to their level of electricity consumption. Its main goal is to facilitate simpler communication between TNB and its various clientele, and it offers a user-friendly interface in addition to several useful functionalities such as implementation of data masking out for IC number [9].

Table 1: Comparison of Existing System

Attributes	HUBmis	myTNB	TCNSyst	SMAPOnline
Platform	Web	Mobile app	Web	Web
Login page	Yes	No	Yes	Yes
Parents management module	Yes	No	Yes	No
Financial management module	No	No	Yes	Yes
Student information management module	No	No	Yes	Yes
Progress report module	Yes	No	Yes	Yes
Subject management module	Yes	No	Yes	Yes
Timetable management module	Yes	No	Yes	Yes
Terms and condition for data protection complies with PDPA	No	Yes	No	No
Input validation	Yes	No	Yes	Yes

Lastly, SMAPOnline is a Student Academic Information System for Universiti Tun Hussein Onn Malaysia (UTHM) which is in Batu Pahat. It has several modules which are bulletin, biodata, registration, examination, graduation, and student's account. The purpose of this system is to help education institutes and students to store, maintain, compile and process student data, attendance, and academic performance [10].

HUBmis has no financial management module, no student information management module, and the data protection does not comply with the PDPA. myTNB is a mobile application for electricity monitoring therefore it cannot be compared wholly to other systems, however, it has terms and conditions for data protection that comply with PDPA. Surprisingly, none of the existing systems in Table 1 implement it. Lastly, SMAPOnline has no parents' management module and does not comply with the PDPA. Based on the comparative study in Table 1, it can be observed that TCNSyst is able provide most of the basic attributes compared to other systems.

3. Methodology

The model that was adopted in TCNSyst development is the Prototype model. The methodology is widely adopted as it enables the software developer to start with the fewest user requirements possible

[11]. The developer can then gather user feedback, make changes to the system based on that feedback, and change the design of the system. The model is chosen because any changes can be made if the system is still in prototype, and testing can be done once the system prototype is done. The results of the testing can then be used to change the design of the TCNSyst.

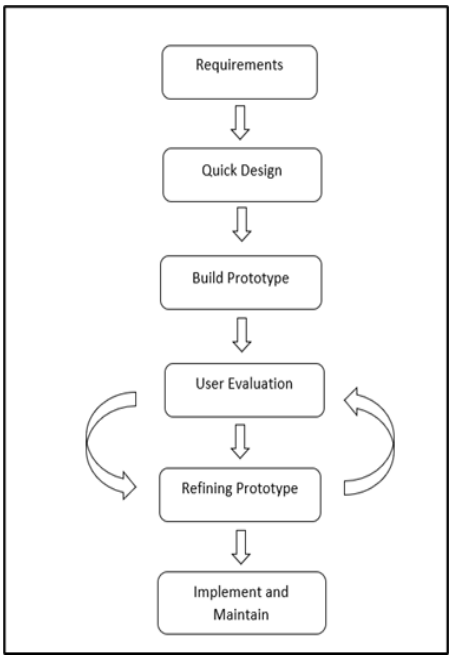


Figure 5: Prototype Model flow

Figure 5 shows the Prototype Model phases. The prototype model is made up of five separate phases: planning, analysis, design, implementation, and testing. The activities and output of each phase from the methodology are presented in Table 2.

Table 2: System Development Activity and Output

Phase	Activity	Output
Planning	● Define problem statement, objectives, and scope. ● Propose the selected title. ● Create project planning and schedule	● Project proposal ● Gantt chart
Analysis	● Do more research on the proposed system. ● Design UML diagrams and STRIDE threat table ● Identify software and hardware needed	● Use-case diagram ● Sequence diagram ● Class diagram ● System architecture ● Activity diagram ● Abuse case diagram ● STRIDE threat model
Design	● Design database ● Develop system user interface and functionality. ● Design pseudo code for generalization and masking out techniques	● Data dictionary ● User interface ● Data anonymization algorithm
Implementation	● Develop and implement prototype. ● End user gives feedback for improvement	● Developed prototype. ● User's feedback
Testing	● Check test plans. ● Identify bugs. ● Evaluate the security features	● User testing ● Application functional testing ● Scenario testing ● Finalized system

Figure 6 shows the interactions between one of the end-users and the system which is admin while Figure 7 illustrates the activity diagram. The admin user will be able to perform tasks such as login and register, update, delete, view, and update data such as teacher and student information, view activity log and more.

