



**Security Enhancements for Person Verification Using  
Multi Model Fusion Keystroke Dynamics and Soft  
Biometrics**

by

**Mohd Noorulfakhri bin Yaacob  
(1643112272)**

A thesis submitted in fulfillment of the requirements for the degree of  
Doctor of Philosophy

**Faculty of Applied and Human Sciences  
UNIVERSITI MALAYSIA PERLIS**

2021

## ACKNOWLEDGEMENT

Alhamdulillah, praise and thanks to Allah ‘Azza wa Jalla for His abundant grace I was able to complete my PhD study and fulfilled the requirements at the Faculty of Applied and Human Sciences (FSGM), Universiti Malaysia Perlis (UniMAP).

I am grateful that all of the predicaments and obstacles encountered during this study were successfully overcome.

Many thanks to Associate Professor Ts. Dr. Syed Zulkarnain bin Syed Idrus Al-Saggoff (Lead Supervisor) and Prof. Dr. Christophe Rosenberger from University of Normandy, France (Co-Supervisor) for their assistances in giving me vital advices during the course of my study. Their dedications in giving me guidance, encouragements and advices will be my lifelong memory.

An unpaid debt of gratitude to Universiti Malaysia Perlis as my employer that had given me their full support by reducing my education costs.

Finally, I would also like to take this opportunity to thank all my family members and friends for their constructive encouragements during the difficult times and crucial situations that I had on completing this study. They are my parents, my wife Siti Masliana binti Bohari, my daughters and all of my good friends who had helped make this study possible.

## TABLE OF CONTENTS

	<b>PAGE</b>
<b>DECLARATION OF THESIS</b>	<b>i</b>
<b>ACKNOWLEDGEMENT</b>	<b>ii</b>
<b>TABLE OF CONTENTS</b>	<b>iii</b>
<b>LIST OF TABLES</b>	<b>vii</b>
<b>LIST OF FIGURES</b>	<b>x</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xiii</b>
<b>LIST OF SYMBOLS</b>	<b>xv</b>
<b>ABSTRAK</b>	<b>xvi</b>
<b>ABSTRACT</b>	<b>xvii</b>
<b>CHAPTER 1 : INTRODUCTION</b>	<b>1</b>
1.1 Background of Study	1
1.2 Problem Statement	8
1.3 Research Questions	10
1.4 Research Objectives	11
1.5 Research Scope	12
1.6 Summary	12
<b>CHAPTER 2 : LITERATURE REVIEW</b>	<b>13</b>
2.1 Introduction	13
2.2 Keystroke Dynamics History	15
2.3 Feature Extraction on Keystroke Dynamics	16

2.3.1	Time Measurement	16
2.3.2	Pressure	24
2.4	Pattern Classification	27
2.4.2	Neural Network	29
2.4.3	Statistical Methods	36
2.4.4	Fuzzy Logic	42
2.4.5	Support Vector Machine (SVM)	44
2.5	Type of Verification in Keystroke Dynamics	48
2.5.2	Short String / Static Verification	49
2.5.3	Session Verification - Continuous Verification	52
2.6	Soft Biometrics	55
2.6.1	Soft Biometrics Application in Keystroke Dynamics	59
2.6.2	Summary of Implementation Soft Biometric in Keystroke Dynamics	61
2.7	Fusion Approach on Keystroke Dynamics	63
2.8	Performance Evaluation	65
2.8.1	Verification Technique	65
2.8.1.1	Statistical Method	66
2.8.1.2	Distance Matrix	66
2.8.2	Classification Techniques	67
2.8.2.1	Data Balance	68
2.8.2.2	Support Vector Machine	70
2.8.2.3	Learning Ratio Performance	71
2.9	Advantages and Disadvantages of Keystroke Dynamics	72
2.10	The Gap in Existing Knowledge	73
2.11	Summary	74
	<b>CHAPTER 3 : METHODOLOGY</b>	<b>75</b>

