استخدام طبعة الأصابع في الحوسبة السحابية المتنقلة الأمينة

SECURE MOBILE CLOUD COMPUTING BASED-ON FINGERPRINT

By

Jalal Yousef AL-Juneidi

Supervisor

Prof. Dr. Alaa H Al-Hamami

A Thesis submitted in partial fulfillment of the Requirements for theDegree of Master in Computer Science

Computer Science Department College of Computer Sciences and Informatics
Amman Arab University

(September, 2014)

المنارة للاستشارات

www.manaraa.com

Authorization

I, "Jalal Yousef AL-Juneidi" authorize Amman Arab University to provide copies of this thesis to libraries, institutions, and other parties upon their request.

Name: Jalal Yousef AL-Juneidi.

Signature:

Date: 17/9/2014.

المنارة للاستشارات

www.manaraa.com

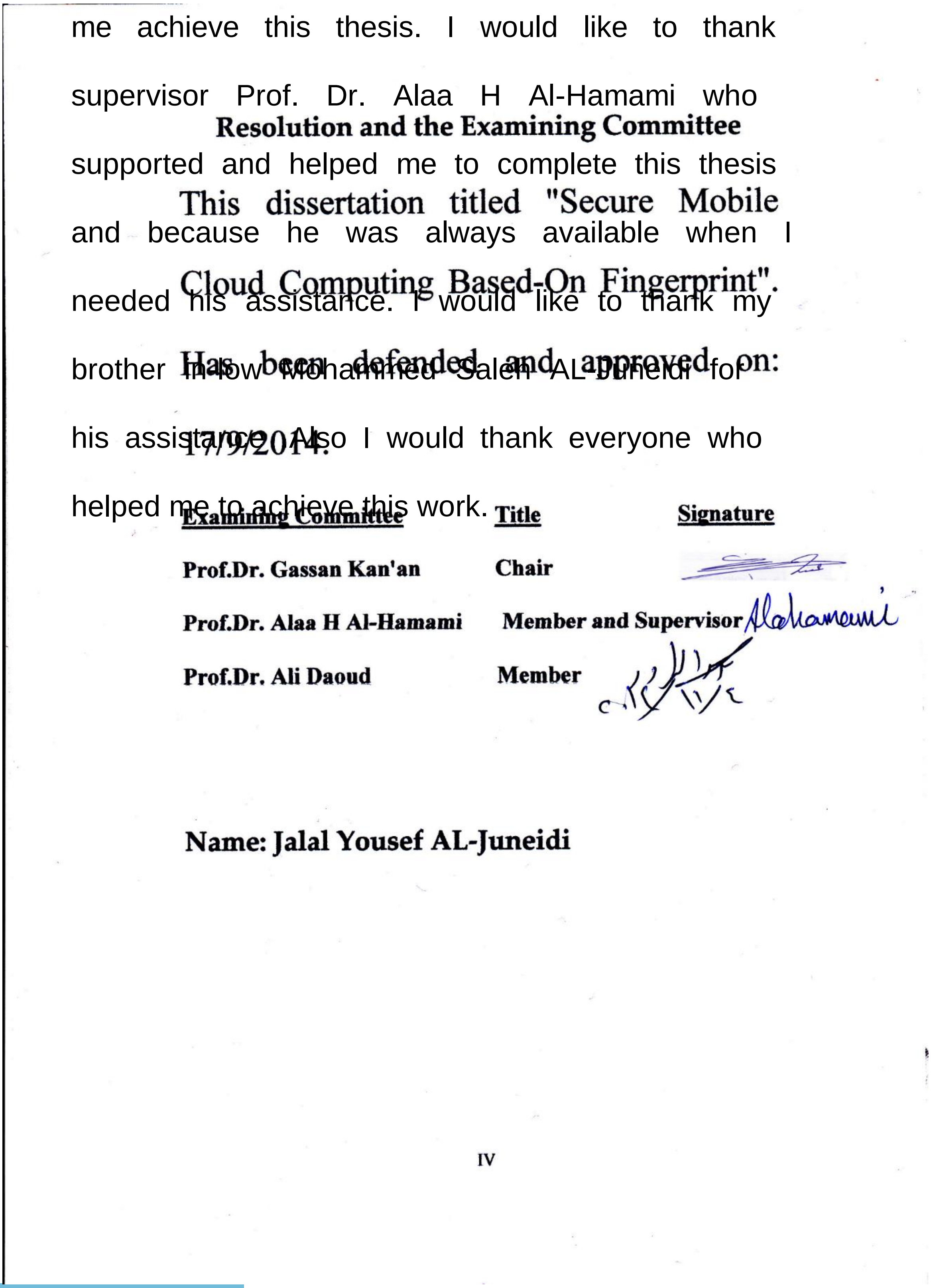
Dedication

I dedicate this thesis to my father, my mother, my brothers, my sisters, my supervisor Prof. Dr. Alaa H Al-Hamami and Dr Akram Othman Almchaakhi and to my lectures in Amman Arab University.

المنارة للاستشارات
www.manaraa.com

Acknowledgment

I want to thank ALLAH for his blessings that help me achieve this thesis. I would like to thank supervisor Prof. Dr. Alaa H Al-Hamami who supported and helped me to complete this thesis and because he was always available when I needed his assistance. I would like to thank my brother in-low Mohammed Saleh AL-Juneidi for his assistance. Also I would thank everyone who helped me to achieve this work.



Resolution and the Examining Committee

This dissertation titled "Secure Mobile Cloud Computing Based-On Fingerprint". Has been defended and approved on: 17/9/2014.

Examining Committee	Title	Signature
Prof.Dr. Gassan Kan'an	Chair	
Prof.Dr. Alaa H Al-Hamami	Member and Supervisor	Alahamami
Prof.Dr. Ali Daoud	Member	١١/٢

Name: Jalal Yousef AL-Juneidi

IV

المنارة للاستشارات
www.manaraa.com

List of Abbreviations

Attribute-Based Encryption	
Communication as a Service	
Consolidated Authentication Model	
Cloud Computing	
Database as a Service	
Global Positioning System	
High Technology	
Infrastructure as a Service	
Internet Key Exchange	
Information Technology	
Key Distribution Centers	
Monitoring as a Service	
Mobile Cloud Computing	
Mobile Cloud Key Exchange	
Multimedia Messages Service	
One-Time Password	

المنارة للاستشارات
www.manaraa.com

Platform as a Service	

Personal Computer	
Software as a Service	
Secure Mobile User-based Data Service Mechanism	
Short Messages Service	
Wide Area Network	

المنارة للاستشارات

www.manaraa.com

List of Figures

المنارة للاستشارات

www.manaraa.com

المنارة للاستشارات

www.manaraa.com

List of Tables

المنارة للاستشارات

www.manaraa.com

Table of Contents

المنـــارة للاستشارات

www.manaraa.com

www.manaraa.com

Abstract

Cloud computing is a new paradigm shift of computing offers managed,scalable and secured and high available computation resources and software as a service that enables the users to access to clod services from anywhere and anytime. Mobile Cloud Computing (**MCC**) refers to the availability of Cloud Computing (**CC**) services in a mobile environment and it is the combination of the heterogeneous fields like mobile phone device, cloud computing & wireless networks. Nowadays the term of MCC is become the buzzword and a major discussion thread in the IT world.

Because new technology brings new threats , the security issue is the most important problem that the cloud computing technology has brought, especially the issue of authentication or identification , and to provide safe technological environment for both companies and individual in order to securely use MCC and to create kind of trust between providers and users of this technology .

In this thesis we have deigned a new effective model to solve the identification problem in MCC. And the proposed solution which we have provided is based mainly on the fingerprint to prove the users identity to determine if this user is authorized or not.

Key words: cloud computing, mobile cloud computing, mobile phone device, fingerprint.

المنـــارة للاستشارات

www.manaraa.com

Abstract in Arabic

تعتبر تقنية الحوسبة السحابية نقلة نوعية جديدة في عالم تقنية الحوسبة، حيث أنها تعمل على تقديم المصادر الحاسوبة المختلفة كخدمة للمستخدمين بشكل متكامل، و تعمل ايضا على اتاحة المجال للمستخدمين بادراة هذه المصادر و التوسع باستخدامها حسب حاجة المستخدم، بالاضافة الى انها تمكن المستخدم من الوصول الى خدمات الحوسبة السحابية من أي مكان و في أي وقت. و الحوسبة السحابية المتنقلة تعني امكانية الاستفادة من خدمات الحوسبة السحابية في بيئة الهاتف المحمول، حيث أن هذه التقنية مزيج بين تقنيات عدة مختلفة و هي تقنية الحوسبة السحابية، جهاز الهاتف المحمول بالاضافة الى الشبكات اللاسلكية. في الوقت الحاضر تعتبر تقنية الحوسبة السحابية المتنقلة من التقنيات المهمه جدا التي ينشط مجال البحث فيها نظرا لاهميتها و ما ستحتلة من مساحة كبيرة في المستقبل القريب.

ولأنة التكنولوجيا الحديثة تجلب معها تهديات جديدة، فان أهم ما جلبته معها هذه التقنية من تهديدات هي التهديدات الأمنية و مشكلة الخصوصية و خصوصا مشكلة اثبات الشخصة. و لذلك فاننا عملنا في هذه الرسالة بمعالجة هذه المشكلة لتوفير استخدام آمن لهذه التقنية.

لقد قمنا في هذه الرسالة بتصميم نموذج جديد و فعال من أجل حل مشكلة اثبات الشخصية في الحوسبة السحابية المتنقلة لتوفير بيئة تكنولوجية أمينة لكل من الشركات و الأفراد ، حيث أن الحل المقترح الذي قمنا بتقدمة مبني بشكل أساسي على طبعة الابهام لاثبات شخصية المستخدم لتحديد فيما اذا كان هذا المستخدم مصرح له بالوصول الى الحوسبة السحابية و الاستفادة من خدماتها أم أنة متطفل و غير مصرح له بالدخول الى الحوسبة السحابية و الاستفادة من الخدمات التي تقدمها هذه التقنية.

الكلمات المفتاحية: الحوسبة السحابية، الحوسبة السحابية المتنقلة، جهاز الهاتف المحمول، طبعة الابهام.

المنارة للاستشارات

www.manaraa.com

CHAPTER ONE:INTRODUCTION

المنارة للاستشارات
www.manaraa.com

CHAPTER ONE:Introduction

1.1 Introduction

Mobile phone devices were rare things in the early new century, but now it is very rare to find a house where there is no mobile phone, it has become a mobile device in the time of technological tools which almost never leaves its user, day or night. According to Portio Research the number of mobile phone users that will reach 7.5 billion users by the end of 2014, which means more than three quarters of the world, the mobile phone device is considered one of the most common devices in the history of technology. The mobile phone device in our time has become a key point of contact between people, as well as a key point of contact between businesses and consumers. Mobile phone devices have changed the way of communication between human beings, not only that, but also it contributed to the creation of new businesses. Because the mobile phone device has enormous capabilities in this device that is small in size, light in weight, it is not a device that sends and receives calls only, but also it has a number of amazing advantages, it is a variety of devices in a single small lightweight device.

