KEYLOGGER FOR SECURITY WITH EMAIL AND TELEGRAM ALERT

KEYLOGGER SECURITY SYSTEM

NIK MUHAMMAD HAFIQ BIN NIK ZULKIFLI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: KEYLOGGER SECURITY SYSTEM WITH EMAIL AND TELEGRAM ALERT

SESI PENGAJIAN: SESI 2020/2023

Saya: NIK MUHAMMAD HAFIQ BIN NIK ZULKIFLI

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)

Alamat tetap: No8, Jalan Seri Merdeka 4,Taman Seri Merdeka, Ampang, Selangor

Tarikh: 10/4/2023

(TANDATANGAN PENYELIA)

(NUR AZMAN ABU)

Tarikh: 10/4/2023

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

KEYLOGGER SECURITY SYSTEM WITH EMAIL AND TELEGRAM ALERT

NIK MUHAMMAD HAFIQ BIN NIK ZULKIFLI

This report is submitted in partial fulfillment of the requirements for the
Bachelor of [Computer Science (Software Development)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

[KEYLOGGER IMPLEMENTATION FOR SECURITY WITH EMAIL ALERT

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

STUDENT : ____________________ Date : 10/04/2023
(NIK MUHAMMAD HAFIQ BIN NIK ZULKIFLI)

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 (Software Development)] with Honours.

SUPERVISOR : ____________________ Date : 10/4/2023
(NUR AZMAN ABU)

PM Dr. Nur Azman Abu
Faculty of ICT,
Universiti Teknikal Malaysia Melaka

DECLARATION

DEDICATION

As a tribute to my numerous friends and family members, I am writing my dissertation. To my beloved parents, who have consistently encouraged and motivated me in everything. My gracious managers, thank you for always giving me those brilliant ideas and priceless time to help me finish this year's final project. My friends, who have always encouraged me and provided me with sage advice. I'm grateful. My affection for each of you cannot be quantified in any manner. God's favor be with you.

ACKNOWLEDGEMENTS

I would like to start by expressing my sincere thanks to my supervisor, Pm Dr Nor Azman Bin Abu, who has been my pillar of support and mentor throughout the completion of my thesis. His tolerance and understanding were a huge assistance to me while I worked on this thesis; without them, I would not have been able to finish it. I also want to express my gratitude to my assessor, Dr. Shekh Faisal Bin Abdul Latip, for his evaluation of me and his candid criticism of my research.

Next, I should thank and praise Allah for allowing me to successfully complete this thesis without encountering any mental or physical issues. I'm appreciative of the strength and excitement you've always provided me so I can finish this thesis.

I also want to express my gratitude to my family, especially my parents Nik Zulkfli Bin Nik Ya and Hasnamurni Binti Naba, for their unfailing support and for giving me the time and space I needed to complete my thesis.

In closing, I want to thank everyone who has supported and encouraged me, especially my friends and fellow students. Because of their enthusiasm to share their knowledge and offer assistance, I am more motivated to successfully finish this thesis. By doing so, I would also want to show my thanks to everyone who has ever been into my life because they are all there to teach us something.

ABSTRACT

A keylogger is a rootkit malware that records keystroke events made on the keyboard and put them into log files. As a result, keylogger can collect sensitive data like usernames, PINs, and passwords and communicate with malicious attackers covertly. Even though keyloggers were mostly used for malicious purposes, if we think about it from a different perspective, keylogger is just a system that record keystroke. Therefore, it can also be used for other purposes. It is critical that one out of every a few sizable businesses routinely observes how its unauthorized users use their computers, the internet, or email. Nowadays, there are many solutions that enable businesses to monitor what their employees do while at work on the company computers, in their email, and online. But what do these figures actually mean? What does it actually look like for a corporation to monitor user/employee email, internet, and computer usage? What kinds of computer activities are now hidden from workplace monitoring, and what kinds of computer activities can an organization/company watch users undertake at their computers? This admittedly document attempts to propose, as concretely as possible, a keyloggers system that is implemented for security. This system offers keylogger software used to monitor and record the keystrokes made on a computer keyboard for security purposes. It can be useful in situations where an employer needs to monitor employee activities on company computers or when a person wants to monitor unauthorized use of their computers. The system also has the ability to send email and telegram alerts. With email and telegram alerts, the keylogger can notify you whenever specific keywords or phrases are typed on the keyboard. On top of that, it will also have the feature to capture screenshots of current activity that happened on the computers and send it in the alert email. This security feature can help you stay aware of any suspicious activity, such as unauthorized access attempts or the use of sensitive information. The keylogger system will give an early recorded warning prior to any unauthorized access to designated security personnel.