3.1	Introduction	75
3.2	Proposed Benchmark / Research Design	76
3.2.1	Acquisition Protocol	77
3.3	Identification Approach	78
3.3.1	Individual Profiles Based on The Way of Typing	80
3.3.2	Data Analysis	80
3.3.3	Identification Performance	84
3.4	Verification Approach	85
3.4.1	Data Analysis	85
3.4.2	Benchmarking Score Calculation	88
3.4.3	Score Calculation for Fusion Technique with Soft Biometric Elements	93
3.4.4	Verification Performance	97
3.5	Summary	97
<b>CHAPTER 4 : RESULTS &amp; DISCUSSION</b>		<b>99</b>
4.1	Introduction	99
4.2	Identification Result	99
4.2.1	Result Based on Race	99
4.2.1.1	Chinese versus Indian	101
4.2.1.2	Malay versus Chinese	102
4.2.1.3	Malay versus Indian	104
4.2.1.4	Others versus Indian	105
4.2.1.5	Others versus Chinese	106
4.2.1.6	Others versus Malay	107
4.2.1.7	Summary of Analysis Based on Race	108
4.2.2	Result Based on Region	109

4.2.2.1	Northern versus Southern Region	111
4.2.2.2	Central versus Eastern Region	113
4.2.2.3	Northern versus Central Region	114
4.2.2.4	Eastern versus Southern Region	115
4.2.2.5	Central versus Southern Region	117
4.2.2.6	Northern versus Eastern Region	118
4.2.2.7	Summary Analysis Based on Region	119
4.2.3	Result Based on Education Level Using CGPA	120
4.2.4	Result Based on Gender	122
4.3	Verification Results	123
4.3.1	Benchmarking for User Verification	123
4.3.2	Fusion with Single Soft Biometric Score	125
4.3.3	Fusion with Multiple Soft Biometric Scores	127
4.3.4	Findings for Verification	130
4.4	Summary	131
	<b>CHAPTER 5 : CONCLUSION</b>	<b>132</b>
5.1	Introduction	132
5.2	Summary Results	132
5.3	Contributions	134
5.4	Future Research	135
	<b>REFERENCES</b>	<b>138</b>
	<b>LIST OF PUBLICATIONS</b>	<b>154</b>
	<b>LIST OF AWARD</b>	<b>155</b>

## LIST OF TABLES

	<b>PAGE</b>	
Table 2.1	Summary of previous researches utilizing digraph, trigraph, and N-Graph - time features	22
Table 2.2	Summary of previous researches utilizing pressure as a feature extraction in keystroke dynamics	26
Table 2.3	Summary of previous researches utilizing Neural Network	34
Table 2.4	Summary of previous researches utilizing statistic	40
Table 2.5	Summary of previous researches utilizing fuzzy logic	43
Table 2.6	Summary of previous researches utilizing SVM	46
Table 2.7	Summary of previous research made based on short user input or user verification	51
Table 2.8	Summary of previous research made based on session verification - continuous verification	54
Table 2.9	Summary of the relevant past studies for soft biometric on keystroke dynamics	62
Table 3.1	Criteria involved in this research	76
Table 3.2	Soft biometric classification	82
Table 3.3	Combined soft biometric score for race and region	87
Table 3.4	The overall combination of soft biometric scores with benchmark scores	87
Table 3.5	Fusion level and equation methods to be used for each combination	96

Table 4.1	Texts used in this study	100
Table 4.2	Total number of keystroke analyzed for each class in race	101
Table 4.3	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Chinese versus Indian	102
Table 4.4	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Malay versus Chinese	103
Table 4.5	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Malay versus Indian	104
Table 4.6	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Others versus Indian	106
Table 4.7	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Others versus Chinese	107
Table 4.8	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Others versus Chinese	108
Table 4.9	Summary of average percentages of five sentences from each category by the race for learning ratio between 50% and 90%	109
Table 4.10	Breakdown of the states in Peninsular Malaysia	110
Table 4.11	Breakdown of keystroke records analyzed by region classes	111
Table 4.12	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Northern versus Southern	112
Table 4.13	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Central versus Eastern	114
Table 4.14	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Northern versus Central	115

Table 4.15	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Eastern versus Southern	116
Table 4.16	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Central versus Southern	117
Table 4.17	Summary of the accuracy obtained from 50% to 90% of the learning ratio for Northern versus Eastern	118
Table 4.18	Average percentages of five sentences from each category by the region for learning ratio between 50% and 90%	119
Table 4.19	Summary of the accuracy obtained from 50% to 90% of the learning ratio for educational level - $CGPA \geq 3.0$ versus $CGPA < 3.0$	121
Table 4.20	EER obtained for benchmark computation for each sentence	124
Table 4.21	EER results for user verification obtained by combining the keystroke dynamics with soft biometric elements using Equation (3.1)	126
Table 4.22	EER results for user verification obtained by combining the keystroke dynamics with soft biometric elements using Equation 3.3	129
Table 4.23	Comparison of EER readings based on benchmark, single fusion and multiple fusion.	130

