



**UNIVERSITI PUTRA MALAYSIA**

***A MULTI-FACTOR AUTHENTICATION SCHEME USING ATTACK  
RECOGNITION AND KEY GENERATOR TECHNIQUE***

**NOOR AFIZA MOHD ARIFFIN**

**FSKTM 2018 14**



**A MULTI-FACTOR AUTHENTICATION SCHEME USING ATTACK  
RECOGNITION AND KEY GENERATOR TECHNIQUE**

By

**NOOR AFIZA MOHD ARIFFIN**

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in  
Fulfillments of the Requirements for the Degree of Doctor of Philosophy**

**October 2017**

## **COPYRIGHT**

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia.



Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

**A MULTI-FACTOR AUTHENTICATION SCHEME USING ATTACK  
RECOGNITION AND KEY GENERATOR TECHNIQUE**

By

**NOOR AFIZA MOHD ARIFFIN**

**October 2017**

**Chairman : Associate Professor Nor Fazlida Mohd Sani, PhD**  
**Faculty : Computer Science and Information Technology**

In today's world, security plays an important role in many authentication applications. Modern era information sharing is boundless and becoming much easier to access with the introduction of the Internet and the World Wide Web. Although this can be considered as a good point, issues such as privacy and data integrity arise due to the lack of control and authority. For this reason the concept of data security was introduced. Data security can be categorized into two which are secrecy and authentication. This research in particular was focused on the authentication of data security.

One popular scheme used for authentication security is the implementation of multi-factor authentication (MFA). There have been several researches which discuss on multi-factor authentication scheme but most of these research do not entirely protect data against all types of attacks. Furthermore, most current research only focuses on improving the security part of authentication while neglecting other important parts such as the systems accuracy and efficiency. Accuracy is based on how perfect is the system able to identify a genuine user or an intruder. Efficiency is based on the processing time of the overall authentication system. Current multifactor authentication schemes were simply not designed to have security, accuracy and efficiency as their main focus.

To overcome the above issue, this research will propose a new multi-factor authentication scheme which is capable to withstand external attacks which are known security vulnerabilities and user attacks which are based on user behavior. On the other hand, the proposed scheme still needs to maintain an optimum level of accuracy and efficiency.

This framework consists of the task to design, implement and perform vulnerability assessment on the proposed multi-factor authentication scheme. In the design phase, the factors of authentication is identified and also clasified accordingly. Basically, all the factors that are used in the proposed research which are username, password, face and fingerprint were selected based on its simplicity, applicability, and cost effectiveness. The factors chosen are still widely used in various applications such as security systems, surveillance systems, and general identity verification systems. The research then continues to the implementation stage which uses Microsoft Visual Studio 2013 as the platform and C# as the programming language. Once the scheme is done, comes the final vulnerability assessment stage which is to evaluate the security level of the proposed scheme. In this stage a vulnerabilities assessment (VA) test was conducted on the proposed scheme with the use of some well-known attacks. Another experiment was then conducted to measure the accuracy and efficiency of the proposed multi-factor authentication scheme. All the results was then compared with previous researches.

From the result of the experiments, the proposed scheme was proven to be able to withstand the attacks. This is due to the implementation of the attack recognition and key generator technique together with the use of multi-factor in the proposed scheme. Furthermore, the experiment on accuracy showed the proposed scheme having a score of 96% accuracy which is more than the score of the other 2 previous schemes. For efficiency the proposed scheme had an average speed processing time 15 seconds which is the lowest among all the compared schemes. This shows that the proposed scheme provides a strong authentication scheme, which ensures security, while still maintaining good accuracy and efficiency.

Finally, the proposed research is suitable to implement in high-security places such as the government sector, financial institutions or health institutions. It largely motivated by improving traditional authentication through the additional layers of security in authentication. These can be used to overcome some of the limitations faced by existing authentications.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

**SKIM PENGESAHAN PELBAGAI FAKTOR MENGGUNAKAN  
PENGECAMAN SERANGAN DAN TEKNIK PENJANA KUNCI**

Oleh

**NOOR AFIZA MOHD ARIFFIN**

**Oktober 2017**

**Pengerusi : Profesor Madya Nor Fazlida Mohd Sani, PhD**  
**Fakulti : Sains Komputer dan Teknologi Maklumat**

Dalam dunia masa kini, keselamatan memainkan peranan penting dalam banyak aplikasi pengesahan. Di zaman moden, perkongsian maklumat tidak terbatas dan menjadi lebih mudah untuk akses dengan pengenalan Internet dan jaringan sejagat. Walaupun ini boleh dianggap sebagai perkara berfaedah, timbul isu seperti privasi dan keutuhan data disebabkan kekurangan kawalan dan kuasa. Oleh sebab itu, keselamatan data telah diperkenalkan. Keselamatan data dapat dikategorikan kepada dua iaitu rahsia dan pengesahan. Bagaimanapun, cadangan penyelidikan ini fokus kepada keselamatan dalam skim pengesahan.

Terdapat beberapa skim yang telah dicadangkan mengenai pengesahan pelbagai faktor. Bagaimanapun, mereka memperkenalkan lebih banyak isu keselamatan, seperti kekurangan teknik keselamatan dalam skim-skim pengesahan yang menyebabkan terdedah kepada serangan. Skim-skim tersebut juga adalah sukar untuk menghasilkan satu sistem pengesahan dengan kelajuan dan ketepatan tinggi. Skim terdahulu hanya menumpukan sama ada pada kelajuan atau ketepatan dalam sistem pengesahan mereka. Tambahan pula, pengesahan cekap berdasarkan kelajuan masa pemprosesan juga belum lagi menjadi subjek tumpuan. Skim ini masih berhadapan dengan masalah iaitu sukar untuk menghasilkan satu sistem pengesahan dengan kecekapan tinggi tanpa berkompromi ketepatan padanan dalam ukuran luas. Maka, pengesahan yang kuat menjadi utama dalam persekitaran perkhidmatan rangkaian.

Untuk mengatasi isu di atas, penyelidikan ini mencadangkan skim pengesahan pelbagai faktor yang baru di mana berkebolehan untuk bertahan serangan ke atas kelemahan-kelemahan keselamatan. Ia juga mengekalkan kelajuan dan ketepatan.

Rangka kerja ini terdiri daripada mereka, melaksanakan dan penilaian kelemahan cadangan skim pengesahan pelbagai faktor. Dalam mereka, ia mengenal pasti dan mengelaskan faktor pengesahan. Pada dasarnya, semua faktor yang digunakan dalam cadangan penyelidikan (nama pengguna, kata laluan, muka dan cap jari) dipilih berdasarkan kemudahan, kebolegunaan, dan keberkesanan kos. Faktor yang dipilih masih popular digunakan dalam pelbagai kegunaan seperti sistem keselamatan, sistem pengawasan, dan sistem-sistem pengesahan identiti yang umum dan sesuai untuk semua jenis permohonan. Penyelidikan ini seterusnya melaksanakan skim yang dicadangkan dengan menggunakan Microsoft Visual Studio 2013 dan dibangunkan dengan menggunakan bahasa C#. Bagi menilai tahap keselamatan skim yang dicadangkan, penilaian (VA) kelemahan-kelemahan dijalankan menguji serangan dalam cadangan skim. Satu lagi ujian dijalankan untuk mengukur kelajuan dan kecekapan cadangan skim pengesahan pelbagai faktor. Semua keputusan dibandingkan dengan penyelidikan sebelumnya.