The emergence of smart phones with high-tech, sophisticated, easy to use, equipped with a large size memory, very fast processor and large touch screens that has enabled us of socializing and communicating with the internet or network connections and the use of web applications and services, and it has also become its capable of storing a large amounts of data of various kinds, for this reasons, mobile phone switched from a complementary device whose use is limited to a certain category of2 people to something essential and irreplaceable and available to everyone, it has become an integral part of our daily lives. Mobile phones has contributed significantly in changing the nature of human life and even institutions of various kinds and activities, the emergence of smart phones have changed the traditional concepts of the names and new concepts have emerged in line with the age of communication and information technology in the field of mobile phones,

المنارة للاستشارات
www.manaraa.com

especially smart ones, the emergence of mobile phones does not only have a technological impact, but also has an economic and social impact.

With the advent of cloud computing, which is considered new technological solutions for both companies and individuals, and what the great benefits it has brought for both of the individuals and companies such as the easy access to data from anywhere and at any times with the possibility to manage it easily, maintaining the data from loss, low cost, the use of computing resources efficiently through low efficiency devices, presenting software and infrastructure as a service for companies and individuals and at low cost. Experts predict that in the year 2020 cloud computing will be an essential part and always in our life, for all these reasons and because the mobile phone has become an indispensable device, the use of cloud computing by mobile has become inevitable and can not be ignored, that will bring a lot of benefits for all members, companies, investors and consumers.
Because new technology brings new threats, the most prominent threats to mobile phones are security ones, which are strongly present, the reason is that mobile phones are small in size and exposed to theft, loss or unauthorized access by hackers. Therefore, the secret and private information on the mobile phone device is exposed to an unauthorized3

use by unauthorized users, and this is a dangerous threat to the mobile phone security. As for the cloud computing and since it's available to everyone, it is also exposed to an unauthorized use by intruders, thus, our private or secret information is exposed to dangerous security threats. Therefore, it is so important to provide a secure use for both of the mobile phones and the cloud computing against these dangers and this is what we are going to try to solve in this thesis.

1.2 Mobile Phone Device

A mobile phone is a device that can make and receive telephone calls over a radio link while moving around a wide geographic area. It does so by connecting to a cellular network provided by a mobile phone operator, allowing access to the public telephone network. In addition to telephony, modern mobile phones also support a wide variety of other services such as Short Message Service (SMS),

المنارة للاستشارات
www.manaraa.com

Multimedia Message Service (MMS), email, internet access, short-range wireless communications (infrared, Bluetooth), business applications, gaming and photography. Mobile phones that offer these and more general computing capabilities are referred to as smart phones [2]; Figure (1-1) shows types of mobile phones device.

Figure (1-1): Types of Mobile Phone Device [3]. 4

المنارة للاستشارات

www.manaraa.com

The mobile phones create a technological revolution in the large communication between people easily, anywhere in the world. In recent years, the mobile phone has become one of the fastest growing communication technologies ever, it is very rare in our time to find someone who does not have a mobile phone, and it has become an integral and irreplaceable part of our daily lives.

1.2.1 Mobile Phone Device Services

The basic service by making the mobile phone is for it to send and receive calls from anywhere in the world without wires via radio waves. But now, and with the great technological development in mobile phones, it offers a variety of services such as Short Messages Service (SMS) is consider more popularity data services on mobile networks at the present time and it allows users to exchange short messages with alphanumeric other users worldwide, Multimedia Messages Service (MMS) is a service for exchange messages that can include any combination of formatted text, images, and photographs, audio and video clips. The Global Positioning System service (GPS) is a Service for geographical positioning, email service is a service enable the users to access their email accounts on any mobile device, internet access service is a service refer to access the world wide web from through mobile device, short-range wireless communications service is a service allows the users to exchange between others via radio waves, business applications, gaming and photography. Mobile phones that offer these and more general computing capabilities are referred to as smart phones; Figure (1-2) shows the services of mobile phones device.

المنارة للاستشارات

www.manaraa.com

Figure (1-2): Mobile Phone Services [4].

1.2.2 Benefits of Using Mobile Phone Device

Mobile phone device has become a popular tool for everyone because it is very convenient and it is a device that provides the user with many benefits, for example, sending SMS and MMS, accessing internet, TV, radio, calculator, taking photographs and videos, playing games, GPS. Although the benefits of mobile, but there are some risks associated with it. The mobile risk includes virus coming from SMS, Bluetooth and PC, data loss due to theft or loss of mobile devices, accessed by unauthorized users, and internet scam or virus infection when accessing network by mobile [5,6].

المنارة للاستشارات
www.manaraa.com

1.2.3 Mobile Phone Device Security

Mobile phone device is not just a device being calls and sends messages only but it also became in our current era (digital revolution era), like a small computer and laptop. Through this small device size we can accomplish many daily chores and sometimes there are tasks cannot accomplish only through mobile. This little device the size that contains all our secrets information or some of them and information that are considered a very private and confidential. This information may be exhibition of loss or theft, and here lies the problem where we are in this case presented our secret and private information to those who stole or found this device or may be the mobile device being attacked by attackers and hackers, and it can be used by a hacker as an access point into many other aspects of your digital life as well the lives of others in your network. And from here we must to think in ways more serious to protect the contents of the mobile phone device information and applications for the device becomes useless for those who find it or steal the mobile phone device. So that security mobile services are needed for authentication, integrity, user privacy and non- repudiation.

1.2.4 Mobile Cloud Computing

Mobile Cloud Computing (MCC) refers to the availability of Cloud Computing (CC) services in a mobile environment; Figure (1-3) shows mobile cloud computing Architecture. It incorporates the elements of mobile networks and cloud computing, thereby providing optimal services for mobile users. In MCC, mobile devices do not need a powerful configuration (e.g., CPU speed and memory capacity) since all the data and complicated computing modules can be processed in the cloud [8].

للاستشارات المنارة
www.manaraa.com

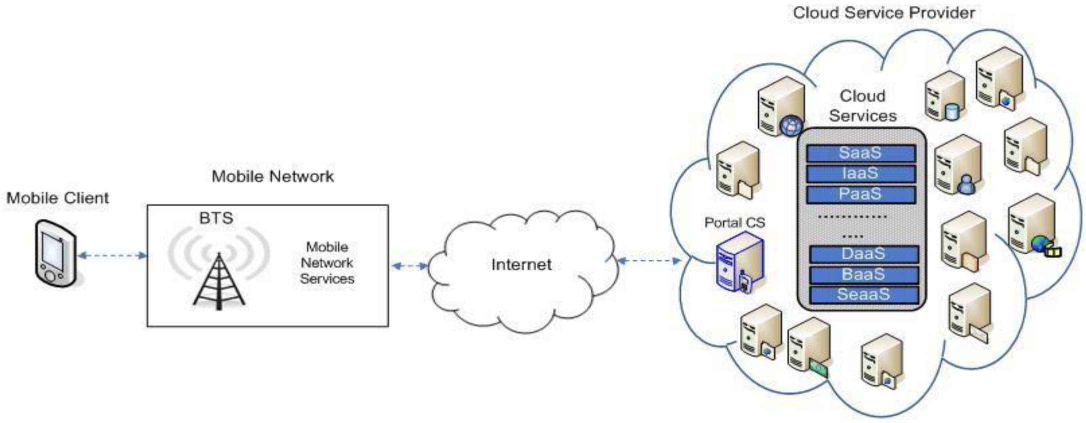


Figure (1-3): Mobile Cloud Computing Architecture [7].

7

المنارة للاستشارات
www.manaraa.com

In MCC the users can get all the CC services in his or her mobile devices through internet. Mobile cloud merged the elements of mobile networks and cloud computing, thereby providing the optimal services for mobile users. Mobile cloud computing which combines mobile computing and cloud computing, has become one of the industry buzz words and a major discussion thread in the IT world. And according to ABI Research [9], “By 2015, more than 240 million business customers will be leveraging cloud computing services through mobile devices, driving revenues of $5.2 billion”. It must be noted that there were only 42.8 million MCC subscribers in 2008 [9]. This underlines the end mobile device user will eventually be the benefactor of the MCC. Company users can share resources and applications without a high level of capital expenditure on hardware and software resources. Nature of cloud applications also is advantageous for users since they do not need to have very technical hardware to run applications as these computing operations are run within the cloud. This reduces the price of mobile computing to the end users. They could see a huge number of new features enhancing their phones due to MCC. At the same time the developers also have real advantages from mobile cloud computing. The largest benefit of cloud computing for developers is access to a broader audience of a wide range of mobile subscribers. Since cloud computing applications go through a browser, the end user’s mobile operating system does not have any impact on the application. Along with the plethora of benefits, there are a large number of issues to be addressed and unsolved problems to be solved. Several challenges such as the dependency on continuous network connections, data sharing applications and collaboration, and security another key challenge for MCC is network availability and intermittency. Also MCC8 concepts rely on an always-on connectivity and will need to provide a scalable and high quality mobile access.

المنارة للاستشارات
www.manaraa.com

1.3 Cloud Computing

Cloud is a new paradigm shift of computing for enabling convenient, on-demand network access to a share pool of configurable computing resources (e.g. network, service, storage, application, and service); that can be rapidly provisioned and released with minimal management effort or service provider interaction [10].

The term cloud also used often as a metaphor for the internet, and currently is further used as an abstraction of complexities .Cloud computing builds on established trends for driving the cost out of the delivery of services while increasing the speed and agility with which services are deployed. It shortens the time from sketching out application architecture to actual deployment. Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software. Because cloud computing is available to everyone, they need to authenticate in order to ensure the entry is authorized to use cloud computing services.

1.3.1 Cloud Computing Deployment

Cloud computing is classified into four basic types of cloud deployment models. They are public, private, hybrid, and community of clouds; Figure (1-4) shows the types of cloud computing [10].