## LIST OF FIGURES

	<b>PAGE</b>
Figure 1.1 Cyber threat reports by MyCert (CyberSecurity, 2019)	4
Figure 1.2 Examples of biometric modalities that can be used to authenticate the users	7
Figure 2.1 Tree diagram for literature review	14
Figure 2.2 Dwelling time and flight time	17
Figure 2.3 Relationship between FAR, FRR and EER (Bajaj et al., 2013)	28
Figure 3.1 Process flow of the identification system	79
Figure 3.2 Shows the breakdown number of volunteers participated according to race fragments	83
Figure 3.3 Shows the breakdown number of volunteers participated by region fragments	83
Figure 3.4 Shows the breakdown number of volunteers participated according to the gender fragments	83
Figure 3.5 Shows the breakdown number of volunteers participated according to the CGPA fragments	83
Figure 3.6 Overview of the multi model fusion to be used in the study	90
Figure 3.7 Shows the process of calculating the mean and standard deviation	91
Figure 4.1 Average accuracy versus learning ratio (Chinese versus Indian)	101

Figure 4.2	Average accuracy versus learning ratio (Malay versus Chinese)	103
Figure 4.3	Average accuracy versus learning ratio (Malay versus Indian)	104
Figure 4.4	Average accuracy versus learning ratio (Others versus Indian)	105
Figure 4.5	Average accuracy versus learning ratio (Others versus Chinese)	106
Figure 4.6	Average accuracy versus learning ratio (Others versus Malay)	107
Figure 4.7	Average accuracy versus learning ratio (Northern versus Southern)	111
Figure 4.8	Average accuracy versus learning ratio (Central versus Eastern)	113
Figure 4.9	Average accuracy versus learning ratio (Northern versus Central)	114
Figure 4.10	Average accuracy versus learning ratio (Eastern versus Southern)	116
Figure 4.11	Average accuracy versus learning ratio (Central versus Southern)	117
Figure 4.12	Average accuracy versus learning ratio (Northern versus Eastern)	118
Figure 4.13	Average accuracy versus learning ratio (CGPA $\geq 3.0$ versus CGPA $< 3.0$ )	120
Figure 4.14	Average accuracy versus learning ratio for gender category (Male versus Female)	122

©This item is protected by original copyright

## LIST OF ABBREVIATIONS

AaMLP	Auto Associative Multilayer Perceptron
ANN	Artificial neural networks
ATM	automated teller machine
BMI	Body mass index
BPPN	Back Propagation Neural Network
BRF	Balanced Random Forest
CER	control event rate
CGPA	Cumulative Grade Point Average
CMU	Carnegie Mellon University
CPU	Central Processing Unit
DA-SVM	Deformable Adaptive
DNA	Deoxyribonucleic Acid
DNN	Deep Neural Networks
DT	Dwelling Time
EEG	Electroencephalogram
EER	Equal Error Rate
FANN	Fast Artificial Neural Network
FAR	False Acceptance Rate
FNMR	False Non-Match Rate
FMR	False Match Rate
FRNN-VQRS	Fuzzy-Rough Nearest Neighbor Vaguely Quantified
	Rough Set
FRR	False Rejection Rate
FT	Flight Time
GREYC	Groupe De Recherche En Informatique, Image, Automatique Et Instrumentation De Caen
GMM	Gaussian Mixture Model
HMOG	Hand Movement, Orientation, And Grasp
HSDPA	High-Speed Downlink Packet Access
IBM	International Business Machines
ID	Identification
IT	Information Technology
ICT	Information and Communication Technology
MB	Megabyte
MR	Malaysia Race