Dari penilaian kelemahan, skim dicadangkan ini telah terbukti untuk bertahan serangan dengan pengecaman serangan dan teknik penjana kunci yang dilaksanakan untuk meramalkan pelbagai jenis serangan. Juga, keputusan eksperimen menunjukkan bahawa cadangan skim amat tepat dalam pelaksanaan dengan 96% daripada ketepatan dan lebih efisien dengan masa pemprosesan pantas dengan purata 15 saat. Dari analisis sekuriti yang dijalankan didalam tesis ini, telah menunjukkan bahawa cadangan skim pengesahan pelbagai faktor ialah skim pengesahan yang kuat, yang memastikan keselamatan, kelajuan, dan kecekapan kepada satu tahap yang besar. Ini dijangka oleh teknik pengecaman serangan yang telah ditambah ke dalam skim pengesahan pelbagai faktor.

Pada dasarnya, cadangan penyelidikan yang dicadangkan ini adalah sesuai digunakan di bahagian sektor Kerajaan, Institusi Kewangan dan / atau institusi-institusi Kesihatan. Ia sebahagian besarnya dimotivasikan dengan meningkatkan pengesahan tradisional melalui dengan lapisan keselamatan tambahan dalam pengesahan. Ini boleh digunakan untuk mengatasi beberapa pembatasan yang dihadapi oleh sistem pengesahan yang sedia ada.

## ACKNOWLEDGEMENTS

All praise to the Almighty ALLAH SWT for it is through His Grace and Mercy that I am able to complete this thesis on time and to the satisfaction of the university.

I would like to take this opportunity to record my gratitude towards the great people whose important support to me during the phases of this research was very heartfelt. Special thanks to my supervisor, Assoc. Prof. Dr. Nor Fazlida Mohd Sani who always has the time when I have problems in this research with her patiently answered my questions, giving valuable comments, guidance and advice through the course of this research.

Also, my deepest appreciation to my co-supervisors Prof. Dr. Ramlan Mahmod and Assoc. Prof. Dr. Zurina Mohd Hanapi for their cooperation, efforts, valuable suggestions and constructive comments.

Great thanks to the Faculty of Computer Science and Information Technology for the facilities and also the university library and Universiti Putra Malaysia for providing the working environment for me to perform this research.

I want to express my special thanks to my father and mother, who never let me believe I could not succeed in this research. Also, special thanks to my husband, my lovely daughters and my siblings for their support, love and encouragement during my research. Finally, I am grateful to my entire friend for their impressive help in my research.



I certify that a Thesis Examination Committee has met on 10 October 2017 to conduct the final examination of Noor Afiza binti Mohd Ariffin on her thesis entitled "A Multi-Factor Authentication Scheme using Attack Recognition and Key Generator Technique" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

**Azizol bin Hj. Abdullah, PhD**

Senior Lecturer  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Chairman)

**Nur Izura binti Udzir, PhD**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Internal Examiner)

**Mohd Taufik bin Abdullah, PhD**

Senior Lecturer  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Internal Examiner)

**Jemal Abawajy, PhD**

Professor  
Deakin University  
Australia  
(External Examiner)



---

**NOR AINI AB. SHUKOR, PhD**

Professor and Deputy Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date: 28 December 2017

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirements for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

**Nor Fazlida Mohd Sani, PhD**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Chairperson)

**Ramlan Mahmod, PhD**

Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

**Zurina Mohd Hanapi, PhD**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

---

**ROBIAH BINTI YUNUS, PhD**

Professor and Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date :

### Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Name and Matric No.: Noor Afiza Mohd Ariffin, GS39310

### Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: \_\_\_\_\_  
Name of Chairman  
of Supervisory  
Committee: Associate Professor Dr. Nor Fazlida Mohd Sani

Signature: \_\_\_\_\_  
Name of Member  
of Supervisory  
Committee: Professor Dr. Ramlan Mahmud

Signature: \_\_\_\_\_  
Name of Member  
of Supervisory  
Committee: Associate Professor Dr. Zurina Mohd Hanapi

## TABLE OF CONTENTS

	<b>Page</b>
<b>ABSTRACT</b>	i
<b>ABSTRAK</b>	iii
<b>ACKNOWLEDGEMENTS</b>	v
<b>APPROVAL</b>	vi
<b>DECLARATION</b>	viii
<b>LIST OF TABLES</b>	xiii
<b>LIST OF FIGURES</b>	xv
 <b>CHAPTER</b>	
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Background	1
1.2 Problem Statement	3
1.3 Objectives	6
1.4 Scope of Research	6
1.5 Contribution of the Research	6
1.6 Thesis Organization	8
 <b>2 LITERATURE Review</b>	 <b>10</b>
2.1 Security and Authentication	10
2.1.1 Types of Authentication	14
2.2 Single-Factor Authentication (SFA)	16
2.3 Multi-Factor Authentication (MFA)	22
2.4 Security Techniques in Authentication	28
2.4.1 Secure Key Generator	33
2.4.2 Plan Recognition Technique	37
2.5 Comparison and Discussion	42
2.6 Summary	46
 <b>3 RESEARCH METHODOLOGY</b>	 <b>47</b>
3.1 Introduction	47
3.2 Phase I: Design, Implementation and Vulnerabilities Assessment of the proposed multi-factor authentication scheme	48
3.3 Phase II: Experiment for an Accurate New Multi-factor Authentication Scheme	53
3.4 Phase III: Experiment of an Efficient New Multi-factor Authentication scheme	55
3.5 Summary	56