المنارة للاستشارات
www.manaraa.com

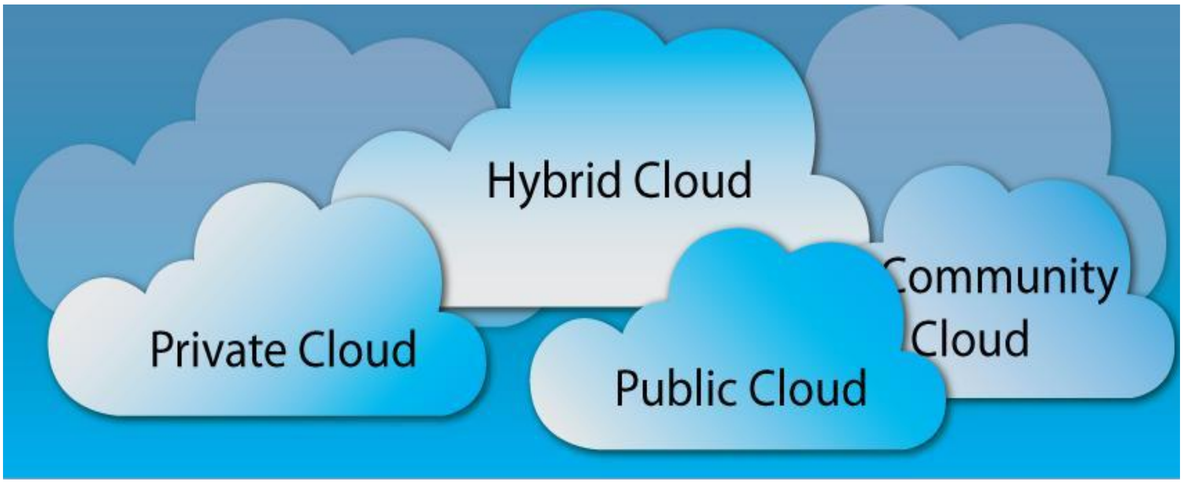


Figure (1-4): Types of Cloud Computing [11].

❖ **Public Cloud**

Provide a pool of shared computing resources, applications, and storage

to the customer as a single virtualized service. They generally allow you to grow or shrink these resources as needed and oftentimes provide built-in failover and redundancy. But, they are delivered (as the name suggests) publicly and in a defined fashion, so you are unable to secure your services with a private firewall or access them privately over your Wide Area Network (WAN) [10]**.**

❖ **Private Cloud**

Provide a dedicated instance of these services for your exclusive use and, as a result, can be secured and accessed privately. While they are housed in provider's data center, they do not leverage the pool of shared resources, so they cannot grow and shrink and do not include failover and redundancy. Private Clouds most of the times utilize the same technology (hardware, virtualization, and security) as an on-premise deployment, but they are outsourced to a service provider for hosting and care and feeding of the environment [10].

المنارة للاستشارات

www.manaraa.com

❖ Hybrid Cloud

The cloud infrastructure is a combine of two or more distinct cloud infrastructure like public, private and community. That remains unique entities, but is bound together by standardized or proprietary technology that enables data and application portability. Application with less stringent security, legal, compliance and service level requirements can be outsourced to the public cloud, while keeping business-critical services and data in a secured and controlled private cloud [10].

❖ Community Cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations) [10].

1.3.2 Cloud Computing Services

Cloud computing has three primary most widely used service models of cloud computing. These services include Software as a service, platform as a service, and infrastructure as a service; Figure (1-5) shows the service of cloud computing.

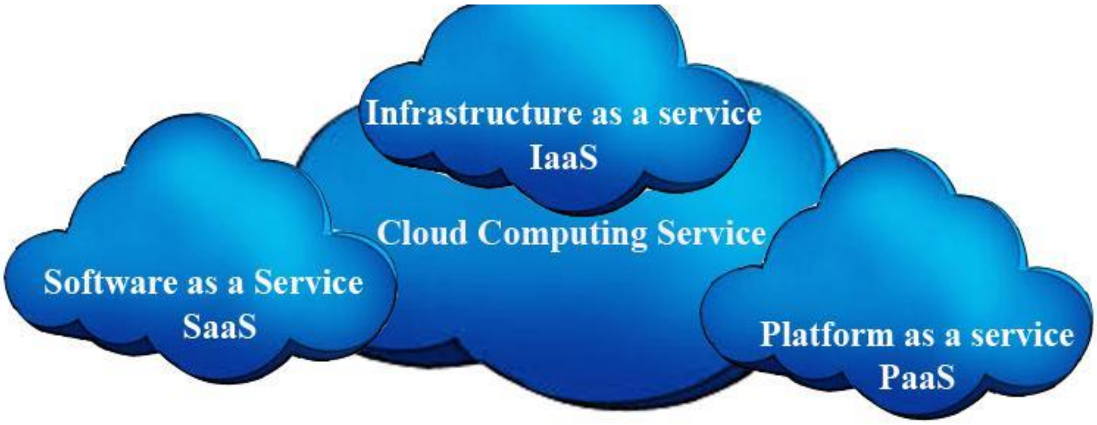


Figure (1-5): Services of Cloud Computing.

المنارة للاستشارات
www.manaraa.com

❖ Software as a Service (SaaS)

The capability provided to the customers is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client infrastructure such as a web browser (e.g., web-based e-mail). The consumer dose not manage or the underlyingcloud infrastructure including network, servers, operating systems, storage, or even individual applications capabilities, with the possible exception of limited user-specific application configuration settings [10].

❖ Platform as a Service (PaaS)

The capability to provide to consumer is to deploy onto the cloud infrastructure consumer-created or required applications created using programming language and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possible application hosting environment configurations [10].

❖ Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components [10].

1.3.3 Benefits of Cloud Computing

Cloud computing brings many benefits as reduce initial investment, reduce capital expenditure, improve industrial specialization, and improve resource utilization. And it has many proprieties and Characteristics.

المنارة للاستشارات

www.manaraa.com

1.3.4 Properties and Characteristics of Cloud Computing

Cloud computing is a paradigm of computing, a new way of thinking about IT industry and it has five essential characteristics of cloud computing; Figure (1-6) Cloud proprieties and Characteristics.

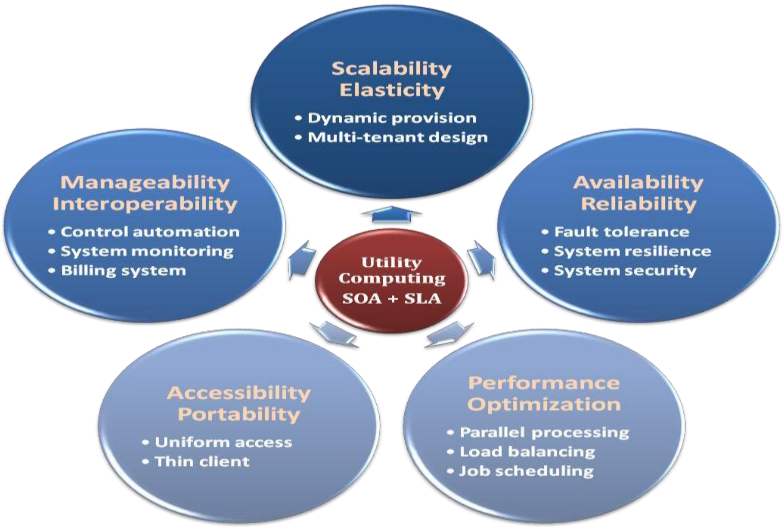


Figure (1-6): Cloud Proprieties and Characteristics [10].

❖ Scalability & Elasticity

Clients should be able to dynamically increase or decrease the amount of infrastructure resources in need, large amount of resources provisioning and deployment should be done in short time, and system behavior should remain identical in small scale or large one [10].

❖ Availability & Reliability

Clients should be able to access computation resources without considering the possibility of hardware failure, Data stored in IaaS cloud should be able to be retrieved when needed without considering any natural disaster damage, and Communication capability and capacity should be maintained without considering any physical equipment shortage [10].

للاستشارات المنارة
www.manaraa.com

❖ Manageability & Interoperability

Clients should be able to fully control the virtualized infrastructure resources which allocated to them, Virtualized resources can be allocated by means of system control automation process with pre-configured policy, States of all virtualized resource should be fully under monitoring, and Usage of infrastructure resources will be recorded and then billing system will convert this information to user payment [10].

❖ Performance & Optimization

Physical resources should be highly utilized among different clients, Physical resources should form a large resource pool which provides high computing power through parallel processing, and Virtual infrastructure resources will be dynamically configured to an optimized deployment among physical resources [10].

❖ Accessibility & Portability

Clients should be able to control, manage and access infrastructure resources in an easy way, such as the web-browser, without additional local software or hardware installation, and provided infrastructure resources should be able to be reallocated or duplicated easily [10].

1.4 Authentication

Authentication means verifying the identity of who wants to access data, resources, or applications. Validating that identity establishes a trust relationship for further interactions. It is considered very important process to prevent any illegal access to any data, sources, or applications through any unauthorized persons to protect the privacy and to provide secure used.

1.4.1 Authentication Methods

There are many ways used to authenticate the secure use of data, resource or applications; Figure (1-7) shows some methods of authentications.

المنـــارة للاستشارات
www.manaraa.com

Figure (1-7): Methods of Authentications.

❖ Password

Passwords are the most widely used form of authentication. The Password is typed unobtrusively in order to Tver protection dramatically so as not to share it with others. This type of authentication in general simple and does not require much processing.

❖ One-time Password

A One-Time Password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks [2].

❖ Digital Signatures

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering [2].

المنارة للاستشارات
www.manaraa.com

❖ Biometric Authentication

Biometrics is the science and technology of measuring and analyzing biological data. It is used to uniquely identify individuals by their physical characteristics or personal behavior traits. It is used to allow users access to data, resource or applications [12].

1.5 Fingerprint

Fingerprints are graphical ridge patterns present on human fingers, which, due to their uniqueness and permanence, are among the most reliable human characteristics that can be used for people identification [13]. Fingerprints are classified into three different groups based on the pattern of the ridges which are Arches, Loops and Whorls; Figure (1-8) shows the types of fingerprints pattern.

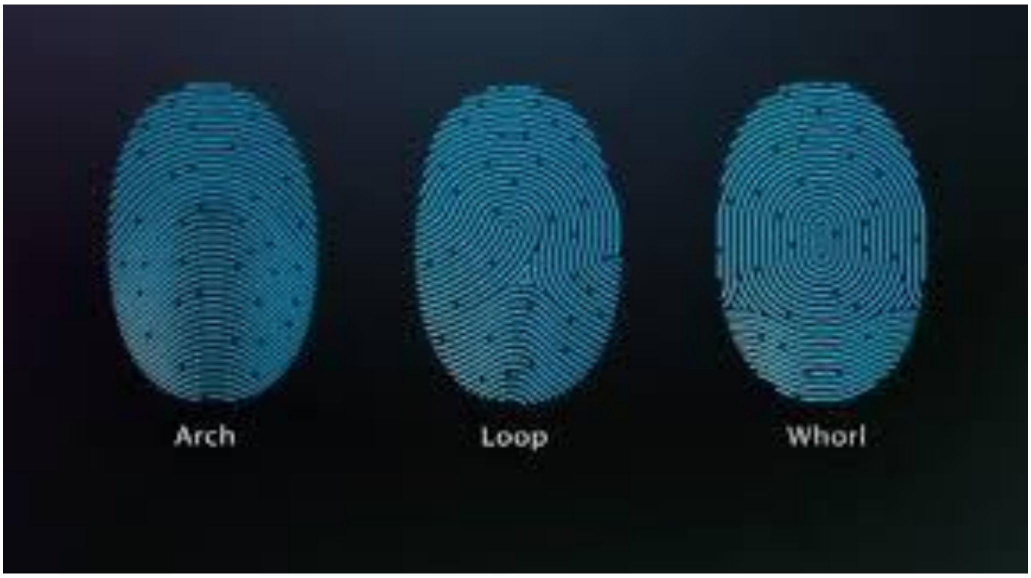


Figure (1-8): Types of Fingerprints Pattern [14].

