PURPOSE-LED
PUBLISHING™

**PAPER • OPEN ACCESS**

# Secure Database on Attendance Verification System by using Data Masking Technique

To cite this article: Siti Faizah Miserom *et al* 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1062** 012030

View the article online for updates and enhancements.

# Secure Database on Attendance Verification System by using Data Masking Technique

**Siti Faizah Miserom[1*], Shima Sabri[1,2], Fatin Farina Aida[1] and Noraini Ismail[2]**

[1] Faculty of Computing and Multimedia, Kolej Univesiti Poly-Tech Mara, Jalan 6/91, Taman Shamelin Perkasa, Cheras, 56100 Kuala Lumpur

[2] Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, 21030 Kuala Nerus, Terengganu Darul Iman, Malaysia

*Corresponding e-mail: faizah@kuptm.uitm.edu.my

**Abstract**. Data Masking Technique is a system designed to secure sensitive data by replacing the front data but not the original data. For instance, the data masking techniques capable to hide any data from being viewed by any unauthorized users. However, fewer studies about data masking techniques in the attendance system are implemented. Previous studies have primarily concentrated on defining sensitive data exposure and the technique of securing sensitive data using data masking. Therefore, the aim of this paper is to integrate the use of the data masking technique towards the attendance verification system. Thus, it is sufficient to stop unauthorized users from accessing confidential data. This study also applied the iterative model as a software development methodology as well as integrated with the hashing concept. Therefore, the attendance verification system can be used to perform the functionalities of easily manage records. By using this technique, the attendance of a student was added with a security element. The result shows that data masking and hashing techniques ensure the confidentiality of student data from being viewed by unauthorized parties. The authorized person is the ability to see the masked of sensitive student data. The significance of this study is capable to implement the security element on the attendance system and verify the user before entering the system

Keywords: Data masking; Security; Database; Attendance verification system

## 1. Introduction

Data Masking Technique is a system designed to secure sensitive data by replacing the front data but not the original data. For instance, the data masking techniques capable to hide any data from being viewed by any unauthorized users. However, fewer studies about data masking techniques in the attendance system are implemented. Previous studies have primarily concentrated on defining sensitive data exposure and the technique of securing sensitive data using data masking [1-2]. Therefore, the aim of this paper is to integrate the use of the data masking technique towards the attendance verification system. Thus it is sufficient to stop unauthorized users from accessing confidential data.

This study also applied the iterative model as a software development methodology as well as integrated with the hashing concept. Therefore, the attendance verification system can be used to perform the functionalities of easily manage records. By using this technique, the attendance of a student was added with a security element. The result shows that data masking and hashing techniques ensure the confidentiality of student data from being viewed by unauthorized parties. The authorized person is the ability to see the masked of sensitive student data.

The significance of this study is capable to implement the security element on the attendance system and verify the user before entering the system. With technological evolution, the world has changed drastically. At every age that human beings have gone through various challenges, and need to acquire new inputs. Due to the dean award ceremony previously had no computerized system and the lecturer on duty only use Microsoft Excel as a platform to store student data. Previously, attendance verification goes through Google Form which students are required to fill out the form provided if they want to verify their attendance.

An unauthorized user can read or steal sensitive information [3]. They have no monitoring database system. Sensitive data exposure will occur. There are some security concerns. The leaks of the information can cause a significant problem to the victim, such as loss of institution reputation and credibility, and worse can cause the institution to specific law acts regarding sensitive data protection [2]. Uncertified students can fill out the provided form. Google Form has no restricted access and if they have a connection, anyone can access it. In KUPTM, MPP will provide Google Form links on multiple platforms such as WhatsApp and Twitter for students to verify their attendance to attend the student appreciation award.

Sensitive information is characterized as data that protects against unauthorized disclosure. Confidential data covers all data containing personal information, records of student education, cardholder information, and more [2]. Some examples of data exposure when a person is accidentally uploaded somewhere, poor crypto, meaning an intruder can read the information if they break into the target of the system successfully [3].