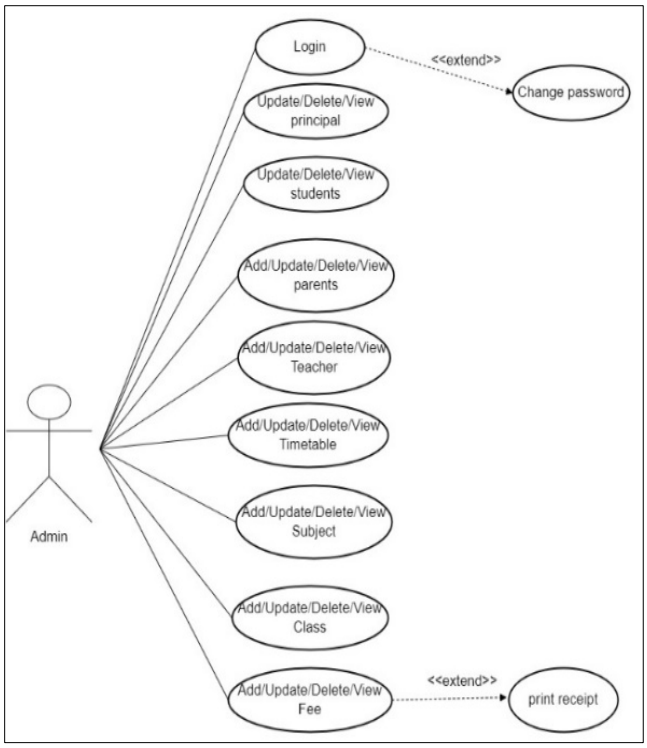


Figure 6: Use case diagram for admin

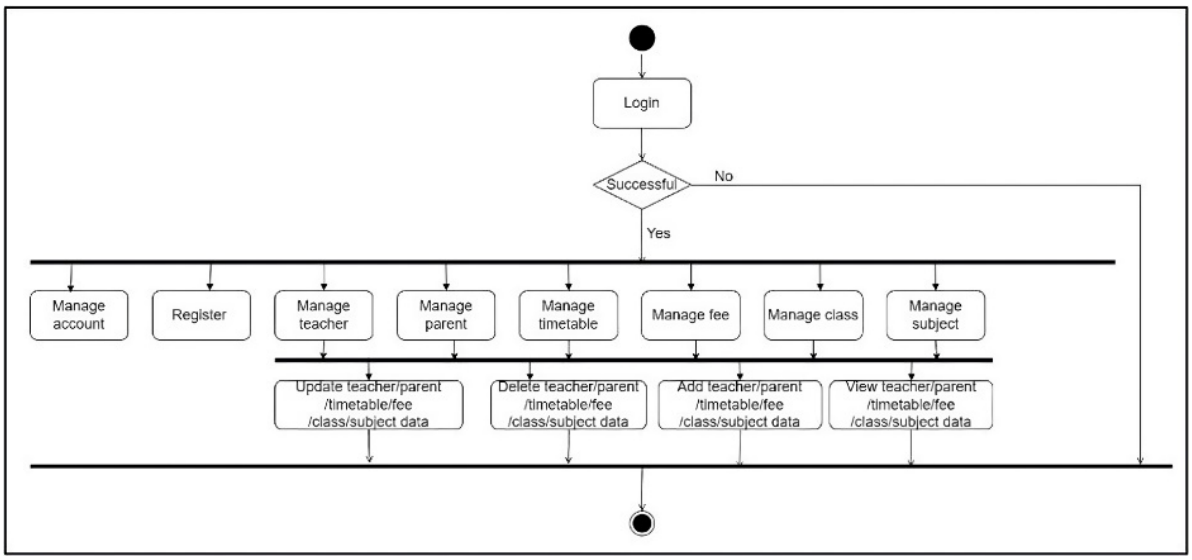


Figure 7: Activity diagram for admin

4. Implementation and testing

This section discusses the implementation phase and the testing phase, which are the final phases in developing the Tadika Cahaya Nurani's Information Management System with Data Anonymization. This phase will explain how the system is developed and evaluated.