<b>4</b>	<b>A SECURE MULTI-FACTOR AUTHENTICATION SCHEME WITH ATTACK RECOGNITION AND KEY GENERATOR TECHNIQUE</b>	<b>57</b>
4.1	Introduction	57
4.2	Previous Multi-factor Authentication Schemes	57
4.3	The Proposed Multi-factor Authentication Scheme	61
4.3.1	Key Generator Techniques for the Proposed Multi-factor Authentication Scheme	63
4.3.2	The Biometric Matching Process for the Proposed Multi-factor Authentication Scheme	65
4.3.3	Attack Recognition Technique for the Proposed Multi-factor Authentication Scheme	66
4.4	The System Process Flow for the Proposed Multi-factor Authentication Scheme	71
4.4.1	System Process Flow for Enrollment Phase	71
4.4.1.1	Face Detection Process	74
4.4.1.2	Fingerprint Detection Process	75
4.4.1.3	Hashing Encryption Process	76
4.4.1.4	Summary of the Enrollment Phase	76
4.4.2	System Process Flow for Authentication Phase	76
4.4.2.1	Summary of the Authentication Phase	78
4.5	Security Analysis	79
4.5.1	Security Analysis on User Attack Plan	79
4.5.1.1	Results of User Attack Plan for the Proposed Scheme	81
4.5.2	Security Analysis on External Attack	82
4.5.2.1	Results of Penetration Testing	84
4.6	Summary	85
<b>5</b>	<b>ACCURACY OF THE NEW MULTI-FACTOR AUTHENTICATION SCHEME</b>	<b>87</b>
5.1	Introduction	87
5.2	Evaluation of Accuracy in Multi-factor Authentication Schemes	87
5.2.1	False Acceptance Rate and False Rejection Rate	88
5.2.2	Failure to Enroll Rate	90
5.2.3	Equal Error Rate	90
5.2.4	Threshold	91
5.3	Experimental Design of the Multi-factor Authentication Scheme	91
5.4	Analysis of Result of the Multi-factor Authentication Scheme	96
5.4.1	Results of the First Experiment	96
5.4.2	Results of the Second Experiment	99
5.5	Summary	102
<b>6</b>	<b>EFFICIENCY OF THE NEW MULTI-FACTOR AUTHENTICATION SCHEME</b>	<b>103</b>
6.1	Introduction	103
6.2	Experimental Design of the Multi-factor Authentication Scheme	104
6.3	Result Analysis of Multi-factor Authentication Scheme	108

6.4	Summary	111
<b>7</b>	<b>CONCLUSION</b>	<b>112</b>
7.1	Summary	112
7.2	Recommendations for Future Works	113
	<b>REFERENCES</b>	<b>114</b>
	<b>APPENDICES</b>	<b>124</b>
	<b>BIODATA OF STUDENT</b>	<b>148</b>
	<b>LIST OF PUBLICATIONS</b>	<b>149</b>



## LIST OF TABLES

Table	Page	
2.1	Comparison between Matching Techniques	31
2.2	Comparison between Secure Key Generators	35
2.3	The contribution of plan recognition from various fields	40
2.4	Capability of Achieving Security Features	42
2.5	Comparison of Authentication Features	45
3.1	Types of attacks	53
4.1	Comparison Features	62
4.2	Comparison between Plan Recognition and Attack Recognition	67
4.3	User Attacks Plan in Attack Template Database	79
4.4	External Attacks in Attack Recognition	79
4.5	Result of User Attack Plan	81
4.6	Penetration Tools	82
4.7	Summary of penetration test	85
5.1	Security Technique for each Scheme in both experiments	92
5.2	Threshold for FAR and FRR	96
5.3	Comparison of Accuracy for Experiment 1	97
5.4	Summary of Result for Experiment 1	99
5.5	Comparison of Accuracy for Experiment 2	99
5.6	Summary of Result for Experiment 2	102
6.1	Measureable Usability metric (Kainda, Flechais, & Roscoe, 2010)	104
6.2	Security Technique for each Scheme	106
6.3	Experiment for Efficiency Measurement	108





## LIST OF FIGURES

Figure		Page
2.1	Classification of user authentication approach (Singh & Thakur., 2012)	15
3.1	Research Methodology	48
4.1	Data Flow Diagram (Raja, A. Y., & Perumal, S. A., 2013)	59
4.2	Data Flow Diagram (Li et al., 2013)	60
4.3	Flow Diagram Proposed Research	62
4.4	Key Generator Algorithm	64
4.5	Biometric Matching Algorithm	65
4.6	Plan of Attack Template Database	69
4.7	Attack Recognition Steps	70
4.8	System Process Flow for Enrollment Phase	72
4.9	The interface for Enrollment phase	73
4.10	Face recognition	74
4.11	Fingerprint recognition	75
4.12	System Process Flow for Authentication Phase	77
4.13	The interface for the Authentication phase	78
5.1	Experiment on Accuracy	92
5.2	User Process for both Experiment	94
5.3	FAR Process	94
5.4	FRR Process	95
5.5	Summaries for both Experiments	95
5.6	FAR, FRR and EER for Experiment 1	98

5.7	FAR, FRR and EER for Experiment 2	101
6.1	Enrollment process	105
6.2	Authentication process	106
6.3	Time Calculation for each Scheme	107
6.4	Summary of the Experiment	107
6.5	Total Time Taken All Scheme	110



## CHAPTER 1

### INTRODUCTION

This chapter introduces the research background, the research problem, the objectives, the scope of research, and the main contributions of this study. The chapter ends with an outline of the organization of this thesis.

#### 1.1 Background

In today's world, the ever changing and improvement of network facilities has brought more electronic devices together where information and resources are shared and openly accessible to anyone who seeks it. Therefore, security has become an important subject when dealing with shared information and data. Security can be categorized into two which are secrecy and authentication. Secrecy is protection of sensitive data against unauthorized and unwanted eavesdropping and modification. On the other hand, authentication is a mechanism that helps to prevent any unwanted forgery and unauthorized access to sensitive data. Thus, the subject of this research is to focus on the security of the authentication process. Security constraints should be incorporated at the highest level in an authentication system. Security will be the top priority to be considered in the process of building up a secure system. It reflects the fact of whether or not the authentication level of a user should be allowed or restricted based on the permission defined in the system. There are three different types of elements (known as factors) that can be used for user authentication. The first would be knowledge factor, which could be a password or PIN. Object factor, the second element which could be a card with a magnetic strip or the use of a smart card. The third element which is biometric factor could be the use physical features such as face imaging, human fingerprints, or human behavioral traits for example user signature. The most common scheme for providing authenticity is the use of a password-based approach that is grouped under the knowledge factor, which has also been the most prevalent approach for authentication in the last couple of decades. Most users can easily choose to remember passwords such as their own name or birth dates, the name of their pets, or the use of any common words. There have been many occasions that even by applying strong passwords on your system, the password can also be hacked by a determined intruder. On the other hand, if too many restrictions are imposed to create a strong password it may impact users as they can easily forget their own password. This in turn will not create a healthy working environment.

However, recent security breaches have shown that the use of single-factor authentication (SFA) mechanisms is insufficient Dragusin (2013). Security threats against poorly protected authentication mechanisms are constantly increasing Khan et al (2015). Due to the problems and shortcomings of single-factor authentication mechanisms, many have turned their heads to the use of multi-factor authentication

schemes (MFA). MFA will be the approach taken by industry leaders and also academic researchers.

Any application of authentication, which includes exposure to the computing environment, requires a higher level of protection, especially from vulnerable attacks that can compromise a user's identity or undermine the security of computer hardware and/or data. Other than security, the efficiency of authentication also needs emphasis, especially in terms of time. This is because an authentication system, which has a high level of security, will take a longer time for a complete message to be authenticated. Authentication has attracted much attention, as a form of technology to compensate certain weaknesses of objects and knowledge factor authentications. With the widespread adaptation of the computing environment, the scope of authentication has been extended to include a broader area, and the number of users that use authentication systems has increased exponentially, especially in biometric authentication. Indirectly, the accuracy of user authentication becomes an important factor with the increase in the number of users.

