DEVELOPMENT OF STATIC KEYSTROKE DYNAMICS AUTHENTICATION SYSTEM

NG WAN THONG

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: [DEVELOPMENT OF STATIC KEYSTROKE DYNAMICS AUTHENTICATION SYSTEM]

SESI PENGAJIAN: [2022 / 2023]

Saya: ____NG WAN THONG__

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
____✓____	TIDAK TERHAD	

(TANDATANGAN PELAJAR)	(TANDATANGAN PENYELIA)
Alamat tetap: No 38, Jalan Marin2, Taman Marin 84000 Muar Johor	PROFESOR MADYA DR MOHD FAIZAL ABDOLLAH Nama Penyelia
Tarikh: ____21/9/2023_____	Tarikh: 22/9/23

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak

DEVELOPMENT OF STATIC KEYSTROKE DYNAMICS AUTHENTICATION SYSTEM

NG WAN THONG

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Security) with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

DEVELOPMENT OF STATIC KEYSTROKE DYNAMICS AUTHENTICATION SYSTEM

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ _____ Date : 21/9/2023
(NG WAN THONG)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of Computer Science (Computer Security) with Honours.

SUPERVISOR : FAIZAL Date : 22/9/23
(PROF. MADYA. DR. MOHD FAIZAL BIN ABDOLLAH)

DEDICATION

This work is wholeheartedly dedicated to my devoted family, whose unwavering encouragement, compassion, and understanding served as the impetus for finishing this senior project. Your unceasing support, selflessness, and faith in my abilities have kept me inspired throughout the difficult times. This accomplishment is a result of our team's efforts and the tightness of our bond. Thank you for always being there for me, for creating a safe space for me, and for teaching me the importance of perseverance and hard work.

ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude to my family, whose unwavering support and encouragement have been the driving force behind the successful completion of my final year project. Their constant belief in my abilities, patience during my busy schedule, and understanding of the demands of this project have been invaluable. I am truly blessed to have such a loving and supportive family by my side.

I would also like to extend my sincere appreciation to my project supervisor, Prof. Dr. Mohd Faizal Abdollah, for the guidance, expertise, and unwavering commitment throughout this project. His valuable insights, constructive feedback, and dedication to my academic growth have immensely contributed to the quality and outcomes of this project. I am grateful for his time, patience, and mentorship, which have played a vital role in shaping my research and development skills.

This final year project would not have been possible without the collective support, guidance, and encouragement from my family and project supervisor. I am truly grateful for their contributions and the impact they have had on my academic and personal growth.

ABSTRACT

Authentication systems have been widely used in daily life for access control purposes. Unfortunately, the use of usernames and passwords to authenticate users is prone to various password attacks. Today, two-factor authentication systems which utilize both password and biometrics authentication systems can be used to mitigate these vulnerabilities. One of the biometrics types which is mostly unique for every person is keystroke dynamics. The typing patterns are based on the timing information of a key pressed and two successive key pressed. The goal of the project is to build a system which is able to record the keystroke patterns of 10 genuine users to determine if the users can be authenticated accurately by using machine learning. The machine learning algorithm used to build the system is Random Forest. The effectiveness of random forest in user authentication is tested and evaluated.

ABSTRAK

Sistem pengesahan telah digunakan secara meluas dalam kehidupan seharian untuk tujuan kawalan capaian. Malangnya, penggunaan pengguna dan kata laluan untuk mengesahkan pengguna terdedah kepada pelbagai serangan kata laluan. Pada masa kini, sistem pengesahan dua faktor yang menggunakan kata laluan dan sistem pengesahan biometrik boleh digunakan untuk mengurangkan kelemahan ini. Salah satu jenis biometrik yang kebanyakannya unik untuk setiap orang ialah dinamik ketukan kekunci. Corak menaip adalah berdasarkan maklumat masa kekunci ditekan dan dua kekunci berturut-turut ditekan. Matlamat projek adalah untuk membina sistem yang mampu merekodkan corak ketukan kekunci 10 pengguna tulen untuk menentukan sama ada pengguna boleh disahkan dengan tepat dengan menggunakan pembelajaran mesin. Algoritma pembelajaran mesin yang digunakan untuk membina sistem ialah Random Forest. Keberkesanan Random forest dalam pengesahan pengguna diuji dan dinilai.