4.1 User Interface

The scripting language used for development is Hypertext Preprocessor (PHP), ensuring the smooth functioning of each module. Figure 8 until Figure 12 present the interfaces of the key modules within the Tadika Cahaya Nurani's Information Management System with Data Anonymization.

Figure 8: Login page interface

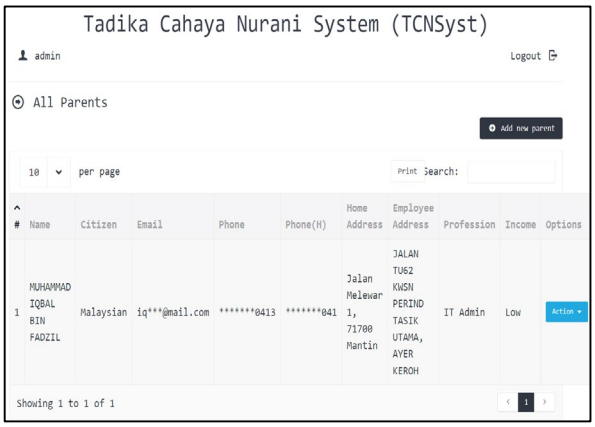


Figure 9: List of all parents' interface

Figure 10: Add parent information interface

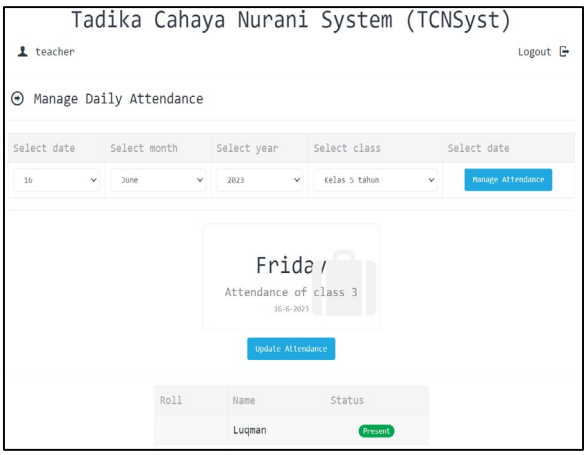


Figure 11: Manage attendance interface

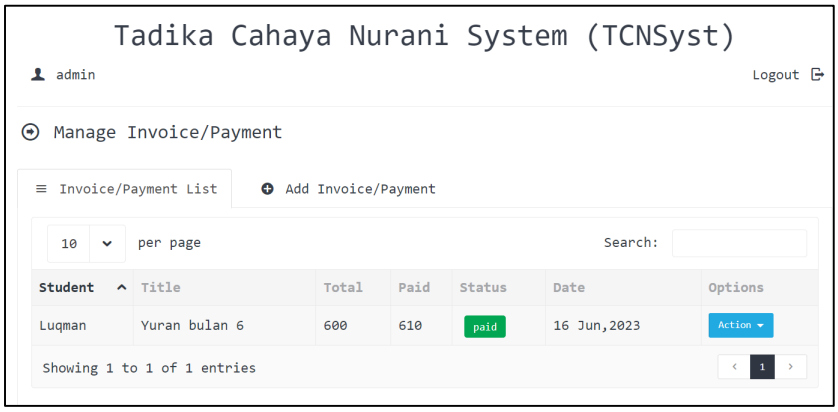


Figure 12: Manage fee interface

4.1.1 Anonymization Techniques

4.1.1.1 Generalization

The user's address and user parents' income are where the generalization method is put into implementation. Only the general address and income will be saved in the database after the user's address has been generalized. The application of the generalization technique to the users' address is shown in Figure 13. Implementing the trim is applied to return street name and postcode so, the address saved in general format instead of the complete address. Comparable results of address generalization were demonstrated in the previous study by Sannasi & Ab Rahman [12]. Subsequently, the risk of privacy linkage attack to TCNSyst using the address data can be minimized, as consistent with Tao et al. [13]. A sample of a generalized address that was saved in the database is shown in Figure 14.

```php
if (!function_exists('mask_address')) {
    function generalize_address($address)
    {
        $address_parts = explode(',', $address);
        $street_name = trim($address_parts[1]);
        $postcode = trim($address_parts[count($address_parts) - 2]);

        return $street_name . ', ' . $postcode;
    }
}
```