The data masking technique is a technique that replaces the realistic data but not the original data [4]. The primary objective of data masking is to ensure that the actual data not exposed from the outside of the environment [2-3]. In general, data masking ensures that only an authorized party can see the original data. Data masking is used to protect multiple types of data, including personal data, protected health data, and financial data, such as payment card information. Therefore, this project is proposed to develop an attendance verification system for the KUPTM student appreciation award with a secure database by using the data masking technique.

This system helps Majlis Perwakilan Pelajar (MPP) easily to manage the record of student attendance verification for student appreciation award. In this system, the student needs to verify their identity first by their ID number. MPP members will register the certified student and only certified students in the list of student appreciation awards can access the system. After that, a student can verify their attendance to attend the student appreciation award by filling the form provided. The MPP can see the student's data. The problem here is that the MPP is also a student, and they should not see the details of the student. With the privileges that colleges give to the MPP, they can misuse their power.

## 2. Methodology

As a cyclical process, the iterative model is best reflected. Design modifications are developed in every iteration, and new functional capabilities are introduced. The basic plan after this method is to develop the system through an iterative cycle and in an incremental part [5]. Improvements can quickly be identified and completed throughout each iteration, moving the next iteration to be at least slightly better than the last [6]. The six stages included in the iterative model are as follows:

### 2.1. Initial Planning

Attendance Verification System for KUPTM Student Appreciation Award with Secure Database by Using Data Masking Technique and will implement the rule-based algorithm. These algorithms are easy to comprehend and expressive algorithms that will extract information from the classification model in the form of rules.

### 2.2. Planning Phase

Through several studies and observations, the problem statements have been identified. It is possible to identify the key discussion of an issue based on an unauthorized person being able to access confidential information.

### 2.3. Requirement Phase

The existing method is analysed and all the requirements that are needed to develop a computerized system are identified. Gathering the requirement of the project with the questionnaire which helps the developer to initiate the development process and at the same time create a mutual understanding of the project objective.

### 2.4. Analysis and Design Phase

Use Case Diagram and Flowchart are designed based on the system requirement.

### 2.5. Implementation and Testing Phase

This system is developed by using PHP, JavaScript, and SQL Server. Three modules were developed which are Administrator module, MPP module, and student module. The module was tested to ensure the system is fully working and meets the requirement.

### 2.6. Evaluation Process

The system is evaluated in the admin section to prove that the student's sensitive data will be secure or not, especially in the part of the data masking technique. Evaluate the system whether MPP can easily handle a list of student attendance verification and students can verify their attendance to attend the student appreciation award without no problem and meets or not in user requirement

### 2.7. Deployment Phase

Once the evaluation is completed, this system is deployed during the student appreciation award announced by the college, so students who are nominated for the award can use the system. The system will be released to the admin to implement whether the system is working properly or not.

As shown in Figure 1, users can test the system and can provide input, which is the involvement of the user more intense positive impact on development. With a prototype, errors and omissions in development can be immediately known. The results can also be received promptly [7]. Furthermore, the model is easier to manage risk, especially the high-risk part. Usually, the high-risk part is done first. Moreover, it also supports changing requirements and supports user feedback.
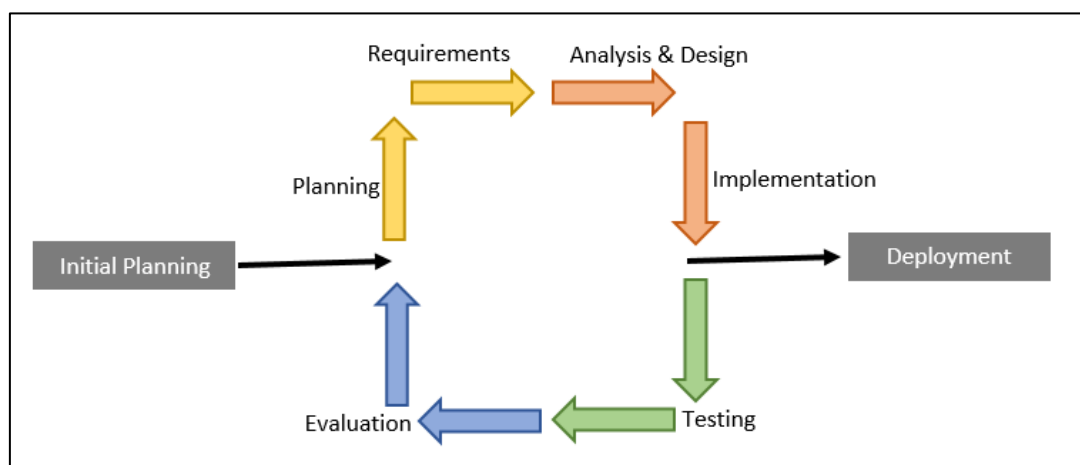