ABSTRAK

Keyloggers adalah sejenis malware rootkit yang merakam peristiwa penekanan kekunci yang dibuat pada papan kekunci dan memasukkannya ke dalam fail log. Oleh itu, ia dapat mengumpulkan data sensitif seperti nama pengguna, PIN, dan kata laluan dan menyampaikannya kepada penjenayah secara tersembunyi. Walaupun keylogger kebanyakannya digunakan untuk tujuan yang tidak baik, jika kita fikir sebaliknya, keylogger hanyalah sistem yang merakam penekanan kekunci. Oleh itu, keylogger juga boleh digunakan untuk tujuan lain. Ianya penting untuk setiap syarikat pantau jika ada pengguna yang tidak sah menggunakan komputer, internet, atau e-mel. Pada masa kini, terdapat banyak teknik berbeza yang membolehkan syarikat memantau apa yang dilakukan oleh pekerjanya semasa bekerja di komputer syarikat mereka, e-mel , dan perkara yang dilakukan dalam talian. Tetapi apa sebenarnya yang perlu diperhatikan? Bagaimanakah sebenarnya syarikat memantau penggunaan e-mel, internet, dan komputer pekerja? Apa jenis aktiviti yang sedang disembunyikan dari pemantauan di tempat kerja, dan jenis aktiviti komputer apakah yang dapat dilakukan oleh pengguna organisasi / syarikat di komputer mereka? Dokumen ini cuba mencadangkan sistem keyloggers yang digunakan untuk aspek keselamatan. Sistem ini menawarkan perisian keylogger yang digunakan untuk memantau dan merakam ketukan kekunci yang dibuat pada papan kekunci komputer untuk tujuan keselamatan. Ia berguna dalam situasi di mana majikan perlu memantau aktiviti pekerja di komputer syarikat atau ketika seseorang ingin memantau penggunaan komputer mereka secara tidak sah. Sistem ini juga mempunyai kemampuan untuk menghantar amaran e-mel. Dengan amaran e-mel, keylogger dapat memberitahu anda setiap kali kata kunci atau frasa tertentu ditaip pada papan.

TABLE OF CONTENTS

PAGE

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Rom	-	Read-Only Memory
API	-	Application Programming Interface
C2DM	-	Cloud to Device Messaging
VMM	-	Virtual machine management
PS	-	Project Statements
RS	-	Research Questions
RO	-	Research Objectives
PYCA	-	Python Cryptographic Authority
BIOS	-	Basic input/output system
PII	-	Personal Identifiable Information
IDE	-	Integrated Development Environment
SDLC	-	Software Development Life Cycle
SMTP	-	Simple Mail Transfer Protocol
MIME	-	Multipurpose Internet Mail Extensions
KSS	-	Keylogger Security System

LIST OF ATTACHMENTS

Chapter 1: INTRODUCTION

1.1 Background

Unauthorized computer use is becoming an increasingly serious issue in today's digital age. With the widespread availability of technology and the Internet, more and more people are gaining access to computer systems and sensitive information. However, this increased accessibility has also led to an increase in unauthorized access, hacking, and cybercrime. The consequences of such actions can be severe, ranging from financial losses and damage to reputation to legal charges and imprisonment. It is crucial to understand the importance of digital security and to take steps to prevent unauthorized computer use to protect personal and organizational data.

Unauthorized computer use happens because physical access to a computer is often taken for granted, even though it can pose a significant threat to data security and privacy. In today's world, where computers are used for a wide range of purposes and store sensitive information, it has become more critical than ever to safeguard them from unauthorized physical access. Unauthorized access to a computer can lead to data theft, identity theft, and cyber-attacks, causing significant financial losses and reputational damage. It is crucial to implement strict physical security measures to prevent unauthorized access.