Biometrics provides a strong user authentication solution. In the rapid technological development of today, every aspect of human life is being replaced with machines. Therefore, security concern is paramount and there is a need to increase the automation of different surveillance techniques and authentication of users. To achieve a more secure authentication, the process should be combined with something unique that the authorized person has. Human biometrics is the use of human characteristics. Combining biometrics with traditional use of passwords to create a functional and highly secure multi-factor authentication (MFA) mechanism. In recent years, biometrics technology has greatly improved and has clearly reached matured level. However, one area in biometrics which is the biometric templates for storage and communication still poses a challenge. Biometrics offers automated schemes of identity verification based on human physiological or behavioral aspects such as face, fingerprint or voice sample. Furthermore, the characteristics measured in biometrics must be unique. Although biometric techniques are more secure compared to other techniques of authentication, these methods are still open to vulnerable attack because most authentications are deployed in real-world applications with just a single-factor authentication. Some of the problems in single-factor authentication can be addressed with the deploying of multi-factor authentications that integrate multiple factors of authentication to enhance security of information. Therefore, it has been increasingly important that multi-factor authentication be deployed in a massive scale to cope with the ever growing need of information security.

As the usage of attack recognition techniques expands continuously. Basically, this research presents a plan recognition technique as attack recognition by using it in authentication. This research chooses to implement the attack recognition technique into the authentication field since there has been no previous research that has implemented the attack recognition in this field. To understand attack recognition more clearly, a scenario can be used. As an example, supposed that someone has asked you for the

location of the DHL Courier office and its availability to deliver packages overseas. You might reasonably think that he or she wanted to quickly get an item to someone in another country and intends to use DHL Courier for delivery. By doing so, you have inferred the goals of the other person and a portion of that person's plan for achieving those goals. This is often referred to as attack recognition. The implementation of the attack recognition technique has long been in existence and has also broadened to include the computer security domain over the past decades, especially in intrusion detection systems (IDSs). The available researches in the field of authentication have not yet implemented the attack recognition technique into authentication systems. Normally, this technique is implemented in language understanding and intrusion detection systems. Attack recognition identifies terrorists. In Artificial Intelligence, attack recognition is a process analyzing user action to determine their goal or result. The result will be accessed and the AI will plan the appropriate responses to any user action. However, in network security, a new set of requirements on attack recognition has been introduced.

## 1.2 Problem Statement

Based on literature studies, a few problems have been discovered in this research. This research explains the problems starting from the viewpoint of security paradigm, followed with the accuracy problem in authentication, and the problem of efficiency in authentication mechanisms.

The problem in security paradigm is the lack of a security technique, especially in authentication systems. A study from Li et al.(2013) states that the problem in security technique prevention and analysis of attacks is still a very tough topic in either the industry or academic institutions. Besides that, authentication security also has its problem. The problem comes from lack of design in creating a suitable encoding procedure for biometrics input signals to be converted and stored in the database. There is also lack of matching designs to match the biometric signal received and compare it with the stored data to generate an authentication decision. Li et al., (2013) proposed the use of a highly robust three-factor user authentication scheme with the use of key agreements designed for multimedia systems. But their scheme still faced with various security issues, especially in dealing with security vulnerabilities. According to Reno, (2013), a key problem in authentication systems is establishing the identity of the user without alienating the user. Multi-factor authentication is a potential fix to the current issues faced by authentication and is beginning to be implemented in websites operated by well-known companies. However, Raja & Perumal, (2013) pointed out that the multi-factor authentication is still a less secure option. So far, these existing security mechanisms lack security measures for practical implementation. The research from Raja & Perumal, (2013) proposed a security authentication scheme with combination of usage of both fingerprint biometric and mobile pin generation. This scheme is focus on security with using the username, password and fingerprint recognition together with pin number verification with mobile. But, this scheme is still vulnerable to certain type of attacks.



Another research by Huang et al., (2013) proposes a new multi-factor authentication scheme, which still has some vulnerabilities such as memory scan attacks, keyboard monitor attacks and software clone attacks due to its focused on mobile phones which has limited resources. A lot of previous security attacks that happened have had successful attempts on many types of authentication systems. This exploit due to security flaws has provided unauthorized users gain to sensitive data and are able to steal private information from unknown users. There were also cases where the normal operation of a system was disrupted because of system breach. Refer to Choudhury, (2011) states that strong security has not been extended into any authentication system as yet. Another problem in security authentication is to ensure that the right user uses or authorizes use of the right resource. The biggest problem in security authentication is to determine a way to secure data and applications that are running in servers away from their own premises (Venkataramana & Padmavathamma, 2012). The proposed scheme by Lee & Liu, (2013) transmits data (e.g. *ID*, *PW*, and *PKI*) in plaintext form, which can be easily intercepted and read by attackers. In addition, their scheme does not emphasis on user data privacy and can be considered poor in security. The scheme of Liao et al, (2006) is still prone to well-known vulnerabilities such as brute force attack, replay attack, and dictionary attack. In smart card-oriented schemes proposed by this research, the problem related with lost smart cards can also be solved. If a potential attacker picks up a lost smart card of a legitimate user, the attacker can then try to impersonate the real user when logging into an offline system. The only thing the attacker needs to do is insert the user password using brute force or dictionary attack. This research therefore proposes ten requirements for evaluating a new password authentication scheme. Another research from Sun et al, (2007) introduces on what he called key-mixed template (KMT). This template uses both user templates with the use of a private key to generate a new kind of template. This scheme helps to protect the biometric template stored in the database from snooping, back-end, and tampering attacks. However, this proposed scheme has had no external security protection, so it is possible to be exposed to risks from particular well known attacks.

Another problem is that it is difficult to produce an authentication system with fast speed and high accuracy. Based on the by Raja & Perumal, (2013), this researcher's scheme claims that their scheme has provided an accurate authentication method, however their scheme has a problem to reduces the speed of processing time without compromising the matching accuracy. According to Rathgeb & Busch, (2012), the accuracy of biometric recognition still face several problems and must be resolved. Among the main problems faced by existing authentication systems is less accuracy in performance concerning reliable person recognition. The authors therefore introduced a technique to provide good invariance theories but this still suffered from computational accuracy.

According to a previous study Rathgeb & Busch, (2012), accuracy of recognition has become the main problem in many authentication applications performed in an insecure network. The research pointed out that recognition problem has been in the limelight for some time but little to no improvement has been made since. The topic on biometric accuracy has also been highly underestimated. More needs to be done for biometric recognition to hit a satisfactory level. Furthermore, since humans are able to recognize

and tell apart a person with the utmost high accuracy, the same cannot be said with biometrics where the problem is not an easy one to solve (Rane et al., 2013). Another research states that the primary and underlying problem for accuracy performance of a biometric authentication system is caused by the limitation of the biometric identifiers. For example, the distinctive information in the geometry of a hand is less than that of a fingerprint. Thus, an increase in scale demands a need for enhanced accuracy among a larger number of targets, and therefore a higher level of matching accuracy is required (Al-Assam et al., 2011). Thus, with authentication systems of a large scale, it is critical to establish a matching system that reduces the volume of computations without compromising the matching accuracy. Furthermore, the matching accuracy generally drops as the matching speed increases. A method of matching at high speed while maintaining high accuracy has not yet been found (Shimahara, 2015).