Figure 13: Implementation of address generalization

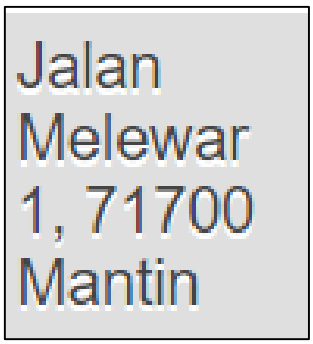


Figure 14: Example of generalized address

Figure 15 shows the application of the generalization technique to the user parents' income. Implementing the code will generalize the income before saved in the database. A sample of a generalized income that was saved in the database is shown in Figure 16.

```php
function generalize_income($income)
{
    // Implement your logic to generalize the income
    if ($income >= 5000) {
        return 'High';
    } elseif ($income >= 2000) {
        return 'Medium';
    } else {
        return 'Low';
    }
}
```

Figure 15: Implementation of income generalization

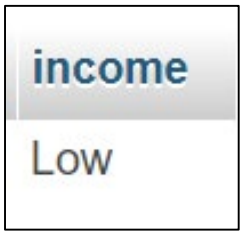


Figure 16: Example of generalized income

4.1.1.2 Masking Out

The IC number and email address are all secured by masking out. Using masking out, the asterisk (*) symbol is used in place of some of the values in the IC number, phone number and email fields as shown in Figure 17 and Figure 18 shows the example of masked out email and IC number. The method is consistent with previous work from Saatci & Gunal [14] and Ratra et al. [15]to protect the privacy of PII. As a result, the risk of attribute correlation attacks against TCNSyst is minimized using data masking.

```php
function mask_email($email)
{
        $maskedEmail = '';

        $emailParts = explode('@', $email);
        $username = $emailParts[0];
        $domain = $emailParts[1];

        // Masking logic for the username
        $maskedUsername = substr($username, 0, 2) . str_repeat('*', strlen($username) - 2);

        $maskedEmail = $maskedUsername . '@' . $domain;

        return $maskedEmail;
}

function mask_phone($phone)
{

    return str_repeat('*', strlen($phone) - 4) . substr($phone, -4);
}

function mask_ic($ic) {
    $masked_ic = substr($ic, 0, -6) . '******';
    return $masked_ic;
}
```

Figure 17: Implementation of masking out

Figure 18: Example of masked out email and IC number.

4.1.2 Other Security Features

4.1.2.1 Strong password credentials

According to the National Institute of Standards and Technology (NIST) Digital Identity Guideline, a strong password should be at least eight characters long and include at least one of each of the following: a digit, uppercase or lowercase letter, a number, a special character, and a special character [16]. If the user's password did not adhere to the necessary pattern, the TCNSyst would not allow the user to register their password.

4.1.2.2 Password hashing

On this web application, hashing is being used on the password. The hashing takes place when a user registers for the first time on this website. The password is hashed using the SHA-256 algorithm's hash function as shown in Figure 19. The SHA-256 algorithm and password hashing are in line with the OWASP's recommended best practices [17].

```php
function mask_password($password)
{
  $hashed_password = hash('sha256', $password);
  return $hashed_password;
}
```

Figure 19: Expression to hash password

4.1.2.3 Input validation

Names, email addresses, phone numbers, and identification card (IC) numbers are the most common inputs that need to be sanitized. An example for validating input of email address is shown in Figure 20. It works by first matching the string value to the regular expression pattern and then comparing the string value with the regular expression.

```php
<div class="form-group">
  <label for="field-1" class="col-sm-3 control-label"><?php echo ('Email');?></label>
  <div class="col-sm-5">
    <input type="email"
    pattern="/^[a-z0-9._%+-]+@[a-z0-9.-]+\.[a-z]{2,4}$/"
    class="form-control" name="email" value="" required>
  </div>
</div>
```

Figure 20: Expression to validate email address

4.2 Testing

Two testing were conducted that are application functional testing and user acceptance testing to make sure the system is functioning well.