Our new technology suggested that to overcome the problem of unauthorized computer use is keylogger software that being implemented for monitoring. Application Programming Interface (API) -based software keyloggers hijack an active application's APIs to record keyboard or keypad inputs. These keyloggers function normally and do not leave any malware-related traces behind. The keystrokes, including key presses and releases, or both, can be recorded and stored (Tianet al., 2017).

In addition, A user does not need to physically access the device after installation while using a software-based keylogger. The software can automatically send logs to a certain location, such an email, because its primary log delivery function allows for this (Shinde & Wanaskar, 2016). Data that is transmitted between the operating system and the keyboard is intercepted by the software keylogger. It captures the keystrokes, transmits them to the us from a distant site, and stores them there (Ahmed et al., 2014)

This keylogger software not only record keystroke made on the keyboard but it also sends an email alert whenever specific keywords or phrases are typed on the keyboard. On top of that, it will also have the feature to capture screenshots of current activity that happened on the computers and send it in the alert email. This will help us to trace if any unauthorized used happened. Although it does not provide a high-level security such as cctv, it is suitable for small/medium companies to provide a medium security level to their physical access to device.

1.2 Project problem Statement

Nowadays, many small companies do not have incomprehensive physical access security for preventing any unauthorized person to use the company computer. The main reason behind this is due to the high installation and maintenance fees for the current monitoring system. This is very dangerous and puts the company at high risk. However, it is very difficult for only security guards to recognize all of the unauthorized and authorized person. Besides, it's time consuming for the guard to monitor a computer's 24 hour just for security reasons.

Furthermore, the current monitoring system did not have any alert being send out when unauthorized access happened. It does not notify the security department immediately or does not provide any application to monitor the system and hence, a quick response action could not be taken promptly to prevent or minimize the loss to the company. It is challenging to deter / provide an early warning and trail to an unauthorized access.

Table 1.1: Summary of Problem Statement

PS	Problem Statement
PS_1	Unable to deter an unauthorized access in real time.
PS_2	No early warning to any probable unauthorized access.
PS_3	Lack of direct trail to an unauthorized access.

1.3 Research Question

The research question for this project was derived from the problem statement in Para 1.2. The summary of research question as shown in Table 1.2

Table 1.2: Summary of Research Questions

PS	PQ	Research Question
PS$_1$	RQ$_1$	How will this system keep monitor the unauthorized access?
PS$_2$		
PS$_3$	RQ$_2$	What is the strategy this system uses to observe the unauthorized access?

1.4 Research Objective

Based on the Research Problem as in Para 1.1 and Research Question in Para 1.2, the objective in the project as derived in Table 1.3

Table 1.3: Summary of Research Objective

PS	PQ		Research Objective
PS$_1$	RQ$_1$	PO$_1$	To thoroughly study and gain a comprehensive understanding of the present state of affairs and progress in the field of keylogging.
PS$_2$			
PS$_1$	RQ$_1$	PO$_2$	To propose a keylogger that monitor, and record keystrokes made on computer for security purposes together with an alerting system.
PS$_2$			
PS$_3$	RQ$_2$	PO$_3$	To test and evaluate the propose keylogger system to detect any unauthorized usage made on the device.

1.5 Project Scope

The scopes of this project are:

i. This project will be done using a personal device.

ii. The keylogger system will record the keystrokes made on a computer keyboard and specific keywords or phrases are typed on the keyboard. If any specific keywords or phrases are typed the system will automatically screenshot the current activity, snapshot the unauthorized user, and record 5 seconds of video for monitoring purposes.
   1. The coding language that will be use is Python and MySQL.

iii. The system sends automatic alerts based on the keystrokes made by the computer and screenshots of the current activity, the typed keystrokes, recorded video, and snapshot will also be sent through emails and telegram.
   1. Develop coding program to send an email and telegram message automatically.
   2. Use smtplib library to send email alerts.
   3. Use telebot library to send telegram alerts.

1.6 Project Contribution

This project is important for any organization that wants to prevent unauthorized access when there is no one to monitor the physical device. Other than detecting unauthorized access, it can help to prevent data loss by reacting fast when the access happened after receiving an alert. This project also can be used or improved by any research to establish a good system for monitoring using different methods. Besides, proper monitoring can provide you with a comprehensive view of your security posture, including all potential threats and vulnerabilities, helping you to better understand and manage your security risks. The benefits of this project are reducing the downtime and administrator can monitor the alert that was sent through