**Figure 1.** Iterative model phases.

## 3. System Design

This section explains the process of the system by using two methods which use case diagram and flowchart. These methods possible to classify accurately the requirements of the designed system and determine users with functions they meet within the system [7].

### 3.1. Use Case Design

The use case diagram shown in Figure 2 shows both interactions between system admin, MPP, and student with Attendance Verification System for KUPTM Student Appreciation Award with Secure Database by Using Data Masking Technique shows the relationship between the admin and users and the different use cases where both parties involved. There are two modules namely the admin site and user site.

In site admin, admin roles areas to login into the system. Admin can register MPP members that have a request to use this system. The admin will also provide a list of certified student names that are eligible for the student appreciation award. So, only the admin system can view the details of the student and only those who can update student data.

The second actor's character is the MPP who is responsible for managing the list of student attendance verification. If the MPP members are assigned a Person in charge (PIC) in managing student attendance verification, they will need to request ID to the admin system. Finally, the student's roles towards the system are that they need to verify their identity using the student ID. This is the reason why MPPs need to register a list of students they got from admins. If identity verification is successful, students will need to fill out the form and verify their attendance to attend the student appreciation award. Only admin and MPP actors can logout as they only go through the system login process.
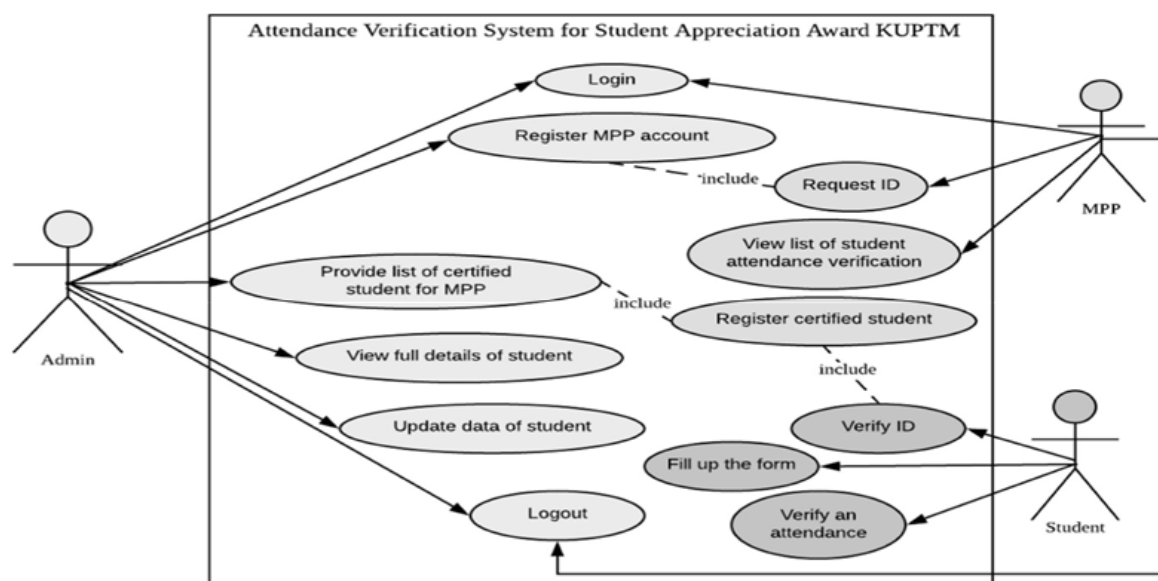


**Figure 2.** Use case diagram of attendance verification system.

### 3.2. Flowchart Design

The flow chart below shows the formalized graphic representation of the system and the development process. It supports the developer to gain a basic language and a reference point when the developer with the project.