Another problem in authentication is that it is difficult to produce an authentication system with high efficiency without compromising the matching accuracy in a large-scale authentication system. As a result, this problem can cause difficulty in terms of acceptable commercial use due to a slow processing time (Gnanaraj et al, 2013). As authentication is the gateway to any secure system and because it evolves with time, it is mandatory to always update security procedures, so that users can continue to enjoy the benefits of fast access without being concerned about any sort of threat. A proposed method by one study Ratha et al, (1995) was found not acceptable for commercial use because it has a slow processing time. In order to be acceptable for commercial use, the processing time of the proposed algorithm must be substantially improved. The Raja & Perumal,(2013) scheme claims that their scheme has provided an efficient authentication scheme. But, this scheme is still has high speed processing time. A scheme Tan, & Bhanu, (2010) claims to provide efficient authentication, however, this scheme still requires more execution time. A lot of effort over the last decade has been undertaken to address the problem of authentication systems, which has always resulted in overheads for the systems and delay for the end users. Previous researchers Gnanaraj et al, (2013) presented a scheme that is claimed to provide a time-efficient authentication, however, their scheme still requires increased time during registration and integrates a heavy weight encryption algorithm. A scheme Mathew & Thomas,(2013) claim that their scheme provides a faster processing time, which ensures higher security, but this scheme still requires a lot of processing time and is still not secure in terms of shouldering surfing attacks and image gallery attacks. The problem of efficiency and processing time in large-scale authentication systems such as national ID matching targets cannot be solved fundamentally (Shimahara, 2015).

According to Shimahara (2015), the authentication processing time will be highly significant for matching data in large-scale systems, which have hundreds of millions of data. As the demand for increased scale goes up, a higher level of efficiency and speed is needed. Authentication systems also have a critical problem in establishing a matching system that reduces the volume of time computations without compromising matching accuracy will be needed (Shimahara, 2015). A research from Kiruthika & Kumar (2014) required a significant execution time in a key-binding biometric cryptosystem to compute the transformation of encrypted templates in a plain domain. Besides that, their



research also faced problems i.e. difficulty in generating keys with high stability and in maintaining matching accuracy.

### **1.3 Objectives**

The main goal of this research is to propose a new multi-factor authentication scheme which is able to withstand attacks while maintaining high accuracy and efficiency to overcome problems caused by security vulnerabilities. In order to achieve this goal, the following objectives have been identified:

1. To propose an attack recognition technique which is able to detect and predict future attacks.
2. To propose a key generator (secure key) technique for increase security during authentication.

### **1.4 Scope of Research**

Basically, this research focuses on security in authentication based on a real life case study. Previous researches have not considered the entire security of transition but are usually focused on the end-to-end protection of the transaction between the user and the application only. The proposed research is therefore suitable for high-security places such as the Government sector, Financial Institutions and/or Health institutions. This research will consider contextual variables such as gender, experience level, and age related to the experiments that have been conducted in order to prove that the research objectives have been achieved. This research will not study the usefulness or utility of a particular computer-supported cooperative work technology product (i.e., groupware). In other words, this research will not consider specific hardware and/or software alternatives as an independent variable.

### **1.5 Contribution of the Research**

This research proposes a new multi-factor authentication scheme to increased security, by integrating the use of a secure key, user-specific fingerprint features, and facial recognition with additional layers of security, namely attack recognition and a key generator technique to improve the accuracy and efficiency on authentication. The main contributions to the field of research are summarized in the following point:

Contribution I: *Propose a new multi-factor authentication scheme with the use of attack recognition, key generator and biometrics to withstand attacks accurately and efficiently.*

The contribution of this research is measured in terms of security access to the proposed scheme in authenticating users based on attack recognition and key generator technique. In this contribution also, the proposed research combine a multi-factor authentication scheme which include username, fingerprint, and face recognition together with attack recognition and key generator technique to increase the security while maintaining a high accuracy and efficiency of the authentication scheme.

This scheme was analyzed against all known attacks through a vulnerabilities assessment for which the analysis results showed that this proposed scheme can withstand attacks. Currently all authentication systems are prone to two kinds of issues which are false acceptance of an intruder and false rejection of legitimate users. This research is well defined in the classical scheme of statistical decision theory, thereby provided two possible outcomes, which can be divided into False Acceptance Rate (FAR) and False Rejection Rate (FRR). According to Bolle et al.,(2002), current biometrics trend is more towards the importance of a high percentage in FAR and with a slight relaxed FRR requirement. By looking at the criteria of the decision, the probabilities outcomes of FAR and FRR can be adjusted in a way that it reflects to the satisfied accuracy level that is agreed. From a previous study Jin, A. T. B.,(2004), obtaining a perfect score of both zero FAR and FRR is nearly impossible and unheard of. This is because the classes are difficult to completely separate in the measurement space. Therefore, this research has proven that the proposed scheme has high accuracy via the implementation of a performance analysis that references FAR and FRR. An experiment was conducted as part of this research to obtain computational time starting from the time taken to input data, match the process with the database, and produce the results. The performance of this proposed scheme was assessed in terms of processing time. Our comparative analysis reveals the higher-level efficiency of this research compared to previous research. From the literature review conducted in this study, the researchers have found methods to improve the speed and efficiency of authentication, but there has been no scheme to increase efficiency during the authentication process. This research therefore addresses this gap by proposing an efficient multi-factor authentication scheme to achieve a fast processing time.

Contribution II: Propose an attack recognition technique to detect and predict future attacks.

The contribution of this research is measured in terms of security access to the proposed scheme in authenticating users based on attack recognition. This research presents an attack recognition technique to analyze attack recognition by using it in authentication. This is to match the need of authentication problem in the network security area. Basically, plan recognition is derived from the research area in Artificial Intelligence (AI) that has been conducted over the past few decades. However, in this research presents a plan recognition technique as attack recognition by using it in security authentication. The main function of the attack recognition technique in the proposed scheme is to detect a potential attacking attempt by an attacker based on scheme's observation of the user's behavior and actions.

Contribution III: Propose a key generator technique to increase security level in authentication.

The contribution of this research is to measure in terms of security access to the proposed scheme in authenticating users based on key generator technique. The secure key used in this research is a one-time password, which means that it is only valid to be used only once per user session. This secure key is generated based on the combination of the current date and time of when the user login process is performed. This combination will be unique as there will be no repetition of the earth date and time happening again. The key generator will generate a secure key, while the user registers with the scheme to make it more secure, thereby restricting unauthorized access. The proposed scheme does not use a password because this scheme does not intend to burden the user with remembering too complicated passwords when enrolling in the scheme. The proposed scheme can guarantee the user's credentials by ensuring the user's authenticity of identity. It also checks for the correct email before sending the secure key to the correct user.