MFN	Multilayer Feedforward Network
MLP	Multilayer Perceptron
PMT-SVM	Projective Model Transfer
PNN	Probabilistic Neural Network
PP	Press-Press
PR	Press-Release
PUC	Pairwise User Coupling
RAM	Random-Access Memory
RBF	Radial Base Function
RBFN	Radial Basic Function Network
RF	Random Forest
RNN	Recurrent Neural Network
ROC	Receiver Operating Characteristic
ROS	Random Over Sampling
RP	Release-Press
RR	Release-Release
RUS	Random Under Sampling
SMD	Scaled Manhattan Distance
SMOTE	Synthetic Minority Oversampling Technique
STD	Standard Deviation
SVM	Support Vector Machine
UED	Using End-User Development
UKKL	Up-Up Keystroke Latency
USB	Universal Serial Bus
VCS	Verification Combine Score

## LIST OF SYMBOLS

SBc	Soft Biometric Class
SBs	Soft Biometric Score
SBv	Soft Biometric Value
$\sigma$	Standard Deviation
$\mu$	Mean
VCS	Verification Combine Score
Ds	Distance Score
SBz	Total Soft Biometric Value

©This item is protected by original copyright

## Pemantapan Keselamatan Untuk Pengecaman Manusia Menggunakan Gabungan Pelbagai Model Bagi *Keystroke Dynamics* Dan Biometrik Lembut

### ABSTRAK

Biometrik digunakan sebagai pagar keselamatan utama di dalam sistem komputer. Biometrik yang terdapat pada diri manusia ini boleh dikategorikan kepada tiga jenis iaitu biologikal, tingkah laku dan morfologi. Kajian ini memberi fokus kepada biometrik tingkah laku iaitu dengan mengkaji berkaitan dinamik ketukan kekunci (*Keystroke dynamics*). *Keystroke dynamics* digunakan sebagai pengesahan peringkat kedua untuk keselamatan sistem yang menggunakan papan kekunci sebagai kawalan akses. Biometrik lembut pula adalah satu kaedah di mana kita dapat mengenalpasti identiti manusia berdasarkan ciri-ciri fizikal atau tingkah laku seseorang yang terhasil secara semulajadi. Masalah yang biasa dihadapi dalam pencerobohan sistem adalah apabila sistem gagal mengenalpasti pengguna sebenar yang masuk ke sistem setelah menggunakan kata kunci yang tepat. Maklumat seseorang pengguna boleh dicuri, diteka dan direkodkan oleh perisian khas menggunakan *keylogger*. Berkemungkinan juga terdapat pengguna yang mampu mencerooboh ke dalam sistem dengan menggunakan kaedah serangan *brute-force* and serangan kamus (*dictionary attacks*). Bagi memastikan dan meningkatkan proses pengesahan pengguna yang menggunakan papan kekunci sebagai kaedah memasuki sistem, kajian ini menggunakan kaedah gabungan pelbagai model bersama *Keystroke dynamics* dan biometrik lembut. Kajian ini memperkenalkan beberapa elemen-elemen biometrik lembut iaitu kaum, tahap pengajian, kawasan dan jantina di dalam *Keystroke dynamics*. *Keystroke dynamics* digunakan bagi membezakan corak menaip bagi setiap kategori ini dan seterusnya ciri-ciri biometrik lembut ini digunakan untuk meningkatkan lagi proses pengesahan pengguna. Formula matematik seperti purata, sisihan piawai dan *Scale Manhattan Distance* telah digunakan untuk mencapai nilai skor penyamar dan pengguna yang sah. Kaedah gabungan pelbagai model telah diperkenalkan dengan mengintegrasikan nilai skor beberapa elemen biometrik lembut dari klasifikasi dengan skor yang diperolehi dari penyamar dan pengguna sebenar bagi menambahbaik proses pengesahan. Bagi tujuan identifikasi, kaedah pengkelasan Mesin Sokongan Vektor digunakan untuk pengkelasan biometrik lembut. Hasil ujian yang diperolehi menunjukkan perbezaan yang ketara pada corak menaip bagi kategori kawasan. Ketepatan tertinggi yang diperolehi adalah 91.17% bagi kategori kawasan. Kawasan ralat yang sama yang diperolehi dari kaedah gabungan pelbagai model adalah 11.33% dengan menggabungkan empat ciri biometrik lembut iaitu jantina, kaum, kawasan dan tahap pendidikan di dalam proses pengesahan. Secara keseluruhannya didapati proses gabungan pelbagai model yang diperkenalkan ini telah membantu mengurangkan nilai kawasan ralat yang sama bagi tujuan pengesahan pengguna di dalam *Keystroke dynamics*.