There are three phases of fingerprint recognition system, the first one is fingerprint acquisition which is used to capture fingerprint image by special sensors. The second phase is feature extraction used to extract the main dots of fingerprint image and save them into specific format.

المنارة للاستشارات
www.manaraa.com

The third phase is fingerprint matching used to compare previously stored templates of fingerprints to candidate fingerprints for authentication purposes; Figure (1-9) shows the fingerprint recognition system.

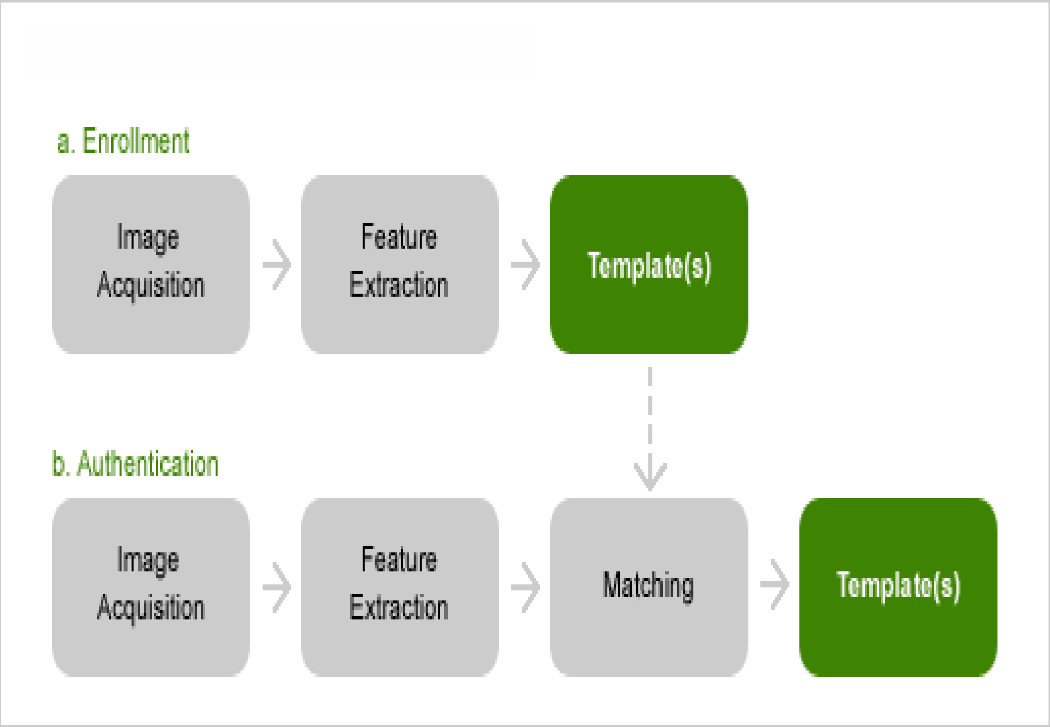


Figure (1-9): Fingerprint Recognition System [15].

There are several reasons to use a fingerprint such as recognition requires a minimal effort from the user, does not capture other information than strictly necessary for the recognition process, and provides relatively good performance [16].

1.5.1 Fingerprint Image Preprocessing

The quality of fingerprint has a great influence on the performance of a fingerprint matching system therefore we must process the noise of fingerprint image to facilitate the extraction of fingerprint features of fingerprint image by using some image enhancement technique. The process of enhancing the image before the feature extraction is called pre-processing.

المنارة للاستشارات
www.manaraa.com

1.6 Thesis Organization

This thesis focuses on explaining the security issue of mobile cloud computing, and then proposes a new method to authenticate the secure use of cloud computing through mobile. In order to achieve this, this thesis is organized in the following manner:

Chapter One: summarizes the main concepts of mobile phone device,cloud computing, mobile cloud computing, authentication and fingerprint.

Chapter Two: the literature review, it includes many researches regarding to the security issue on both cloud computing and mobile cloud computing that helps understanding what have been already tested and implemented so it gives us a head start to complete from the point where others stopped.

Chapter Three: the theoretical design which is a description of the proposed solution for the research problem.

Chapter Four: this chapter contains the implementation of the proposed solution in order to solve the authentication issues on mobile cloud computing by using the fingerprint authentication and the actual of design model.

Chapter Five: this chapter includes conclusions and future works, illustrations the result of the implementing of the proposed solution to solve the authentication issue on mobile cloud computing, then the suggested future works related to this subject is introduced from the researcher's point of view.

المنارة للاستشارات
www.manaraa.com

CHAPTER TWO: LITERATURE REVIEW

www.manaraa.com

CHAPTER TWO:Literature Review

2.1 Introduction

Cloud computing has imposed itself as a new technology can not be abandoned, and because of the important services they provide to its users. It is a technology that can be accessed from anywhere and at any time, and allows users to store their files cheaply and without concern from the loss. It is also offering a variety of services to its users, such as providing SaaS and IaaS. We should seriously think about cloud computing protection from penetration or unauthorized access. The cloud computing is available to everyone, contain millions of important information, provide many important services to its users that can access it by authorized user just, and using cloud computing through mobile phone device added new challenges related to security for both providers and users. Therefore the providers of cloud computing service must provide secure use to their customers.

With regard to fingerprint authentication or sometimes called fingerprint recognition, it is perfect way to authenticate individuals, who have accounts on internet website services, through their fingerprints. There are many reasons to use fingerprint in security era, some of these reasons that every human being has unique fingerprints, can't be lost, can't be stolen, difficult to falsify. Fingerprint recognition system is Consist of three phases, the first one is fingerprint Acquisition which is used to capture fingerprint image by special sensors. The second phase is feature extraction used to extract the main dots of fingerprint image and save them into specific format. The third phase is fingerprint matching used to compare previously stored templates of fingerprints to candidate fingerprints for authentication purposes.

In this chapter, we will discuss the Statement of Problem and show the previous work associated with this thesis.

المنارة للاستشارات
www.manaraa.com

2.2 Statement of Problem

Using cloud computing over mobile devices securely without any threats from hackers and ensuring the use the mobile cloud computing in a secure way regardless of any breaches or unauthorized access to the cloud account that could occur by hackers. This can be applied by using one of the authentication methods which is the fingerprint. Most of the new Mobile devices use fingerprint as a method for user authentication. It is possible to use this criterion for cloud user authentication.

2.3 Literature Review

Cloud computing is a new paradigm shift will be a big change of network world, but there are many issues threat using the cloud computing, the most significant one is security aspects.

There are many researches in cloud computing field which are focused on the security aspects. These aspects are used to ensure the secure use between the cloud computing servers and its user especially using the cloud computing through the mobile phone device.
In this chapter, we will present related works that are focused on security aspect. With regard to fingerprint authentication, it is perfect way to authenticate individuals, who have accounts on internet website services,through their fingerprints. It is a great idea for use the fingerprint authentication in mobile cloud computing to protect it from the challenges facing this new technology.

Michał Szczepanik & Ireneusz J´o´zwiak [17]
They proposed a selective attention algorithm which increases the reliability of biometrics security system based on fingerprint recognition.
They made a comparison between the existing fingerprint recognition algorithms and examined their own algorithm on fingerprints database which changes the structure as a result of physical damage.
They proposed new selective attention algorithms, which helped the detecting of the most sensitive to damaged areas, and added it as a step of fingerprint analysis for the fingerprint recognition procedures. They also proposed

المنارة للاستشارات
www.manaraa.com

a new algorithm that does not require complex hardware systems, so it can be applied in new smart mobile devices, which restrict unauthorized access to sensitive data or other user resources.
This paper proposed a new step for fingerprint matching approach, which is based on selective attention. The proposed solution can be used by everyone who is exposed to damage of fingerprints. The system can also be applied to protect access to important data or premises which are very important for mobile device users but it required devices with better performance

Marius Tico & Pauli Kuosmanen [18]

This paper introduced a representation scheme for fingerprint patterns that permit nonminutia features integration as well as the minutia details of the fingerprint. The basic idea consists of the appearance description of the fingerprint pattern with respect to each landmark point (minutia), in a capture attempt of more characteristic features from the reach information content presented in the fingerprint.Their work investigated the integration of ridge orientation information into the fingerprint representation. This representation: provides additional nonminutiae information for calculating a more reliable degree of similarity between fingerprint impressions; which allows the design of a low complexity algorithm for solving the feature correspondence problem; and decreases the interdependencies among minutia details, which can be missed or erroneously detected by a minutiae extraction algorithm.

This paper presented a novel fingerprint representation scheme that depends on describing the orientation area of the fingerprint pattern with respect to each minutia detail. This representation permits the derivation of a similarity function between minutiae that is used to identify corresponding characteristics and assessing the resemblance between two fingerprint impressions. The proposed representation is developed and examined with a series of experiments conducted on two public domain collections of fingerprint images just.

www.manaraa.com

Weiwei Jia Haojin Zhu, Zhenfu Cao & et al [19]

The authors designed a Secure Mobile User-based Data ServiceMechanism (SDSM) to provide confidentiality and fine-grained access control for data stored in the cloud. This mechanism enables the mobile users to enjoy a safe outsourced data services at a minimized security management overhead.

The main idea of SDSM is that SDSM outsourcers not only the data but also the security management to the mobile cloud in a trusted way. Their analysis illustrated that the proposed mechanism has many advantages over the existing traditional approaches such as lower overhead andcomfortable update, which could better cater the requirements in mobile cloud computing scenarios to improve the security of mobile cloud users.

This paper discussed the privacy problems faced by the data stored in cloud computing and it tried to solve these problems by proposing a mechanism to provide confidentiality and fine-grained access control for data stored in the cloud. But the proposed mechanism needs high cost of an access policy and communication update.

Akhil Kaushik, Hari Om Awashti & et al [20]

This paper proposed three different methods to safely and easily login to a cloud service using one time password with the user's mobile phone as an authentication device. Furthermore, three different suggestions that are secure and easy to use for registering new users to the cloud service have been made.The best encryption algorithm to use in cloud services with respect to security and speed has been evaluated. The Suggestion ended up in a working solution that uses one time password authentication in a mobile for the login procedure, a very safe registration system and with all traffic transmissions encrypted with RC4.

للاستشارات المنارة
www.manaraa.com

This paper talked about cloud computing concepts and presented a solution to the lack of trust between the parties in cloud computing environment by using OTPs with the user's mobile phone as an authentication device. This solution is impractical, especially when a mobile phone is stolen; it becomes available for the robber who can easily use the cloud computing.