## 1.6 Thesis Organization

This thesis is organized as follows:

**Chapter 1** is the introductory chapter that discusses the problem statement of the research, the objective, the scope of research, and research contributions.

**Chapter 2** presents a review of the related literature on existing authentication schemes, security techniques in authentication, and plan recognition techniques. This chapter also provides a summary of the comparison between the proposed scheme and existing schemes in terms of authentication techniques, authentication features, and capability of achieving security features.

**Chapter 3** covers detailed discussions on the methodology applied in this research. The research methodology gives step-by-step guidance to the reader so that this research work can be understood based on the scope and objective of this research. All the steps required in the methodology are also discussed here.

**Chapter 4** organizes the requirements of the proposed scheme to integrate a generic attack recognition method to increase security in authentication and evaluate the results of security attacks.

**Chapter 5** focuses on the evaluation of the second objective of the research which is the accuracy of the new multi-factor authentication scheme based on FAR and FRR.

**Chapter 6** focuses on the evaluation of the efficiency of the proposed multi-factor authentication scheme. The process of evaluation is implemented to fulfill the third

research objective introduced in Chapter 1. Furthermore, some experiments are discussed and the results are presented to prove the performance of the proposed scheme in terms of speed of processing time.

**Chapter 7** presents the conclusions of the research work carried out in this thesis and points out several recommendations for future works for exploration and also open problems that have been discovered throughout this research period.



## REFERENCES

- A. K. Jain and S. Pankanti (2001), "Biometrics Systems: Anatomy of Performance", IEICE Transactions Fundamentals, Vol. E84-D, No. 7, pp. 788-799.
- Acar, T., Belenkiy, M., & Küpçü, A. (2013). Single password authentication. *Computer Networks*, 57(13), 2597-2614. Accuracy of Fingerprint Identification Systems in Support of Public Bodies. NEC Technical Journal/Vol.9 No.1/Special Issue on Solutions for Society - Creating a Safer and More Secure Society.
- Agundez, I.R. and Bringas, P.,(2012); Sobotka, J. and Dolezel, R., 2010
- Al-Assam, H., Sellahewa, H., & Jassim, S. A. (2011). Accuracy and security evaluation of multi-factor biometric authentication. *International Journal for Information Security Research*, 1(1), 11-19.
- Alfawaz, S., May, L. J., & Mohannak, K. (2008). E-government security in developing countries: a managerial conceptual framework.
- AlZomai, M., AlFayyadh, B., Jøsang, A., & McCullagh, A. (2008). An experimental investigation of the usability of transaction authorization in online bank security systems. In *Proceedings of the sixth Australasian conference on Information security*-Volume 81 (pp. 65-73). Australian Computer Society, Inc..
- Badrinath, G. S., & Gupta, P. (2011). Stockwell transform based palm-print recognition. *Applied Soft Computing*, 11(7), 4267-4281.
- Bang, Y., Lee, D. J., Bae, Y. S., & Ahn, J. H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. *International journal of information management*, 32(5), 409-418.
- Barbosa, M., Brouard, T., Cauchie, S., & De Sousa, S. M. (2008). Secure biometric authentication with improved accuracy. In *Australasian Conference on Information Security and Privacy* (pp. 21-36). Springer Berlin Heidelberg.
- Besbes, F., Trichili, H., & Solaiman, B. (2008). Multimodal biometric system based on fingerprint identification and iris recognition. In *Information and Communication Technologies: From Theory to Applications*, 2008. ICTTA 2008. 3rd International Conference on (pp. 1-5). IEEE.
- Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, 15(5), 529-560.

- Blythe, J., Camp, J., & Garg, V. (2011). Targeted risk communication for computer security. In Proceedings of the 16th international conference on Intelligent user interfaces (pp. 295-298). ACM.
- Braz, C., Robert, J.M. (2006): Security and Usability: The Case of the User Authentication Methods. In: Proceedings of d'Interaction Homme-Machine, pp. 199–203.
- Buckley, S. (Ed.). (2006). Encyclopedia of contemporary Japanese culture. Routledge.
- Cai, Z., Feng, Y., Gan, Y., Zhang, R., & Zhang, J. (2014). Research on Plan Recognition Based on Misleading Action Processing. Open Automation and Control Systems Journal, 6, 1029-1037.
- Candaele, B., Soudris, D., & Anagnostopoulos, I. (2015). Trusted Computing for Embedded Systems (p. 151). Springer]
- Carberry, S. (1996). Plan recognition: achievements, problems, and prospects. A A, 5, 6.
- Chang, C. C., & Wu, T. C. (1991). Remote password authentication with smart cards. IEE Proceedings E-Computers and Digital Techniques, 138(3), 165-168.
- Chen, G., Yao, H., & Wang, Z. (2010). An intelligent WLAN intrusion prevention system based on signature detection and plan recognition. In Future Networks, 2010. ICFN'10. Second International Conference on (pp. 168-172). IEEE.
- Cheng, D. C., & Thawonmas, R. (2004). Case-based plan recognition for real-time strategy games. In Proceedings of the Fifth Game-On International Conference (pp. 36-40).
- Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. (2011). A strong user authentication framework for cloud computing. In Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific (pp. 110-115). IEEE. Conference on Artificial Intelligence (AAAI-86), 1986, 32-38.
- Deepika, C. L., & Kandaswamy, A. (2009). An algorithm for improved accuracy in unimodal biometric systems through fusion of multiple feature sets. ICGST-GVIP Journal, ISSN, 33-40.
- Doherty, Anastakis, & Fulford, (2011); Kankanhalli et al., (2003); Straub & Welke, (1998); Drogkaris, P., Geneiatakis, D., Gritzalis, S., Lambrinoudakis, C., & Lilian, M. (2008). Towards an enhanced authentication framework for government services: the greek case. na.



- Elfadil, N. A., & Al-raisi, Y. J. (2008). An approach for multi factor authentication for securing smart cards' applications. In *Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on* (pp. 368-372). IEEE.
- Fagundes, M. S., Meneguzzi, F., Bordini, R. H., & Vieira, R. (2014). Dealing with ambiguity in plan recognition under time constraints. In *Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems* (pp. 389-396). International Foundation for Autonomous Agents and Multiagent Systems.
- Geib, C. W., & Goldman, R. P. (2001). Plan recognition in intrusion detection systems. In *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings* (Vol. 1, pp. 46-55). IEEE.
- Geib, C., & Goldman, R. (2002). Requirements for plan recognition in network security systems. In *Proceedings of the Recent Advances in Intrusion Detection conference*.
- Gnanaraj, J. W. K., Ezra, K., & Rajsingh, E. B. (2013). Smart card based time efficient authentication scheme for global grid computing. *Human-centric Computing and Information Sciences*, 3(1), 1-14.
- Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. *Journal of Intelligent Manufacturing*, 25(2), 217-230.
- Guo, D., & Wen, F. (2013). A New Remote Authentication Scheme for Anonymous Users Using ECC. In *2nd International Symposium on Computer, Communication, Control and Automation*. Atlantis Press.
- Gupta, U. (2015). Application of Multi factor authentication in Internet of Things domain. *arXiv preprint arXiv:1506.03753*.
- He, D., Chen, J., & Zhang, R. (2010). Weaknesses of a dynamic ID-based remote user authentication scheme. *International Journal of Electronic Security and Digital Forensics*, 3(4), 355-362.
- Huang, X., Xiang, Y., Chonka, A., Zhou, J., & Deng, R. H. (2011). A generic framework for three-factor authentication: preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, 22(8), 1390-1397.
- Huang, Y., Huang, Z., Zhao, H., & Lai, X. (2013). A new one-time password method. *IERI Procedia*, 4, 32-37.