## **Security Enhancements for Person Verification Using Multi Model Fusion Keystroke Dynamics and Soft Biometrics**

### **ABSTRACT**

Biometric is used as a main security fence in a computer system. Human's biometrics can be categorized into three types: morphological, biological and behavioral. This study focuses on behavioral biometric by studying keystroke dynamics. Keystroke dynamics is used as the user's second level verification for the systems that use the keyboard to login into a system. Soft biometric is a method by which we can identify human identity based on the physical characteristics or behaviors of a person that are naturally produced. A common problem of system intrusions is that the system fails to identify the real user who signs in using the keyboard when the login is correct. A user's login information can be stolen, guessed, and recorded by special software such as a keylogger. There is a possibility that someone else tries to break into the system by using brute-force and dictionary attacks. To ensure and improve user's verification who use the keyboard to enter their logins into the system, this study has used multi model fusion methods to combine keystroke dynamics and soft biometric. This study introduces new soft biometric elements in keystroke dynamics that is gender, race, region and educational level. Keystroke dynamics is used to distinguish typing patterns in each of these categories and uses these soft biometric features to further enhance the verification capabilities. Mathematical formulas such as mean, standard deviation and Scale Manhattan Distance have been used to obtain the score of the imposter and genuine user. Multi model fusion methods have been introduced by integrating the score values of several soft biometric elements from classification with scores obtained from imposter and genuine user to improve the verification process. For identification purposes, Support Vector Machine classification method is used to perform this classification for soft biometric identification. The results show that there are significant differences in the typing pattern in the region category. The highest accuracy achieved is 91.17% in this classification process for the region category. Equal error rate (EER) obtained from a multi model fusion approach is 11.33%. which is to incorporate four features of soft biometrics (gender, race, region and educational level) into the verification process. Overall, it is found that the multi fusion process introduced has managed to reduce the EER values for the purpose of verification in keystroke dynamics.

## CHAPTER 1 : INTRODUCTION

### 1.1 Background of Study

The developments in the field of Information and Communication Technology (ICT) have begun drastically during the mid 1990s since the introduction of the Internet worldwide. At this present day, almost every system that ever developed would require an Internet connection as the core of their systems (Sunyaev, 2020). With the existence of Internet technology, users are now able to access information they need immediately and easily using personal computers or mobile phone via latest broadband technology such as 3G, Streamyx, Unifi and High-Speed Downlink Packet Access (HSDPA).

Alongside with the advancement of the Internet, developed nations are also associated with the advanced computing systems such as e-governments, e-commerce, and e-medicine. These systems are meant to execute critical tasks in managing data, which mostly are confidential residing in the accounting information systems, military control systems and patient information systems (Gupta et al., 2020; Patnala et al., 2020). Most systems with these confidential information have certain security features to secure data. Nonetheless, user verification is the main security measure deployed for each system to safeguard access to any systems. This shows the importance of computer security in the process to secure vital information.

Computer security also known as Information Technology (IT) security or cyber security includes protection and defense of important information in a system against

being hacked or exposed to users without authorities to that information (Gasser, 1988).

Thus, computer security can be categorized into three main parts:

**i Hardware Security**

Hardware security protects against any potential security risk and vulnerability using the hardware being used by an application system. For example, security of a storage device. Every data stored in storage devices must be encrypted (Fadiheh et al., 2019; Riazi et al., 2020).

**ii Network Security**

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment. (Abdulrahman & Jumaa, 2016)

**iii Software Security**

Software security is a process to control programming during system development so it would not be easy to hacked into or get attacked by outsiders (van Oorschot, 2020).

Combination of all these three security aspects are very important to secure entire confidential information inside a system. Intruders will always peek upon vulnerability of each aspect before carrying out any attacks. Therefore, thorough and deep research on each aspect is needed to ensure data safety from being hacked or abused. Various hardware have been introduced to help reduce the risk of cyber attacks. Multiple hardware products known to help stop cyber attack are RazorGate, SurfControl, NetEnforcer, Fortinet, Bluecoat and Cisco IronPort Web Security (Edward, 2019). All these devices utilize latest technologies to enable them to operate well.