4.2.1 Application functional testing

Figure 20 depicts the results of the user testing on the login module interface, while Figure 21 shows a graph related to the testing of the admin page module. Meanwhile, Figure 22 shows the results of user testing on parent page module and Figure 23 represents the graph of user testing on teacher page module which fulfills the user requirements.

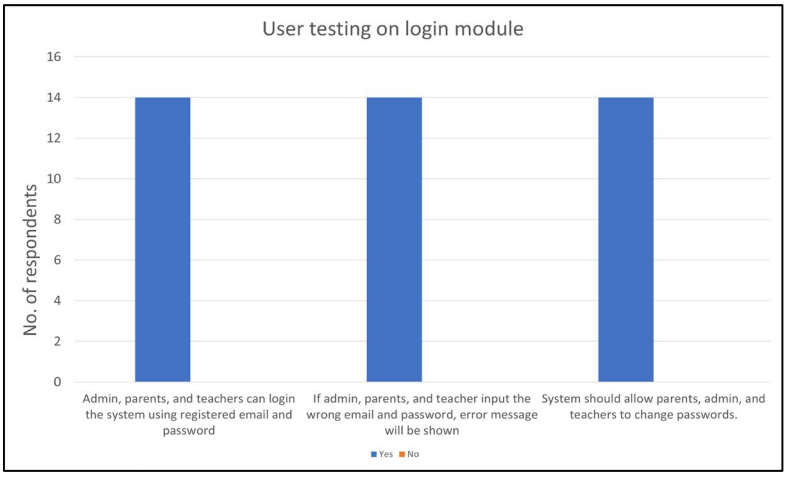


Figure 20: Result of user testing on login module

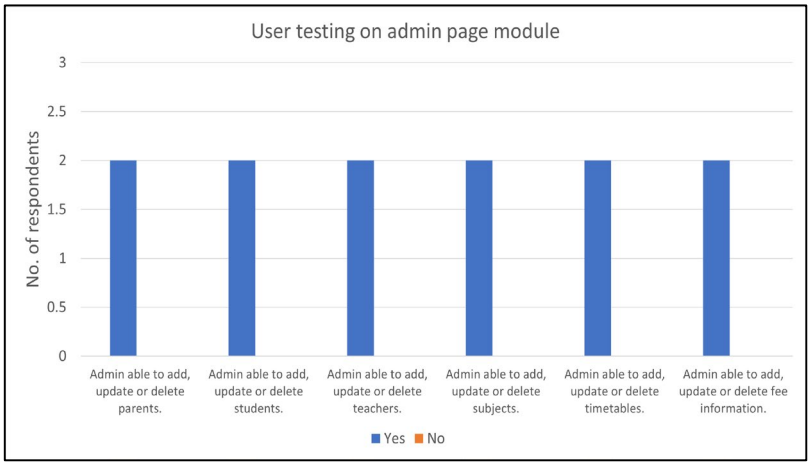


Figure 21: Result of user testing on admin page module

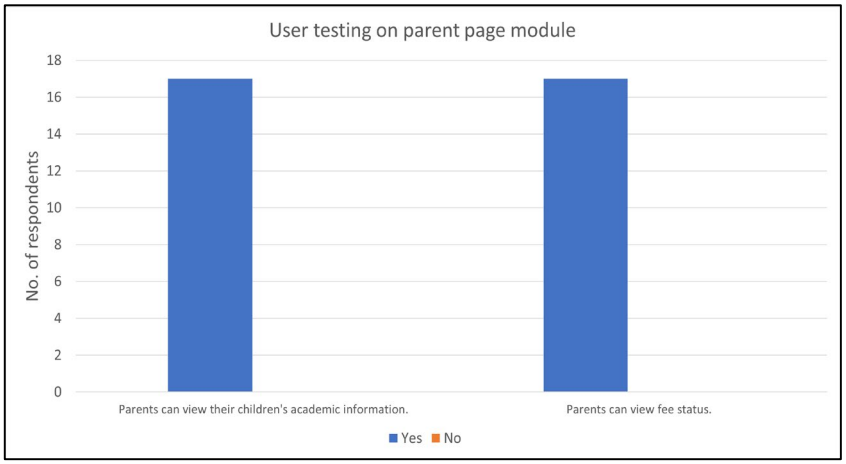


Figure 22: Result of user testing on parent page module

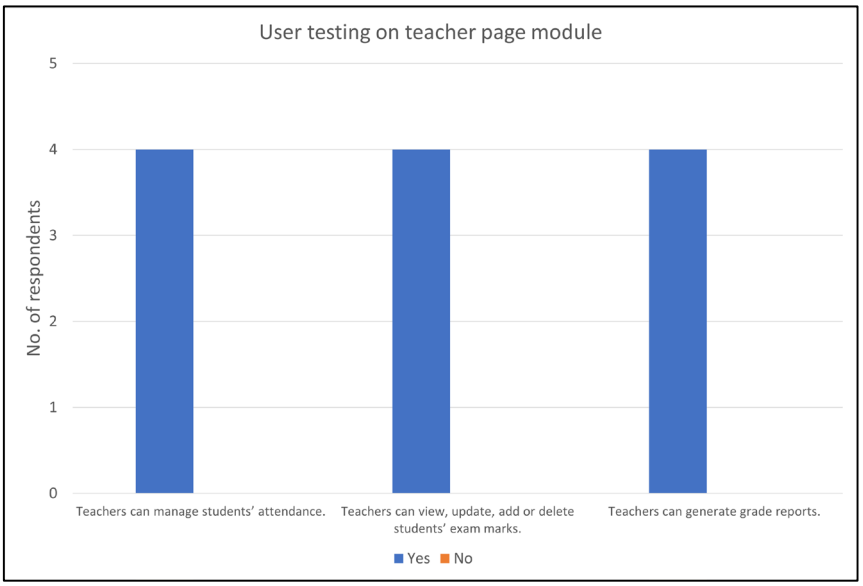


Figure 23: Result of user testing on teacher page module

Table 3 illustrates security effectiveness testing, which is used to confirm and validate the system's security features and evaluate their functionality.

Table 3: Test report of security and anonymization effectiveness

Anonymous security effectiveness testing checklist	Pass	Fail
Only accept strong password – minimum ten characters, must have alphanumeric, special characters, one uppercase and one lowercase	/	
Login attempts are only five attempts before the system is halt	/	
All user input such as user's personal information and marks record is validated	/	
All passwords are hashed	/	
Masked out last six numbers of all IC numbers using asterisk symbol (*) before stored in the database	/	
Masked out first two alphabets and before '@' of email address using asterisk symbol (*) before stored in the database	/	
Generalized income by justify the income range: low, medium, or high before stored in the database	/	
Generalized all address by removing house number, residential area name and state name before stored in the database	/	

4.2.2 Usability evaluation

User testing is a technique used to assess the usability of a system with real users. The purpose of this user testing is to ensure whether the developed system meets and fulfills the users' requirements or not. This testing involves twenty individuals, including the two administrators, four teachers, and fourteen parents. Figure 23 shows the usability evaluation for TCNSyst to assess whether the system meets client's requirements, usability criteria, and suggest improvements and expectations for future works. Based on the results, the system fulfills all the requirements of a kindergarten and target users find the system is easy to use. However, five respondents would like to see improvements and they made a few suggestions.