Neeraj Bhargava & et al [21]

This paper mainly discussed the performance analysis of the cloud computing. The general performance of cloud computing relies on “How light the interface?” and “How is the availability of resources at the server?” It discusses essential application areas of cloud computing and concludes that performance of data center is affected by distance and number of users. It is a new stage of information technology, where companies are competing by offering free cloud storage with an attractive interface. The cloud itself has distinguished meaning when it integrates with internet as a bridge, so any computer from the internet can access the cloud. The author in this paper has expanded types of service model in cloud computing to Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Communication as a Service (CaaS), Monitoring as a Service (MaaS) and Database as a Service (DaaS).

This paper discussed the performance of the cloud computing, the core application areas of cloud computing and it mentioned the types of service models in cloud computing. This research mainly focuses on the performance analysis of the cloud computing.

Soeung-kong, Jung-Hoon Lee & Sung Woo Kim [22]

The authors talked about security issues concerning mobile cloud computing. Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers pay attention to. Because mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into categories: mobile network user's security, and mobile cloud security.

للاستشارات المنارة
www.manaraa.com

This paper talked about the security issue of mobile cloud computing and the data privacy and integrity of mobile cloud computing user's and it mentioned that the security issue is one of the key issues of mobile cloud computing.

Nithiavathy.R & et al [23]

The authors proposed an effective method to accomplish secure and reliable cloud storage by using distributed storage integrity auditing mechanism, which incorporate homomorphic token and distributed erasure-coded data for dynamically storing data.

The proposed design permits the user with lightweight communication and computation cost. To keep reliable cloud storage correctness, and to locate the misbehaving server in which the data are frequently changing in a cloud. This research design allowed the user with lightweight communication and computation cost, to maintain reliable cloud storage correctness, and to locate the misbehaving server in which the data are frequently changing in cloud.

This paper has discussed the threats of mobile cloud computing security. The researcher addressed this problem by proposing an effective method to accomplish safe and dependable cloud storage by using distributed storage integrity auditing mechanism, which incorporate homomorphic token and distributed erasure-coded data for dynamically storing data.

المنارة للاستشارات
www.manaraa.com

Jaejung Kim & Seng-phil Hong [24]

The authors suggested a secure and convenient user authentication model that mobile phone device users can effortlessly use credentials in cloud computing environments. Also they discussed the security and privacy issues of the current user authentication model that is not able to supply credential roaming in cloud computing environments. This inability is resulting from the absence of securely available credential protocol in consolidated user authentication method. In order to solve this problem, the paper proposed the secure Consolidated Authentication Model (CAM) architecture so that one credential is applicable to various mobile devices in cloud computing environments.

This paper suggested the secure CAM architecture in cloud computing environments, which not only does it provide more flexible authentication framework but also leads to safer credential management in operating various mobile devices such as smart phones, smart pads, etc. Also it defines framework architecture, credential profile, protocol framework for consolidated authentication mechanism in order to provide an appropriate user authentication model for acloud computing environments.

This paper has mentioned that the access to the internet through smart phones and pads has become essential because the access to the internet through the smart phones and pads allows the user to access the available services on the internet. There are many issues that make use of user concern of these services and the most important of these issues are security and privacy issues.

Mrs. Yogita D. Mane & Prof. Kailas K. Devadkar [25]

The authors discussed protection in regard to concerns in mobile cloud computing, which consists of an introduction to all issues which are related to security issues of mobile cloud computing.

www.manaraa.com

Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers pay attention to. Since mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: mobile network user's security; and mobile cloud security.

This paper presented the results of a questionnaire on the issues faced by mobile cloud computing, these issues are divided into two parts: the issue of security and privacy. Also it discussed security issues of mobile cloud computing briefly.

Thamba Meshach W & Suresh Bab K S [26]

The researchers suggested authenticated key exchange scheme, namely Mobile Cloud Key Exchange (MCKE), which aimed at efficient security-aware scheduling of scientific applications? The scheme has been designed based on the commonly-used Internet Key Exchange (IKE) scheme and randomness-reuse strategy, both theoretical analyses and simulation results have demonstrated that. Compared with the IKE scheme, the MCKE scheme has significantly improved the efficiency by dramatically reducing time consumption and computation load with the same level of security.

In this paper the authors stated that the biggest challenge in both cloud and mobile technologies right now is security. The authors proposed an authenticated key exchange scheme and namely mobile cloud key exchange to solve this issue. But the suggested scheme is more time consuming.

Swati P. Ramteke & et al [27]

The researchers suggested a new model for data storage and access in clouds. The model scheme avoids storing multiple encrypted copies of same data. Model designed for secure data storage, cloud stores cyphered data (without being able to decrypt them), and the main innovation of a proposed model is addition of Key Distribution Centers (KDCs).

المنارة للاستشارات
www.manaraa.com

This paper talked about privacy and intrusion issue that are facing the sensitive data stored in the cloud computing. To address this problem the researchers suggested a solution which removes the trusted central authority, and protects the user’s privacy by preventing the authorities from pooling their information on particular users. But this paper did not improve the security features in cloud computing environment.

In this chapter we have presented literature review which is related to the research of this thesis. This chapter discussed cloud computing and mobile cloud computing in general, and declared the main challenges in the cloud such as security, privacy and authentication. Some papers talked about fingerprint recognition and mentioned that there are three phases of fingerprint recognition; the first one is fingerprint acquisition then feature extraction and finally the fingerprint matching .this chapter talked about the main challenges faced by the fingerprint recognition.

All the literature reviews explained that the main problem in all challenges is how to prevent unauthorized user from accessing the cloud computing, but did not present a particular method for protection of cloud and how to prevent unauthorized user from accessing the cloud.

In this thesis we have suggested method checking the user authorization and presenting a method to the users for securing access to their own data and applications in the cloud through mobile phone device.

المنارة للاستشارات
www.manaraa.com

CHAPTER THREE:THE PROPOSED MODEL DESIGN

المنارة للاستشارات
www.manaraa.com

CHAPTER THREE:The Proposed Model Design

3.1 Introduction

Cloud computing and mobile phone device are considered new technology and widely used in these days, therefore using cloud computing through mobile is inventible, because the mobile device became almost never leaves its user day or night. According to Portio Research the number of mobile phone users that will reach 7.5 billion users by the end of 2014, which means more than three quarters of the world. Using the cloud computing through mobile is called mobile cloud computing, which is very a perfect idea to using cloud computing through a mobile phone device, because it will bring many benefits to both customers and companies. From these benefits that users can access their files or applications which are stored in cloud from anywhere and at any times with the possibility to manage it easily. Maintaining the data from loss, low cost, the use of computing resources efficiently through low efficiency devices, presenting software and infrastructure as a service for companies and individuals and at low cost…etc. Because new technology brings new threats, the most prominent threats to mobile phones and cloud are security ones.

Passwords and usernames are a traditional method to make any users authorized, and because the password and username exhibition of loss, theft or forgetfulness, it was necessary to find a safer way to maintain privacy and data security. Fingerprint authentication or sometimes called fingerprint recognition, is perfect way to authenticate an individuals, who have an account on internet website services, through their fingerprints. There are many reasons to use the fingerprint in security era, from these reasons that every human being has unique fingerprints, can't be lost, stolen, and difficult to falsify.

In this thesis, we designed new efficient security model for mobile cloud computing that enables users to use ten fingerprints instead of one in order to choose the suitable password to authenticate themselves on cloud computing through mobile phone device.

المنارة للاستشارات
www.manaraa.com

3.2 The Proposed Solution

In this thesis, we have designed a new efficient model, this model scans all the user's fingerprints with their password which is considered a new and good idea because it will provide more security to the mobile cloud computing, in this model the user can choose any fingerprint and its password he/she wants in order to authenticate himself/herself on the mobile cloud computing where the suggested solution goes by scanning the ten fingerprints and then the password of each entered fingerprint, and the fingerprint's password is the user's original password as well as the fingerprint position in the hand. For example: if the user's original password is (Jalaljuneidi), then the fingerprint's password will be (JalaljuneidiL1) where L refers to the left hand and number 1 refers to the finger's order in the left hand. Then, the scan fingerprint along with its password are sent and stored in the database in the cloud computing server, where the matching process is performed later between the stored fingerprint and the fingerprint that will be used by the user who wants to access the account on the cloud computing through a mobile phone device. When the user wants to access the account, he/she must enter the defined password of the proposed model, and then the fingerprint will be entered with its password. If the password of the read fingerprint is valid, the application will match it with the previously stored one in the database. If both fingerprints are matched, the user will be authorized to access the cloud computing and can get benefit from the cloud computing utilities; Figure (3-1) shows the proposed solution. In this thesis, we will use the basic fingerprint algorithms, one for fingerprint orientation, another is for the fingerprint feature extraction and the last is for the matching process.

المنارة للاستشارات
www.manaraa.com

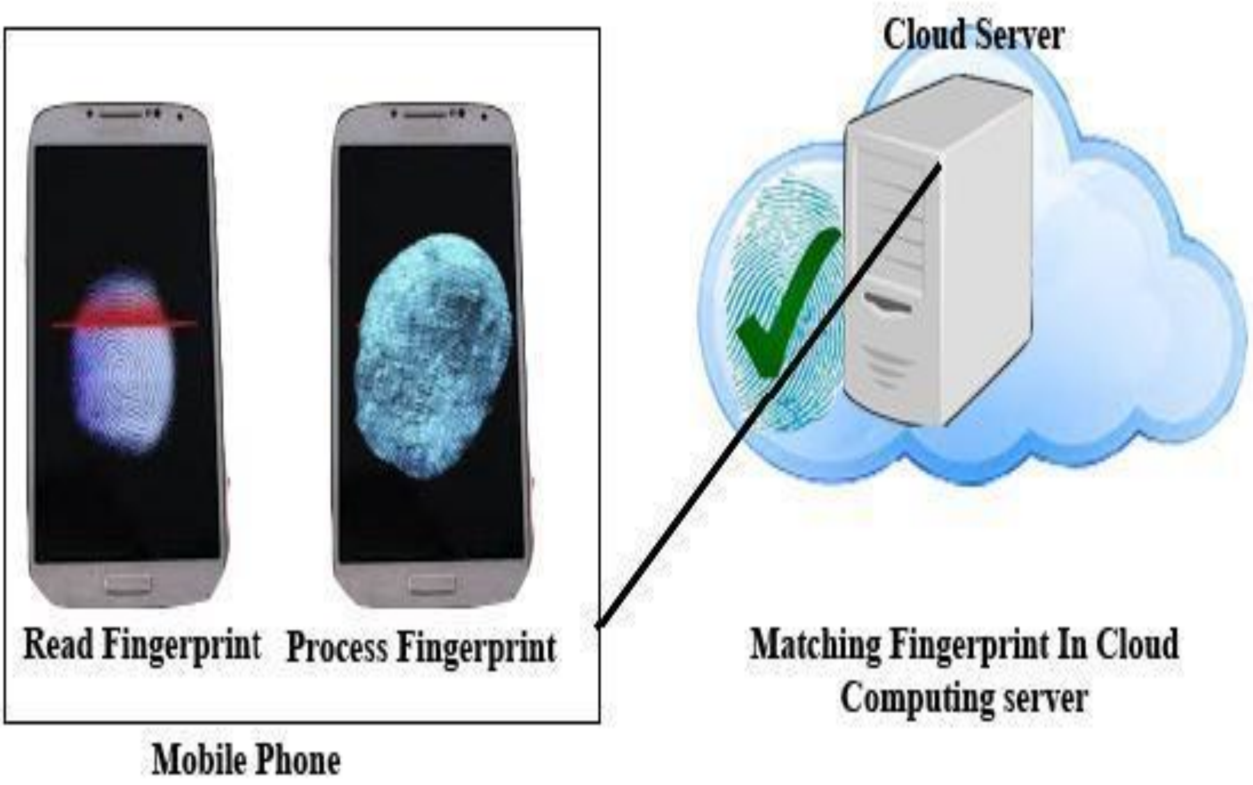


Figure (3-1): Fingerprint Authentication Model

المنارة للاستشارات
www.manaraa.com

3.3 The Proposed System Design

The proposed system design consists of two stages:-

- ❖ Store the fingerprints (fingerprint features) in the data base (new user stage).
- ❖ Matching the fingerprints (fingerprint features) with the fingerprints that were previously stored in the cloud server's database (registered user stage).