- Indu, S.; Sathya, T.N.; Saravana Kumar, V. (2013). "A stand-alone and SMS-based approach for authentication using mobile phone," *Information Communication and Embedded Systems (ICICES)*, 2013 International Conference on , vol., no., pp.140,145, 21-22.
- Islam, S. M., Davies, R., Bennamoun, M., Owens, R. A., & Mian, A. S. (2013). Multibiometric human recognition using 3D ear and face features. *Pattern Recognition*, 46(3), 613-627.
- Jafri, R., & Arabnia, H. R. (2009). A survey of face recognition techniques. *Jips*, 5(2), 41-68.
- Jain, A. K., Hong, L., & Kulkarni, Y. (1999). A multimodal biometric system using fingerprint, face and speech. In *Proceedings of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication*, Washington DC (pp. 182-187).
- Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85(9), 1365-1388.
- Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., & Ross, A. (2004). Biometrics: a grand challenge. In *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on (Vol. 2, pp. 935-942)*. IEEE.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1), 4-20.
- Jarvis, P. A., Lunt, T. F., & Myers, K. L. (2005). Identifying terrorist activity with AI plan recognition technology. *AI Magazine*, 26(3), 73.
- Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 37(11), 2245-2255.
- Josang, A. (2012). PKI trust models. *Theory and Practice of Cryptography Solutions for Secure Information Systems*, 279.
- Kainda, R., Flechais, I., & Roscoe, A. W. (2010). Security and usability: Analysis and evaluation. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 275-282)*. IEEE.),
- Kaur, D., & Talwar, M. (2012) *Analysis of Enhanced Multimodal Biometrics System for Speech & Signature using Noisy Samples*
- Kautz, H., Allen, J.F. (1986). Generalized plan recognition. In *Proceedings of the Fifth National*



- Khalid, O., Khan, S. U., Madani, S. A., Hayat, K., Khan, M. I., Min-Allah, N., ... & Chen, D. (2013). Comparative study of trust and reputation systems for wireless sensor networks. *Security and Communication Networks*, 6(6), 669-688.
- Khan, S. H., Akbar, M. A., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, 48(2), 458-472.
- Kiruthika, R. & Prof. B. Rajesh Kumar M.E. (2014). Combination of Fingerprint for Security Protection, *International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 5*.
- Ko, T., & Krishnan, R. (2003). Fingerprint and face identification for large user population. *Journal of Systemics, Cybernetics and Information*, 1(3), 87-92.
- Kontogiannis, K. A., DeMori, R., Merlo, E., Galler, M., & Bernstein, M. (1996). Pattern matching for clone and concept detection. In *Reverse engineering* (pp. 77-108). Springer US.
- Kose, N., & Dugelay, J. L. (2012). Classification of captured and recaptured images to detect photograph spoofing. In *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on* (pp. 1027-1032). IEEE.
- Lee J K, Ryu S R, Yoo K Y.(2002). “Fingerprint-based remote user authentication scheme using smart cards”. *Electronics Letters*, vol.38, no.12, pp:554-555.
- Lesh, N., Rich, C., & Sidner, C. L. (1999). Using plan recognition in human-computer collaboration. In *UM99 User Modeling* (pp. 23-32). Springer Vienna.
- Leslie Lamport. (1981). Password authentication with insecure communication. *Commun. ACM*, 24(11):770–772.
- Li, X., Niu, J., Khan, M. K., Liao, J., & Zhao, X. (2013). Robust three-factor remote user authentication scheme with key agreement for multimedia systems. *Security and Communication Networks*.
- Lin, C. H., & Lai, Y. Y. (2004). A flexible biometrics remote user authentication scheme. *Computer Standards & Interfaces*, 27(1), 19-23.
- Lin, I. C., & Chang, C. C. (2009). A countable and time-bound password-based user authentication scheme for the applications of electronic commerce. *Information Sciences*, 179(9), 1269-1277.
- Liou, J. C., & Bhashyam, S. (2010). On Improving Feasibility and Security Measures of Online Authentication. *Int. J. Adv. Comp. Techn.*, 2(4), 6-16.

- Lisý, V., Píbil, R., Stiborek, J., Bosanský, B., & Pechoucek, M. (2012). Game-theoretic Approach to Adversarial Plan Recognition. In ECAI (Vol. 242, pp. 546-551).
- M. R. (2011). What is single-factor authentication (SFA)? - Definition from WhatIs.com. Retrieved from <http://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA>
- Malik, J., Girdhar, D., Dahiya, R., & Sainarayanan, G. (2014). Reference Threshold Calculation for Biometric Authentication. *International Journal of Image, Graphics and Signal Processing*, 6(2), 46.
- Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.
- Mao, W., Gratch, J. (2004). A utility-based approach to intention recognition. *AAMAS 2004 Workshop on Agent Tracking: Modelling Other Agents from Observations*.
- Mathew, G., & Thomas, S. (2013). A Novel Multifactor Authentication System Ensuring Usability and Security. *arXiv preprint arXiv:1311.4037*.
- Mhatre, A., Palla, S., Chikkerur, S., & Govindaraju, V. (2001). Efficient Search and Retrieval in Biometric Databases”, *SPIE Defense and Security*. In Symposium, March-2005.
- Milos Milovanovic, et al.,(2010) Choosing Authentication Techniques in e-Procurement System in Serbia, in *International Conference on Availability, Reliability and Security 2010, IEEE Xplore*. p. 374- 379.
- Murakami, T., & Takahashi, K. (2011). Fast and accurate biometric identification using score level indexing and fusion. In *Biometrics (IJCB), 2011 International Joint Conference on* (pp. 1-8). IEEE.
- Nigam, A., & Gupta, P. (2015). Designing an accurate hand biometric based authentication system fusing finger knuckleprint and palmprint. *Neurocomputing*, 151, 1120-1132.
- O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12), 2021-2040.
- P.J.Philips,P.Grother,R.J.Micheals,D.M.Blackburn,E.Tabassi,and J. M. Bone. *FRVT (2002): Overview and Summary*. [Online]. Available: <http://www.frvt.org/FRVT2002/documents.htm>.
- Parameswari, D., & Jose, L. (2011). SET with SMS OTP using Two Factor Authentication. *Journal of Computer Applications (JCA)*, 4(4), 4.Caine et al.,2013; Jemima, P. and Rodrigo, R.,2013