Despite multiple methods introduced, research and new technologies to secure computers against intrusion, where cases are still being reported until now (Patrick & Fields, 2017). Attack and intrusion on computer systems became the main issue and agenda on data security. Report by Anti-Phishing Working Group shows that as many as 146,994 phishing attacks occurred from April to June 2020 (Aaron, 2020). Phishing is a method employed by cyber criminal to steal personal information using a combination of malware and social engineering. Most current malware designs utilize social engineering methods to deceive users.

Cyber criminals also trap Internet users by stealing their identity such as obtaining their users' identification (ID) from a particular system. They would deceive their victims via fake emails sent to the users. Subsequently, these cyber criminals would use stolen identities to obtain other confidential data and information (Dastbaz et al., 2018). The followings are the latest reports on intrusion incidents globally in general:

- i Dropbox - Online storage provider company reported that up to 68 million email and password were stolen by hackers since 2012 (Jones, 2016).
- ii Email attacks - News on 27 September 2016 reported that government of United States will be taking actions against cyber intruders trying to access Gmail accounts of the White House personnel (Jones, 2016).

Malaysia is also not spared from cyber threats. According to the reports produced by MyCert, up until December 2019, reports on computer security threats have not been reduced, since the record began in 1997 (CyberSecurity, 2019) . Various computer threats and attacks have been reported and recorded. Figure 1.1 shows the report on threats produced by MyCert as of December 2019, where there are nine categories of cyber threats recorded by the agency. This proves that the research on improving computer security are still needed.

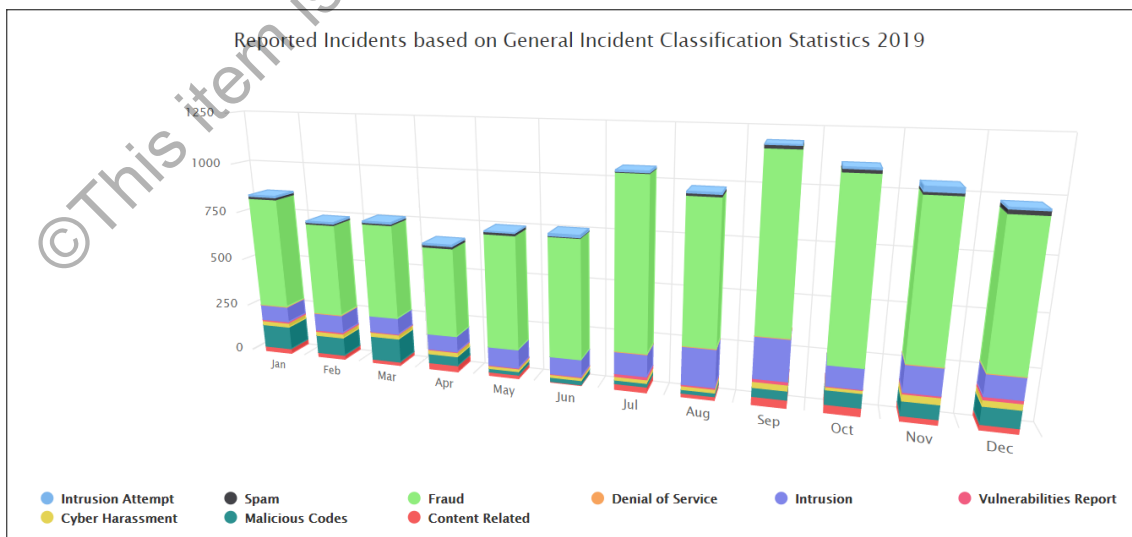


Figure 1.1 Cyber threat reports by MyCert (CyberSecurity, 2019)

In order to handle issues pertaining to computer security, most developed applications are built with a user verification screen to allow the users to input their user IDs and passwords before using the system. This method is one way to secure computer through the software security aspect and also known as user verification.