The proposed model consists of two stages; the first one is used by new users in order to sign up a cloud account for them on the proposed application. At this stage the new user must enter a user name and a password and then scan the fingerprints of ten fingers on both hands. The user must set a password for each fingerprint; after the user completes the registration process the system sets the sign as a registered user in the system. The second phase is dedicated for registered users, while if the user is registered, he must first enter the password in order to gain access to the system interface for registered users to complete the security measures required for entry to the system and access to cloud computing. And if the user enters the wrong password, he is considered an intruder user, and therefore he will not be able to access to the cloud computing; Figure (3-2) shows the algorithm of proposed model.

المنارة للاستشارات
www.manaraa.com

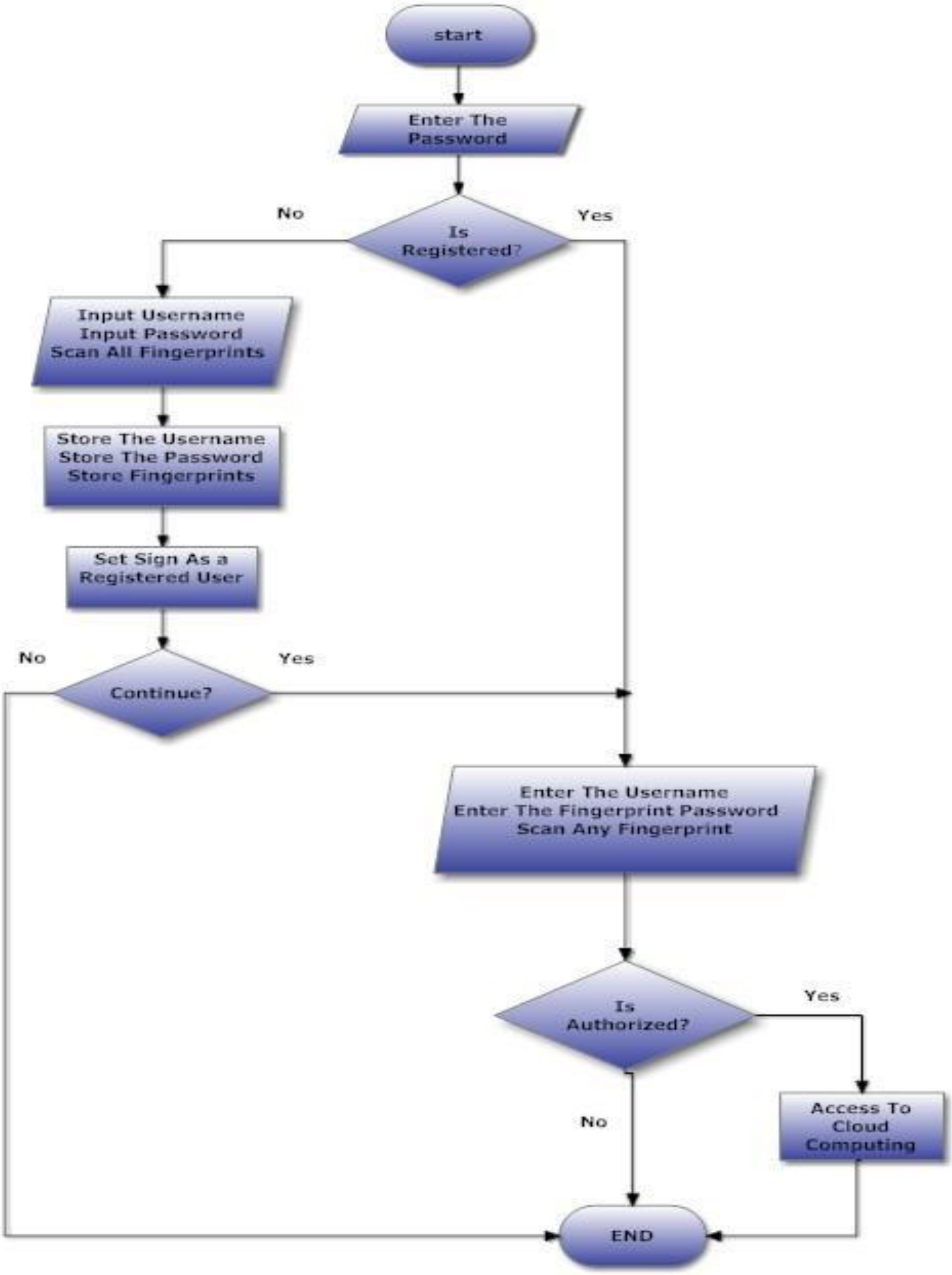


Figure (3-2): The Proposed Model.

المنارة للاستشارات
www.manaraa.com

Algorithm: the proposed model algorithm. //
- Input: user password, username, fingerprints and its password.

- This algorithm used to determine the user is authorized or unauthorized. //

```
Input password
IF registered user THEN
Input username
Input fingerprint password
Scan any fingerprint
IF username, fingerprint password, fingerprint match THEN
Access to cloud computing
Else
Reject user
End if
Else
Input username
```

المنارة للاستشارات
www.manaraa.com

```
Input password
Scan all fingerprints
Store username
Store password
Store all fingerprints
Set sign as a registered user
IF user want to continue THEN
Input username
Input fingerprint password
Scan any fingerprint
IF username, fingerprint password, fingerprint THEN
Access to cloud computing
Else
Reject user
```

www.manaraa.com

```
End if
Else
End
End if
End
```

3.3.1 Store the Fingerprints (fingerprint features) in theDatabase (New-user Stage)

This stage also called new user-stage, in this stage the user will be registered by entering username and password, then the user must scan all the fingerprints with password for each fingerprint (fingerprint password is the original password plus the location of the finger in the user's hand). After that the fingerprint features with its passwords will be send to the database to store it for the next stage, then the system set sign as registered user to distinguish later between the new user and registered user; Figure (3-3) shows store fingerprint features with it's password algorithm.

المنارة للاستشارات
www.manaraa.com

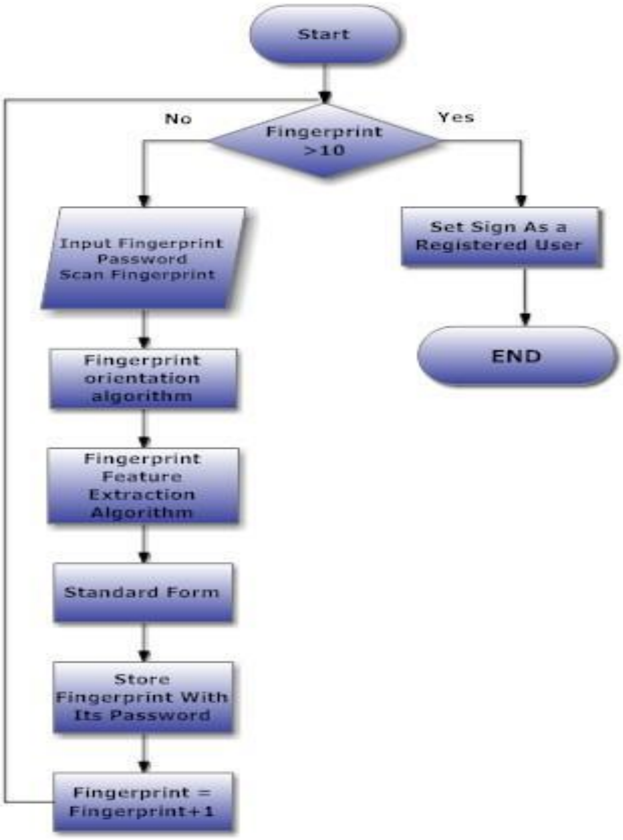

Start
No
Fingerprint >10
Yes
Input Fingerprint Password Scan Fingerprint
Set Sign As a Registered User
END
Fingerprint orientation algorithm
Fingerprint Feature Extraction Algorithm
Standard Form
Store Fingerprint With Its Password
Fingerprint = Fingerprint+1

Figure (3-3): Fingerprint and its Password Storing.

Algorithm: fingerprints acquisition and store it's in the database. //
- Input: fingerprints and its password.

- This algorithm used to read fingerprint and its password and store the feature of these fingerprint and its password in the database.

```
// X←10

I← 1 to X


IF I < 10 THEN


Input password
```

المنارة للاستشارات
www.manaraa.com

```
Input fingerprint
Oriented← fingerprint
Feature-extraction← oriented [fingerprint]
Stander-form← fingerprint-features
Store← fingerprints-user [Stander form] fingerprints [password]
I←I + 1
Else
Set as a registered user
Exit
End loop
```

3.3.2 Matching the Fingerprint and Password Stage (Registered-User Stage).

This stage also called registered user-stage, in this stage the user must enter the password to open the mobile device, then must enter the username and fingerprint password, then in the second level the user must enter the fingerprint password and if it is valid the user will go to the next level and if it is wrong the user will be rejected because the user is un authorized. If the user entered valid fingerprint password, then he/she must send fingerprint by special sensor that is located on mobile phone devise.

المنارة للاستشارات
www.manaraa.com

After the user fingerprint has been read and send to the date base, the system will match it with the fingerprint that was previously stored in the cloud server's data base and if the matching is ok, the user will be considered as authorized and any process can be done on the cloud account; Figure (3-4) shows fingerprint and its password algorithm.