Figure 3 present a Flowchart of the Attendance Verification System for KUPTM Student Appreciation Award with Secure Database by Using Data Masking Technique for the admin site. In the site admin, the system flow is to start with the admin will be logged into the system. After that, the admin can make an option where the admin can select the menu. There are two sections: register account

for MPP or view details of the student. If MPP members request an account for them, the admin will register for the MPP. Admins can also view student details if they want and update student data for specific reasons. After finishing the business in the system, admins can go directly to process logout.
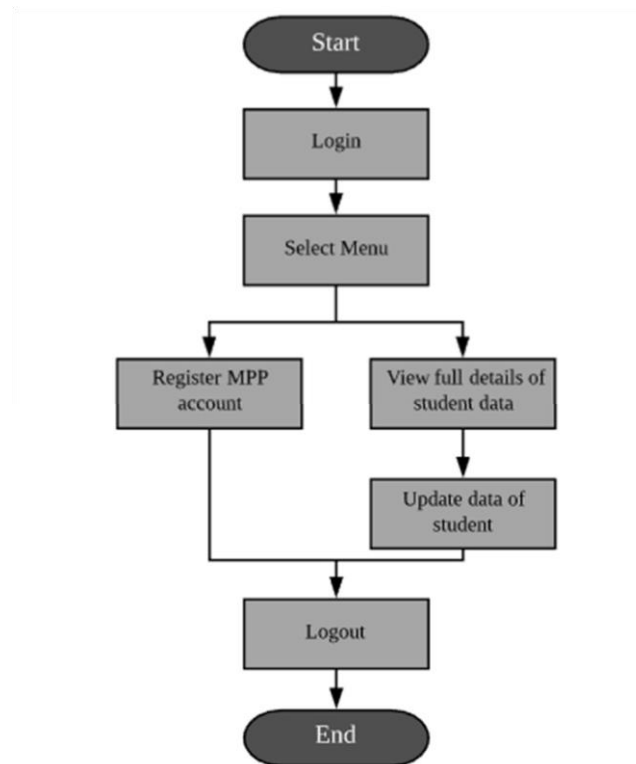


**Figure 3.** Flowchart of admin site.

Figure 4 demonstrates a flowchart of the system of the MPP site who is appointed as a person in charge (PIC) manages the student attendance verification records. PIC does not have an account, they can request the system admin manually to create their account. If the MPP already has its account, they can log into the system. They can also make choices by selecting the menu provided. These include register an account for certified students or view the list of students who have verified attendance. MPP should register a certified student in the list of student appreciation awards that they receive from the admin system. This is to verify student identity later. The admin will provide the list of student names nominated in the student appreciation award list where the MPP receives only the student's name, student ID, and program code. MPP is not allowed to view the full details of students. Only admins can view the details of the student. After the MPP is done in the system, the MPP can log out of the system.