- Pernul, G. (1995). Information systems security: Scope, state-of-the-art, and evaluation of techniques. *International Journal of Information Management*, 15(3),165–180.
- Qin, X., & Lee, W. (2004). Attack plan recognition and prediction using causal networks. In *Computer Security Applications Conference, 2004. 20th Annual* (pp. 370-379). IEEE.
- R. Dragusin, Data Breach at IEEE.org:100k Plain text Passwords, (2013), (<http://ieeelog.com>), Online (accessed18.11.13)
- Radha, N., & Kavitha, A. (2012). Rank level fusion using fingerprint and iris biometrics. *Indian Journal of Computer Science and Engineering*, 2(6), 917-923.
- Raja, A. Y., & Perumal, S. A. (2013). Effective Method of Web Site Authentication Using Finger Print Verification. *International Journal of Computer and Electrical Engineering*, 5(6), 545.
- Ramani, R., Selvaraju, S., Valarmathy, S., & Niranjana, P. (2012). Bank Locker Security System based on RFID and GSM Technology. *International Journal of Computer Applications*, 57(18).
- Ramasamy, R., & Muniyandi, A. P. (2012). An Efficient Password Authentication Scheme for Smart Card. *IJ Network Security*, 14(3), 180-186.
- Rane, S., Wang, Y., Draper, S. C., & Ishwar, P. (2013). Secure biometrics: concepts, authentication architectures, and challenges. *Signal Processing Magazine, IEEE*, 30(5), 51-64.
- Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3), 614-634.
- Ratha, N., Chen, S., and Jain, A. K. (1995) “Adaptive flow orientation based feature extraction in fingerprint images,” *Pattern Recognition*, vol. 28, no. 11, pp. 1657–1672.
- Rattani, A., Kisku, D. R., Bicego, M., & Tistarelli, M. (2007). Feature level fusion of face and fingerprint biometrics. In *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on* (pp. 1-6). IEEE.
- Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, 19(4), 439-444.

- Reno, J. (2013). Multifactor Authentication: Its Time Has Come. *Technology Innovation Management Review*, 3(8), 51.
- Ross, A., Nandakumar, K., & Jain, A. K. (2008). Handbook of Biometrics, chapter Introduction to multibiometrics. Springer-Verlag, 2, 3.
- Rowley, H. A., Baluja, S., & Kanade, T. (1998). Neural network-based face detection. *IEEE Transactions on pattern analysis and machine intelligence*, 20(1), 23-38.
- S. H. Ju and H. S. Seo, (2011). "Password based user authentication schemeology using multi-input on multi-touch environment," *Journal of the Korea Society For Simulation*, vol. 20, no. 1, pp.39-49.
- S. Nanavati, M. Thieme, and R. Nanavati, (2002). *Biometrics: Identity Verification in a Networked World*. New York: John Wiley & Sons, Inc.
- Sadi, M. S., & Kanij, T. (2011). Fingerprint verification: A comparison of three approaches. In *Defense Science Research Conference and Expo (DSR)*, 2011 (pp. 1-5). IEEE.
- Sadri, F. (2010). Logic-based approaches to intention recognition. *Handbook of Research on Ambient Intelligence: Trends and Perspectives*, 346-375.
- Sarkar, S., & Roy, A. (2013). Survey on Biometric applications for implementation of authentication in smart Governance. *Researchers World*, 4(4), 103.
- Schneiderman, H., & Kanade, T. (2000). A statistical method for 3D object detection applied to faces and cars. In *Computer Vision and Pattern Recognition, 2000. Proceedings. IEEE Conference on* (Vol. 1, pp. 746-751). IEEE.
- Scmidt, C., Sridharan, N., Goodson, J. (1978). The plan recognition problem: an intersection of psychology and artificial intelligence. *Artificial Intelligence*, Vol. 11, 1978, 45-83.
- SHIMAHARA Tatsuya, (2015). Technologies for Improving the Speed and Accuracy of Fingerprint Identification Systems in Support of Public Bodies. *NEC Technical Journal/Vol 9 No.1/ Special Issue on Solution for Society- Creating a Safer and More Secure Society*.
- Singh, P. I., & Thakur, G. S. M. (2012). Enhanced password based security system based on user behavior using neural networks. *International Journal of Information Engineering and Electronic Business*, 4(2), 29.
- Srivastava, K., Awasthi, A. K., & Mittal, R. C. (2014). An Improved Biometric Remote User Authentication Scheme Based on Nonce.

- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*, 441-469.
- Sun, H. M., & Yeh, H. T. (2006). Password-based authentication and key distribution protocols with perfect forward secrecy. *Journal of Computer and System Sciences*, 72(6), 1002-1011.
- Sun, S. W., Lu, C. S., & Chang, P. C. (2007). Biometric template protection: A key-mixed template approach. In *Proceeding IEEE International Conference Consumer Electronics* (pp. 10-14).
- Suzić, R., Svenson, P. (2006). Capabilities-based plan recognition. In *Proceedings of the 9th International Conference on Information Fusion, Italy, July 2006*.
- Thomas, L., & Parkin, S. S., Hayashi, M.(2008). Magnetic domain-wall racetrack memory. *Science*, 320(5873), 190-194.
- Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: a case study in fingerprints. In *Proceedings of SPIE (Vol. 5306, pp. 622-633)*.
- Venkataramana, K., & Padmavathamma, M. (2012). Agent based approach for authentication in cloud. *IRACST-International Journal of Computer Science and Information Technology & Security*, 2(3), 598-603.
- Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. In *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on (Vol. 1, pp. I-511). IEEE.*
- Wang, D., & Wang, P. (2015). Offline dictionary attack on password authentication schemes using smart cards. In *Information Security (pp. 221-237)*. Springer International Publishing.
- Wang, L. (2012). Research of artificial intelligent plan recognition. In *Electrical & Electronics Engineering (EEESYM), 2012 IEEE Symposium on (pp. 419-421). IEEE.*
- Wang, L. (2015). Research of Artificial Intelligent Plan Recognition Method in the Multi-Agents Conditions. *Advances in Intelligent Systems Research*.
- Wang, S. Q., Wang, J. Y., & Li, Y. Z. (2013). The Web Security Password Authentication based the Single-Block Hash Function. *IERI Procedia*, 4, 2-7.
- Wilensky, R. (1983). *Planning and understanding*. Addison Wesley, Reading, MA, 1983.

- Xu, J., Zhu, W. T., & Feng, D. G. (2008). Improvement of a fingerprint-based remote user authentication scheme. In Information Security and Assurance, 2008. ISA 2008. International Conference on (pp. 87-92). IEEE.
- Yang, W. H., & Shieh, S. P. (1999). Password authentication schemes with smart cards. Computers & Security, 18(8), 727-733.
- Zuo, H., Shen, Y., Li, S., & Shen, H. (2012). Two-Way Real-Time Authentication System Based on Dynamic Password and Multi-biometric. In Computer Science & Service System (CSSS), 2012 International Conference on (pp. 1254-1257). IEEE.