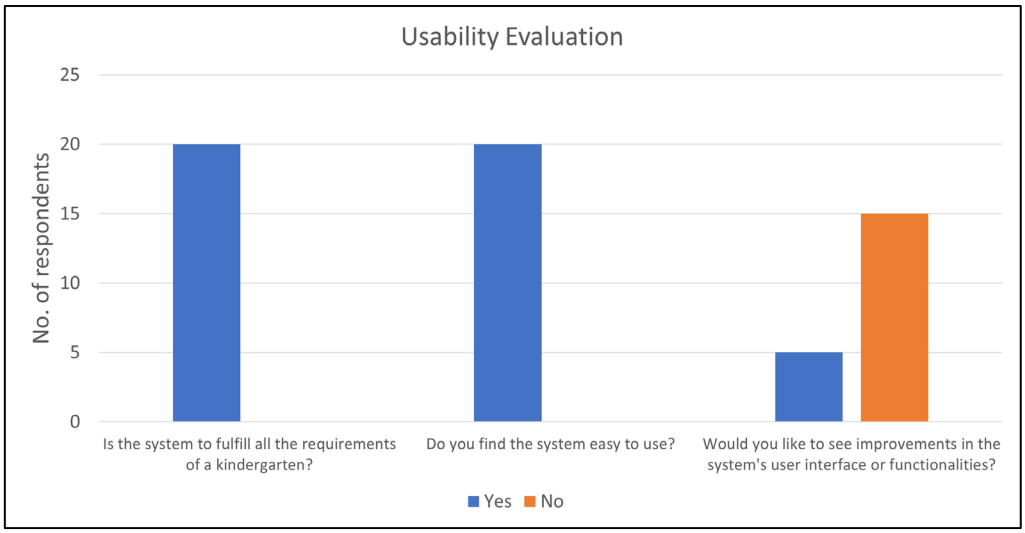


Figure 23: Usability evaluation for TCNSyst

Meanwhile, Figure 24 shows user perception of data anonymization, which transforms data so it cannot be used to identify specific individuals. Data anonymization is perceived differently, as shown in the graph, where only fifteen respondents agree with the general address format and the rest are neutral or disagree. All respondents strongly agree with generalizing address and income and the format. They support data masking for IC numbers and email addresses and the format.

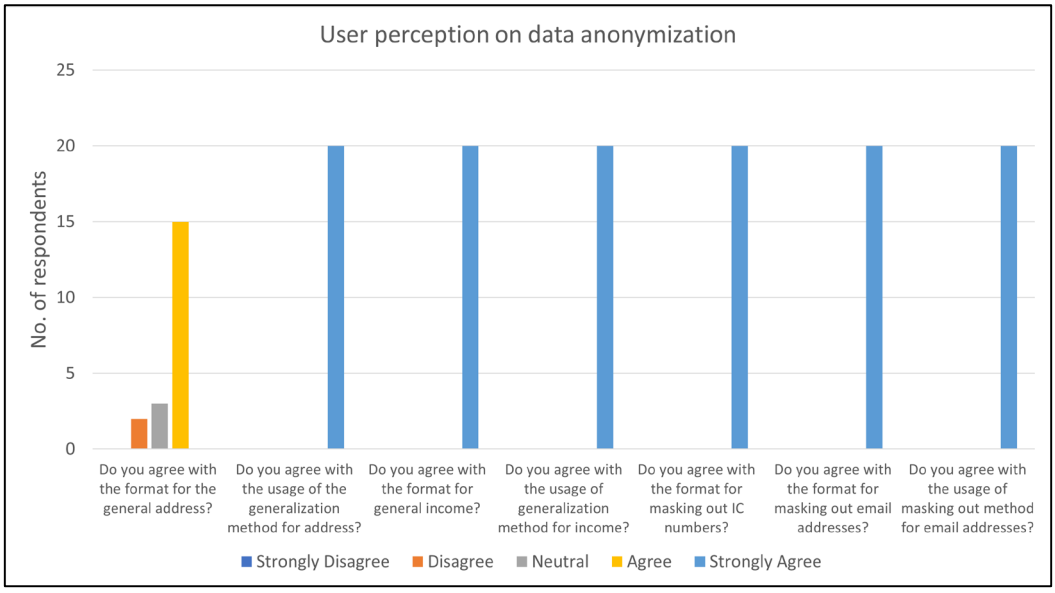


Figure 24: User perception on data anonymization of TCNSyst

5. Conclusion

The Kindergarten Information Management System for Tadika Cahaya (TCNSyst) is designed to effectively manage users' information and ensure the protection of personally identifiable information (PII). The system allows users to create, update, and delete data while implementing anonymization techniques to safeguard PII. Additionally, TCNSyst incorporates password hashing, input validation, and strong password credentials to maintain the system's confidentiality, integrity, and availability.

One of the significant contributions of TCNSyst is data anonymization, which involves masking out and generalizing PII in the user registration records. PII, such as address, phone number, IC number, and email address, is anonymized and stored securely in the database. Furthermore, TCNSyst efficiently manages users, fee payments, and attendance, thus fulfilling its primary functionalities.

TCNSyst offers several advantages. Firstly, it ensures the preservation of user's PII through effective anonymization techniques. Secondly, the system allows for convenient tracking of unpaid fees by recording fee payments. Lastly, TCNSyst efficiently manages and maintains records of students, teachers, and parents' information. However, it also has certain limitations, including the absence of an upload receipt feature, lack of two-factor authentication, no log activity module for admin monitoring, and the absence of auto calculation for unpaid fees.