The flowchart illustrated in Figure 5 shows students do not need to have their account for access to the system. Students only need to verify their identity by entering the student ID into the system. If the identity is not verified, the process will end where they cannot access the system. If their identity is verified, meaning that their names have been registered as students who attend the student appreciation nominated for the award. After that, students will go through a process where they have to fill out the form provided. After completion of the form, the student will have to verify the presence of the award and the process for students to end.
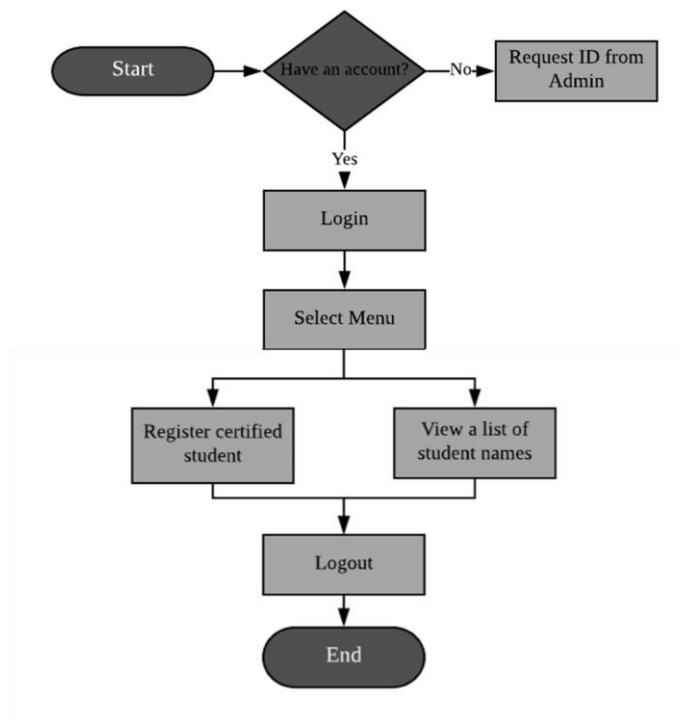
**Figure 4.** Flowchart of the system.
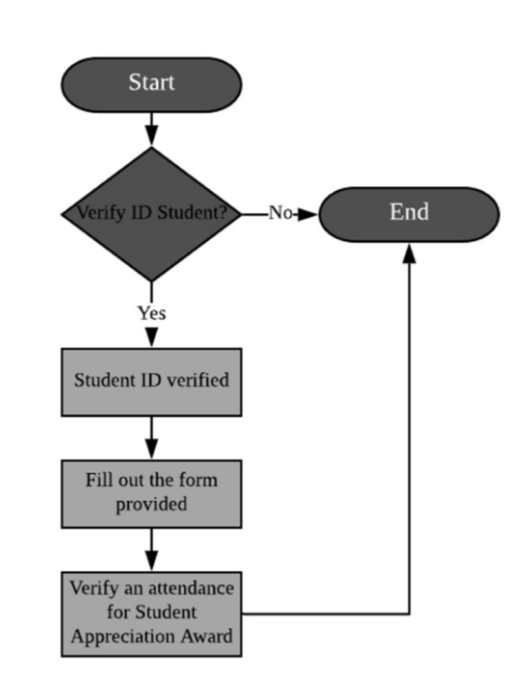


**Figure 5.** Flowchart of the system for student module.

## 4. The Proposed System

The objectives of the proposed system are to secure sensitive student data from being read and stolen by unauthorized parties. Using the Data Masking Technique also helps Majlis Perwakilan Pelajar (MPP) manage the student attendance verification record because the system automatically filters out an uncertified student in the list of student appreciation awards from accessing the system. MPP members may only register students with data provided by the chosen lecturer assigned to handle the event.

All the sensitive student data that has been collected will be masked by using the data masking technique. Only the system admin can see the details of the student. The process of changing or hiding certain data elements within a set of data so that the data structure remains the same while the contents are changed will be applied to the proposed system. This is done to protect sensitive information such as real names, addresses, identity card (IC) numbers, ID students, and so on.

Figure 6 is the main page that will pop-up which includes full information such as date, time, and location of the event. Students need key-in their ID number to verify join the event.