Figure (3-4): Fingerprint and its Password Matching.

```
Algorithm: fingerprints and its password matching. //
- Input: fingerprints and its password.

- This algorithm used to read finger password then check if it is valid
or no, and if it is valid the algorithm do matching process between the
stored fingerprint and the fingerprint that will be used by the user
when he wants to access his account on the cloud computing.
//

Input password

IF password valid THEN

Input username

Input fingerprint_password

Scan fingerprint

Oriented ←fingerprint

Features ← extract [oriented fingerprint]
```

المنارة للاستشارات
www.manaraa.com

```
Matching← match [features]
IF username, fingerprint password, fingerprint match THEN
Access to cloud computing
Else
Reject user
End If
Else
Reject user
End if
```

In this thesis we present new security model depend on fingerprint and its password to solve authentication issue on mobile cloud computing that is used through mobile phone devise (mobile cloud computing), our model is new and efficient to protect mobile cloud computing from security threats. In chapter four we will explain the proposed solution in practical method.

المنارة للاستشارات
www.manaraa.com

CHAPTER FOUR:IMPLEMENTATION NDEXPERIMENTAL WORKS

المنارة للاستشارات
www.manaraa.com

CHAPTER FOUR:Implementation and Experimental Works

4.1 Introduction

The mobile cloud computing as mentioned before in previous chapters is available for everyone and both companies and individuals can benefit from the services provided by this new technology. Experts expect that it will play a great role in the world of technology and it will be increasingly used and the reason is that the users can access their files stored in the mobile cloud computing. Furthermore, it provides the software as a service and it also provides the service of infrastructure in addition to many other services that can be beneficial for many companies and individuals and they can access these services from anywhere and at any time with the cheapest prices and so easily.

The use of the mobile cloud computing through a mobile phone device has made it more common and usable than ever. Since the mobile phone device is small in size, light in weight and can easily be carried around wherever the user wants. So it's a permanent mate that almost never leaves its owner day or night, and as we mentioned that using the cloud computing through a mobile phone device is called the mobile cloud computing.

New technologies bring new threats, therefore, using the technology of mobile cloud computing has added great additional challenges to this new technology, and the one of the most important threats that faces the mobile cloud computing is the issue of security. The authentication in the mobile cloud computing is almost the most critical issue as a result of all the intruders and the unauthorized individuals who try to use the cloud computing from mobile phone devices that don’t belong to them. Therefore, we must seriously think to design a new model that is good and effective to prevent the unauthorized access of unauthorized users.

المنارة للاستشارات
www.manaraa.com

In this thesis, we present a new efficient model for user authentication in mobile cloud computing, our model introduces method to provide a very effective method to protect the mobile cloud computing from various threats by intruders, that's where this method relies on the user's fingerprint to verify the user's identity. The proposed model attempts to use easy and strong method to protect mobile cloud computing users from different security threats.

In this chapter, the proposed model includes the following procedure:-

❖ **Authentication procedure**

This procedure is designed to provide authentication for protect the mobile cloud computing from any threat and it's important to determine the identity of the user and know whether authorized or not.

4.2 Execution of Authentication Procedure

The authentication procedure is designed to define the user is authorized or not, it is including two stages; Figure (4-1) shows the stages of authentication procedure:-

❖ New-user stage.

❖ Registered user stage.

المنارة للاستشارات
www.manaraa.com

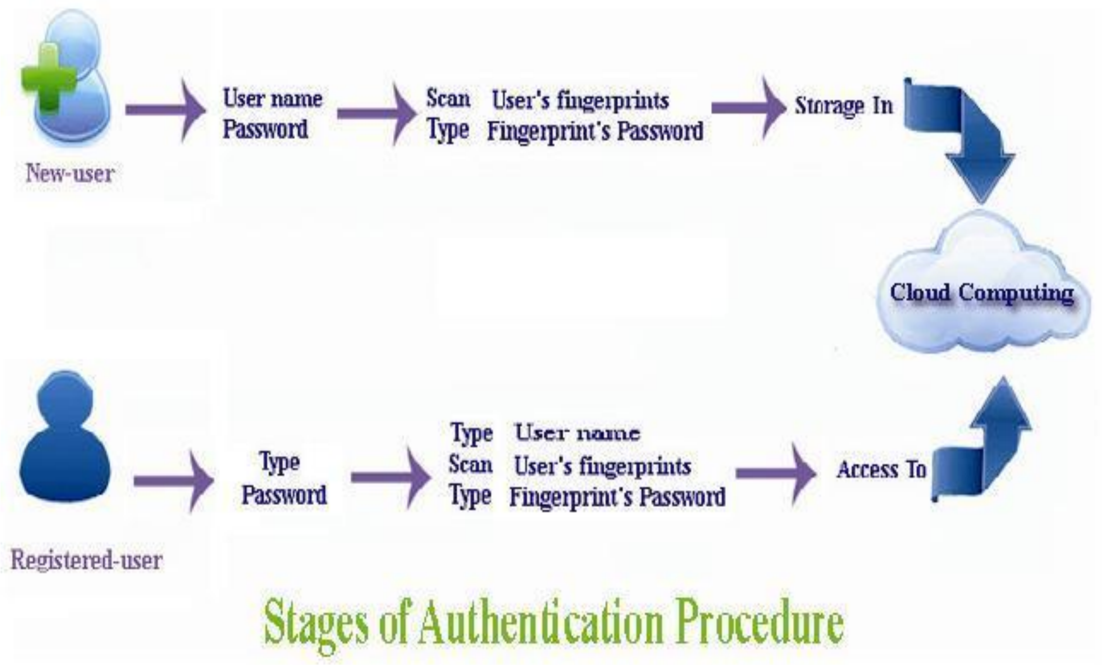


Figure (4-1): Authentication Procedure Stages.

4.2.1 Execution New-User Stage

The new users use this stage to create new account on mobile cloud computing application for the first time. The first interface shows to the user in the application as appear in the Figure (4-2).

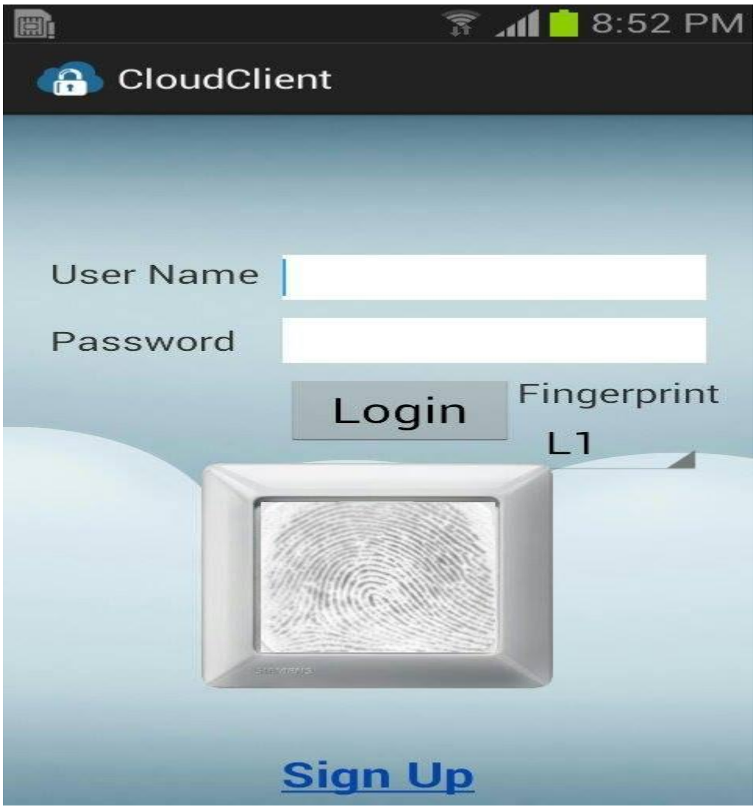
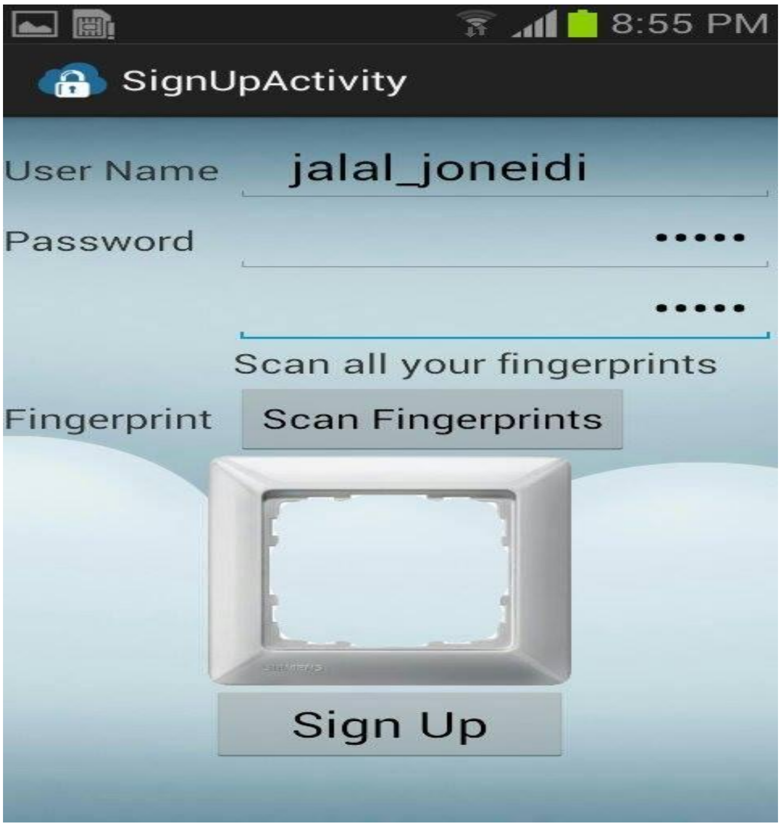


Figure (4-2): The Main Interface in Mobile Cloud Application.

The users must choose sign up button from the registration interface, if they don't have account on the mobile cloud application, then they will register all the required information and scan all fingerprints in both hands. The user must write fingerprint password for each fingerprint before scan it. Figure (4-3) shows the registration interface for new user.

المنارة للاستشارات
www.manaraa.com



User Name jalal_joneidi

Password •••••

•••••

Fingerprint

Figure (4-3): New User Registration Interface.

When the user completes the registration and scans all fingerprints in

both hands, the application will make sure the information is correct. Then the system set sign as a registered user in order to show different interface to registered user to provide greater security for authorized users. All information and fingerprints features will be stored in cloud server for the next process.