For future implementation, TCNSyst should consider adding an upload receipt feature, enabling users to provide payment evidence. Implementing One Time Password (OTP) as a two-factor authentication measure on the login page can enhance system security. Additionally, including a log activity module would allow administrators to monitor user activity and detect any unauthorized access or attacks. Furthermore, implementing an auto calculation feature for unpaid fees would assist administrators in efficiently tracking outstanding amounts. Lastly, enhancing the existing security features to protect against new types of attacks should be a priority.

Acknowledgment

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

References

[1] The Edge Markets, “Cybersecurity expert raises alarm over increasing data leaks in Malaysia | The Edge Markets”, Apr. 6, 2022. https://www.theedgemarkets.com/article/cybersecurity-expert-raises-alarm-over-increasing-data-leaks-malaysia (accessed Oct. 09, 2022).

[2] Parliament of Malaysia, “Personal Data Protection Act 2010”, 2010. [Online]. Available: https://www.pdp.gov.my

[3] F. Abdul Ghani, S. Mohd Shabri, M. A. Mohd Rasli, N. Ahmad Razali, and E. H. Ahmad Shuffri, “An Overview of the Personal Data Protection Act 2010 (PDPA): Problems and Solutions,” *Global Business and Management Research: An International Journal*, vol. 12, No.4, 2020.

[4] Office of the Australian Information Commissioner, “What is privacy?”, 2022. https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy (accessed Dec. 03, 2022).

[5] HEAVY.AI, “What is Data Anonymization?”, 2022. https://www.heavy.ai/technical-glossary/data-anonymization (accessed Jan. 09, 2023).

[6] H. Abdul Malak, “What is Information Management System? Why is it Important?”, 2022. https://theecmconsultant.com/information-management-system/ (accessed Dec. 03, 2022).

[7] CFI Team, "Data Anonymization", 2022. https://corporatefinanceinstitute.com/resources/business-intelligence/data-anonymization/ (accessed Dec. 03, 2022).

[8] WCBS, "HUBmis", 2022. https://www.wcbs.co.uk/mis-cloud/ (accessed Nov. 21, 2022).

[9] TNB, "myTNB App", 2023. https://www.mytnb.com.my/mytnb-app (accessed Jun. 17, 2023).

[10] UTHM, "SMAPOnline", 2022. https://smap.uthm.edu.my/ (accessed Jan. 09, 2023).

[11] G. Gurung, R. Shah, and D. P. Jaiswal, "Software Development Life Cycle Models-A Comparative Study," in *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 30–37, Jul. 2020, doi: 10.32628/cseit206410.

[12] T. Sannasi and N. H. Ab Rahman, "MyAttend: A Development of Mobile-based Attendance System with Anonymization Approach to Preserve Location Privacy", *Applied Information Technology and Computer Science*, vol. 3, no. 2, pp. 185–196, 2022, doi: 10.30880/aitcs.2022.03.02.012.

[13] Y. Tao, H. Chen, X. Xiao, S. Zhou, and D. Zhang, "ANGEL: Enhancing the utility of generalization for privacy preserving publication" in *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 7, pp. 1073–1087, Jul. 2009, doi: 10.1109/TKDE.2009.65.

[14] C. Saatci and E. S. Gunal, "Preserving Privacy in Personal Data Processing" in *1st International Informatics and Software Engineering Conference: Innovative Technologies for Digital Transformation, IISEC 2019 - Proceedings*, Nov. 2019, doi: 10.1109/UBMYK48245.2019.8965432.

[15] R. Ratra, P. Gulia, and N. S. Gill, "Evaluation of Re-identification Risk using Anonymization and Differential Privacy in Healthcare," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 2, pp. 563–570, 2022, doi: 10.14569/IJACSA.2022.0130266.

[16] P. A. Grassi, M. E. Garcia, and J. L. Fenton, Digital Identity Guidelines, 2017.

[17] J. Steven, J. Manico, and D. Righetto, "Password Storage · OWASP Cheat Sheet Series", 2023. https://owasp.deteact.com/cheat/cheatsheets/Password_Storage_Cheat_Sheet.html (accessed Jun. 20, 2023).