Continue from Figure 6 its will go to interface Figure 7. This form to verify attendance is shown in Figure 7. Students need to enter their IC, CGPA, Email, and Telephone Number. Students are required to answer the three questions details industrial training, attend the event, and transportation options. The last requirement, press the "Submit" button to verify the attendance of the KUPTM Student Appreciation Award.
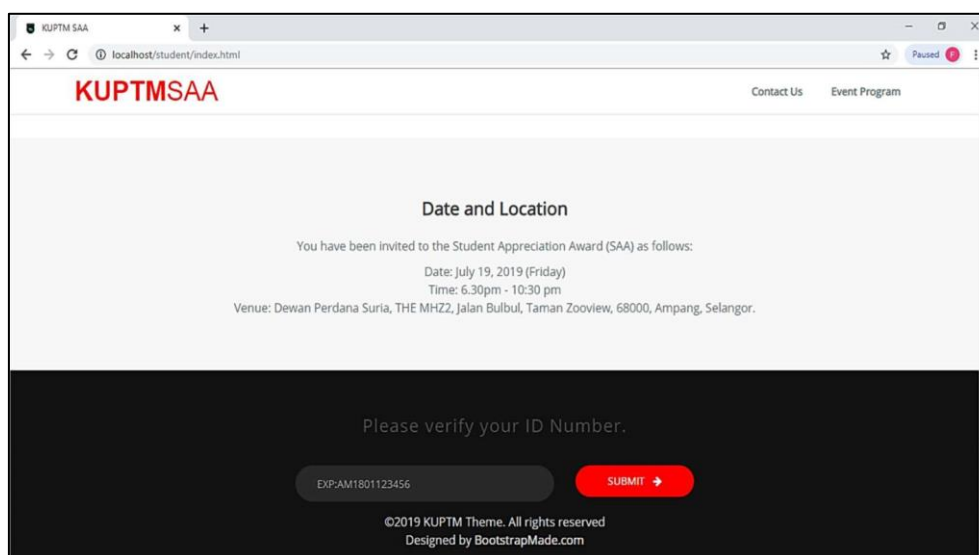


**Figure 6.** Main page.

As shown in Figure 8, Majlis Perwakilan Pelajar (MPP) manage the student attendance verification record student appreciation award from accessing the system. MPP members may only register students with data provided. MPP will enter Student ID, Full Name of student are qualified and Program Code.

**Figure 7.** Verify and update information.



**Figure 8.** Register form by admin.

## 5. Conclusion and Recommendation

Attendance Verification System for the KUPTM Student Appreciation Award with the Secure Database by Using Data Masking Technique do has the limitation and other elements that need to be enhanced and implemented to gain and have the perfect system project. The system would be able to reduce the workload of the KUPTM Student Appreciation Award committee and hasten the process of managing the attendance verification for the event. By using this system, integrate the use of the data masking technique towards the attendance verification system is successful. Based on the result, data masking and hashing techniques can ensure the confidentiality of student data from being viewed by unauthorized parties. The features and elements that will be improving in the future might be as stated below.

The Student Appreciation Award system automatically imported the database of a student who nominated to attend the Student Appreciation Award by the student's CGPA. Also, the system can filter

all students by the previous semester so easy to admin handle the KUPTM Student Appreciation Award through Campus Management System (CMS) and MPP System.

Account verification is essential whenever a new user who is MPP who assigned as Person in Charge (PIC) registered on the admin system. Whenever a new user registers a verification code with the link is sent on the email, and if the user is genuine, MPP clicks on a link with the code sent on their email, and then they verified themselves for the website. Email is more effective, fraud prevention is improved and the ability to protect sender reputation increases.

Compatible mobile view for KUPTM Student Appreciation Award System. Students prefer a simple and user-friendly system. In this way, the attendance confirmation record is quickly available to the MPP. MPP will also do their job efficiently.

## References

[1]  Ajayi O O, and Adebiyi T O 2014 *IOSR Journal of Engineering* **4(2)** 13-21
[2]  Ravikumar G K, Justus R B, Manjunath T N, Ravindra S H and Archana R A 2011 *International Journal of Engineering Science and Technology (IJEST)* **3(6)** 5150-5159
[3]  Santos R J, Bernardino J and  Vieira M 2011 *IDEAS '11: Proceedings of the 15th Symposium on International Database Engineering & Applications* 61–69
[4]  Manjunath T N, Ravindra S H and Ravikumar G K 2010 *International Journal of Computer Science and Information Technologies* **2(1)** 477-485
[5]  Domingo-Ferrer J and Mateo-Sanz J M 2002 *IEEE Transactions on Knowledge and Data Engineering* **14(1)** 189- 201
[6]  Adam N R and Wortmann J C 1989 *ACM Computing Surveys* **21(4)** 515 –556
[7]  Goyal C 2015 *International Research Journal of Management Science & Technology* **6(5)** 221-229