There are three methods implementable to authenticate users (Monrose, 2000):

- i **Something the user knows.** It is related to things that users know such as user ID and password. This method is the most preferred method amongst systems developer to be applied in the system that is being developed. Most systems in use today utilize this method for system usage authorization. In order to use this method, users are required to input one unique user id and password. However, research has found that users regularly used easy or same passwords for all application (Yıldırım & Mackie, 2019). This practice made it easy for user id and password to be guessed using dictionary attack.
- ii **Something the user has.** This method uses additional physical accessories owned by registered user. Simplest example for this method is house or office key; only person with the key are allowed access to the place. This method is applied in computer system with additional accessory given to user such as USB key (Gregory, 2015), token (Suwald & Burghardt, 2020) and Smart Card (Hussain et al., 2019). The user of these additional accessories is required to keep them from being lost, stolen or copied by others. Should there be an incident of misplaced, stolen

or unauthorized duplication, users are bound to report to system administrator to block the particular device.

iii **Something the user is.** It is about unique features of users or most commonly known as biometrics. User identification using biometrics methods have started since the last few decades. Biometrics technology is closely related with human physical body or features on human. This method is divided into three main categories: Morphological, Behavioral and Biological (Choudhury, 2020; Tripathi, 2011) (refer to Figure 1.2)).

a) **Morphological** biometrics uses physical features on user for identification. Example for this feature would be fingerprints(Sokolov & Ponomareva, 2020), iris or eye retina (Hájek & Draňanský, 2019), facial shape (Best-Rowden & Jain, 2017), and palm geometry (Alpar & Krejcar, 2017). This method is dependable since it is hard to change its ownership or borrowed (Nawaya et al., 2019).

b) **Behavioral** biometrics is related to the behavior of a system user. Measurement and verification for this method can be either voice identification (Kuśmierczyk et al., 2020), keyboard typing style (Mondal & Bours, 2017), walking style (Condell et al., 2017) and signature (Kancharla et al., 2018). This measurement criteria is done on user spontaneously or without user noticing so that the real user behavior can be recorded (Alrumaih et al., 2020).

- c) **Biological** biometrics is a method to identify user based on biological features available on users. Example for user identification using this technology would be DNA, molecule structure, bones, teeth and internal organs (Correa et al., 2020).

Each of this method has its own advantages and disadvantages. The actual usage of physical biometrics, smart card, USB Key and token in a system would involve high costs (A. V. S. Kumar, 2019). Each user wishes to use the system with those features are required to purchase related equipments or devices, at a higher price. On the contrary, methods of using user ID and password, and behavioral biometrics do not require additional cost for equipments (Saeed, 2016). However, only a few methods of biometric user identification have been utilized by commercial systems to perform verification of the validity of users. For example, Morphological identification method using finger print, iris and face recognition have been used by the security force of the United States to control the country border entry point (Buhrow, 2016).

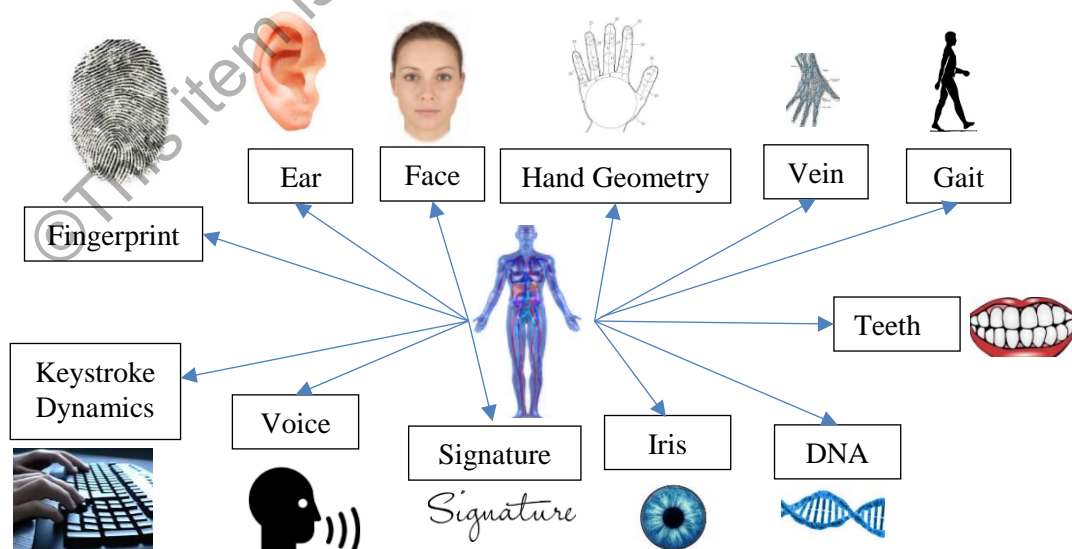


Figure 1.2 Examples of biometric modalities that can be used to authenticate the users