TABLE OF CONTENTS

PAGE

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

LIST OF ABBREVIATIONS

FAR	**-**	**False Acceptance Rate**
FRR	**-**	**False Rejection Rate**
ROC	**-**	**Receiver Operating Characteristic**
EER	**-**	**Equal Error Rate**
RF	**-**	**Random Forest**
NN	**-**	**Neural Network**
SVM	**-**	**Support Vector Machines**
LR	**-**	**Logistic Regression**
DT	**-**	**Decision Tree**
MLP	**-**	**Multilayer Perceptron**
OCC	**-**	**One-class Classification**
IF	**-**	**Isolation Forest**
OCSVM	**-**	**One-class Support Vector Machines**
LOF	**-**	**Local Outlier Factor**

CHAPTER 1: INTRODUCTION

1.1 Project Background

User authentication system refers to a security mechanism employed to verify the identity of a user before granting the user's access to protected assets. There are multitude of methods to authenticate a user while the most common way is static method which involves the use of password or PIN. Although trustworthy, protected assets are vulnerable to those who gained access once a password or PIN is compromised. Some common password attacks which cause passwords to be compromised are phishing and social engineering, dictionary attacks, brute force, shoulder surfing, keylogging as well as database attacks. Even if a password is not compromised, a password authentication solution still provides a less efficient authentication. According to common password policies, employees should generate a strong password which is a long password with high entropy. Choong et al. (2014) state that employees spend a total of 18.6 hours or 2.25 days within 60 days on generating passwords for their work. Employees spend a lot of time in password generation and thus the time to manage these passwords can grow significantly. The strictness of password policy as security protocol facilitates the chance of login failures.

The use of dynamic authentication system is able to counter the issues. Keystore dynamics authentication is classified as behavioral biometric authentication method which is a part of dynamics authentication. Keystore dynamics authentication provides a backend solution that records the keystroke patterns of the users when they insert their text-based authentication into the system. Keystroke pattern recognition is a more efficient and more secure way to acknowledge the user since keystroke patterns

cannot be easily imitated. To overcome the problem of password authentication which subject to human memory error, passphrase is suggested to be added to the password policy as an additional option for users (Bhana and Flowerday, 2020). A user authentication solution using passphrases and keystroke dynamics can increase both security and usability.

A static keystroke dynamics authentication system specifically runs on an interface instead of continuously recording all the user's interactions with the system. Throughout this project, a static keystroke dynamics authentication system is designed and launched on a login screen. Passphrase is used as a replacement to complex password during authentication.

1.2 Problem Statement

Implementation of static user authentication using username and password to verify user is vulnerable to password attacks. Once a password is compromised, an attacker is authenticated by using the corresponding password and authorized to access protected assets. Besides, due to enforcement of password management and complexity policy, users are encouraged to use strong and complex passwords to mitigate the risk of password attack. A complex password might be difficult to memorize. The authentication process is subject to human memory error. Hence, a static keystroke dynamics authentication system which uses passphrase as login credentials is able to counter the issue. Keystroke dynamics authentication system validates user by checking the user's keystroke dynamics as well as the passphrase at the same time instead of checking at the password only. Keystroke dynamics is unique and not easy to copy. Thus, keystroke dynamics authentication system overcomes the limitation of password authentication system. A summary of problems that influence the motive of the project is shown in Table 1.1.

Table 1.1: Summary of Problem Statement

PS	Problem Statement
PS_1	Static user authentication using username and password as login credentials is vulnerable to password attack.

1.3 Project Question

To counter the problems stated in the problem statement, there is a question that arise and need to be answered in this project. A summary of project questions is shown in Table 1.2.

Table 1.2: Summary of Project Question

PS	PQ	Project Question
PS_1	PQ_1	How keystroke dynamics authentication system helps in avoiding password attack?

1.4 Project Objectives

According to the problem statement and project question highlighted in Table 1.1 and Table 1.2, there are objectives that are aimed to be achieved in this project. These objectives are summarized in Table 1.3.

Table 1.3: Summary of Project Objectives

PS	PQ	PO	Project Objectives
PS_1	PQ_1	PO_1	To investigate the use of static keystroke dynamics authentication as an access control mechanism.
		PO_2	To develop a static keystroke dynamics authentication system using machine learning
		PO_3	To test and validate the accuracy of static keystroke dynamics authentication system.

1.5 Project Scope

The scope of this project is listed as below:

1. To focus on the development and implementation of a static keystroke dynamics authentication system.

2. Normal user is the target user of this project

3. Passphrase from target user as login credential

4. Keystroke pattern of target user

1.6 Project Contribution

The expected outcome of this project which may contribute to the community is stated in Table 1.4.

Table 1.4: Summary of Project Contribution

PS	PQ	PO	PC	Project Contribution
PS_1	PQ_1	PO_1	PC_1	Proposed a suitable machine learning algorithm for keystroke pattern recognition.
		PO_2		
		PO_3	PC_2	Proposed a static keystroke dynamics authentication system.

1.7 Report Organization

Chapter 1: Introduction

This chapter provides an overview of the project. It discusses the project background, problem statement, project question, objectives of the project, project scope, project contribution and report organization.

Chapter 2: Literature Review

This chapter shows how this project relates to existing research. It is mainly about a survey on scholarly sources related to the specific topic of this project. Strengths and weaknesses of past research on the specific topic are discussed and justification is made.

Chapter 3: Project Methodology