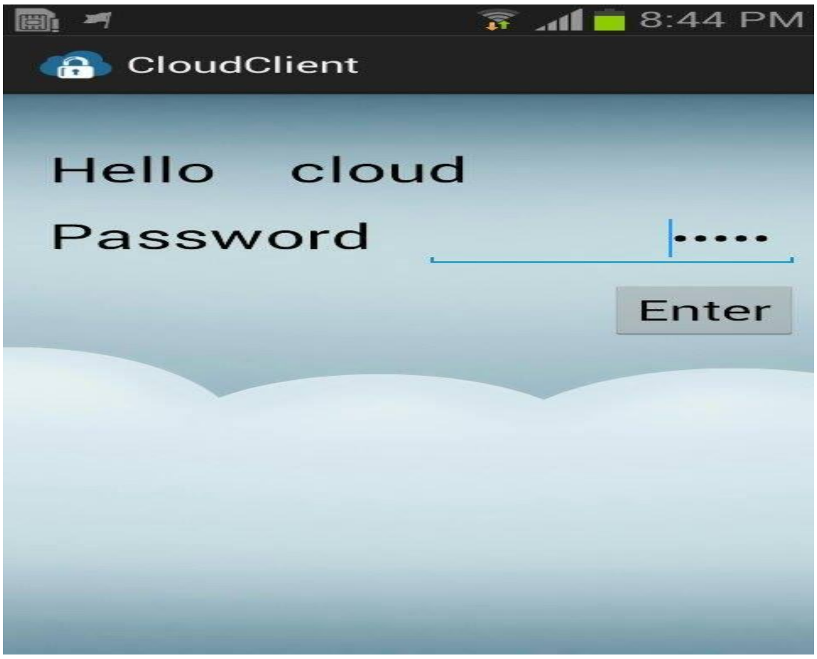
4.2.2 Execution Registered User Stage

The users of mobile cloud computing application after they register themselves on this application by fulfill all the information required and scan all fingerprints in both hand, the users considered as registered and when the user wants to access to the cloud computing will pass in three stages:

المنارة للاستشارات
www.manaraa.com

❖ **The first stage: when the users want to access the mobile cloud**

computing through the proposed model after register themselves must type their password so they could enter the main interface which enables access to cloud computing. The benefit of this interface is to provide greater security to authorized users; Figure (4-4) shows the protection interface.



Hello cloud

Password •••••

Figure (4-4): The Protection Interface.

The aim of this interface is to provide greater security for the users that are registered and have an account on the mobile cloud application. User must type the password after he/she will be able to enter to the login interface of the mobile cloud application because he/she is authorized to enter the login interface. Through the login interface of the mobile cloud application will enable the user to access to the cloud computing and take advantage of the services provided by the users because it is an authorized user. If the user is an intruder where he hasn't an account on mobile cloud application that this user certainly does not know the password and thus he will not be able to enter to the login interface of mobile cloud application, which enables him to access to the mobile cloud computing.

المنارة للاستشارات
www.manaraa.com

❖ **The second stage: After the user has entered the correct password**

in the protection interface, the login interface will appear to the user to complete the procedures for access to cloud computing; Figure (4-5) shows the login interface. The login interface contains on the username, password field and fingerprint acquisition, when the user want to access to the cloud computing must type the own username in the username field, password of the fingerprint that the user will use it on acquisition sensor to match it with the stored one in the cloud server, and to provide greater security, we removed the sign up button in order to prevent the intruder user if he got the password illegally take advantage of the mobile cloud application services, and thus he will be unable to register himself in the mobile cloud computing.

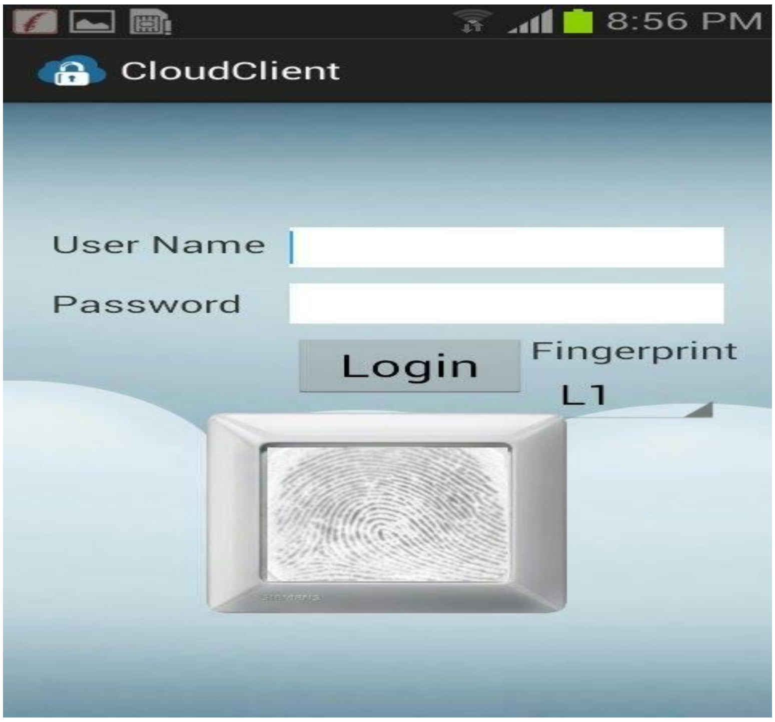
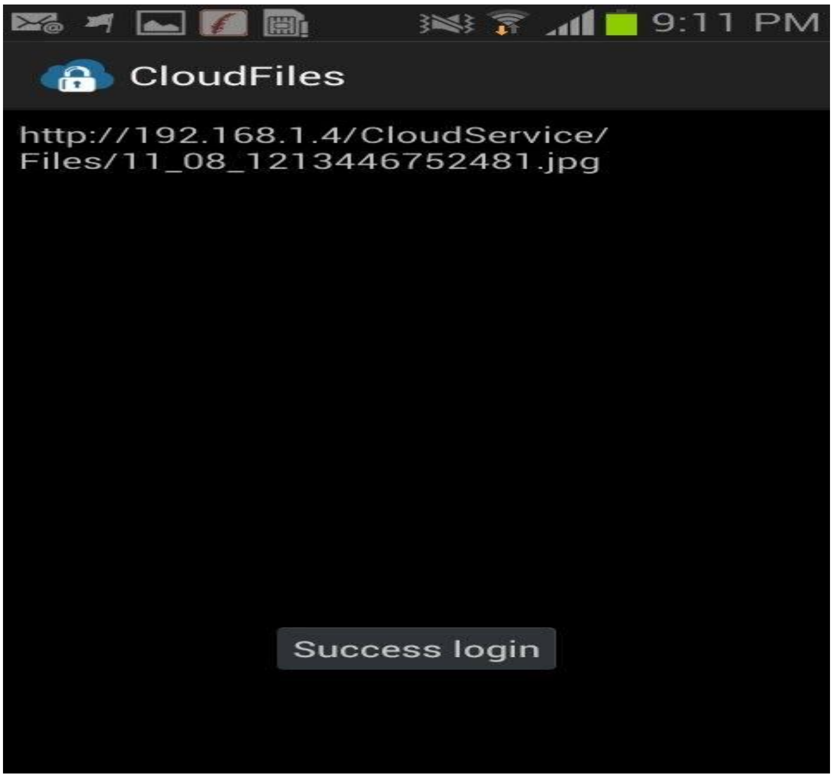


Figure (4-5): The Login Interface.

www.manaraa.com

❖ The third stage: If the user types the correct username and

password, he/she must scan one fingerprint by fingerprint acquisition sensor that is located on the mobile phone device, then if the matching happened between them that means the user is authorized, and he/she can access the cloud computing, then can get benefit from the services of the cloud computing; Figure (4-6) shows the interface success login.

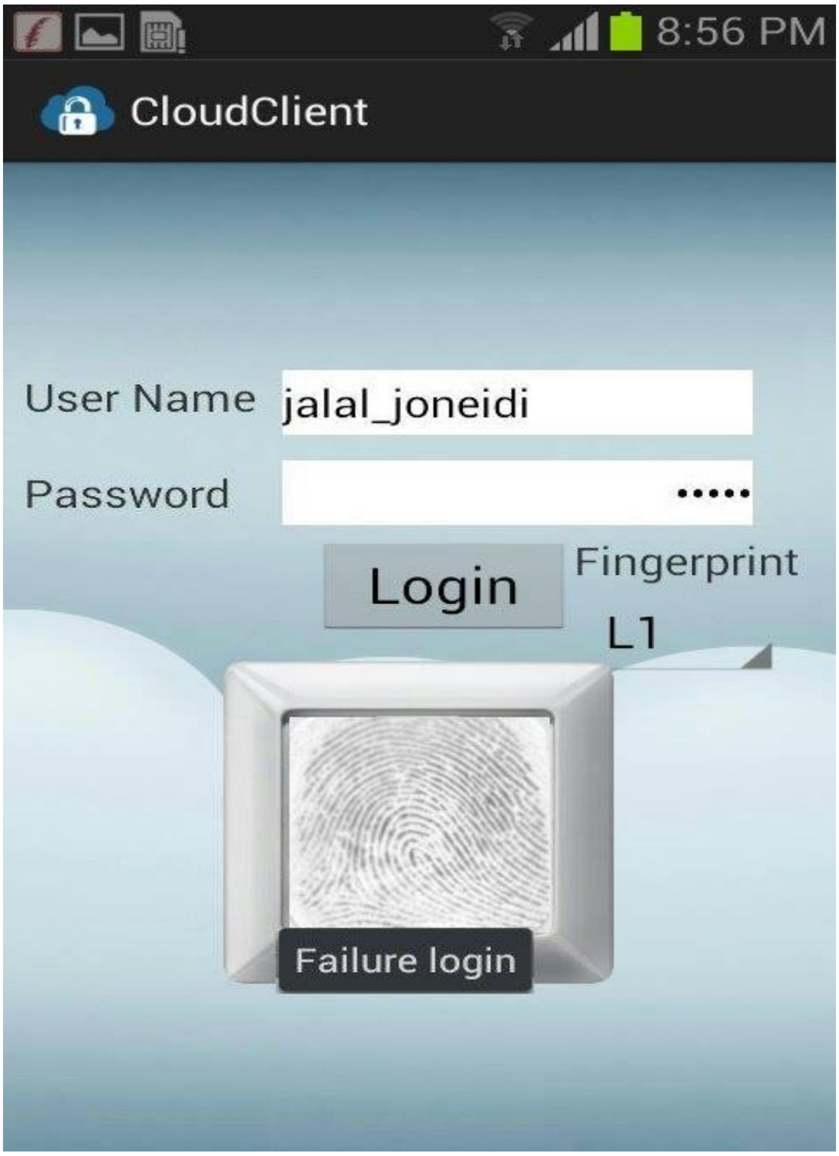


http://192.168.1.4/CloudService/Files/11_08_1213446752481.jpg

Figure (4-6): The Successful Login Interface.

But If the user is failed to enter the correct password or username or if did not get a matching between a fingerprint and readable fingerprint stored previously in cloud server, the mobile cloud application will reject access the user to cloud computing and will show a message telling the user that the process of access into the cloud computing failed. Figure (4-7) shows the interface of failure login.

المنارة للاستشارات
www.manaraa.com



User Name jalal_joneidi

Password •••••

Fingerprint L1

Failure login

Figure (4-7): The Failure Login Interface.

4.3 Experimental Works Results and Observations

We have done in this work several experiments to check the successful rate; Figure (4-8) shows the Successful Attempts Results. The experiment was to check each fingerprint for ten times. We have entered the passwords and the fingerprints for each finger to calculate the successful rate.

المنارة للاستشارات
www.manaraa.com

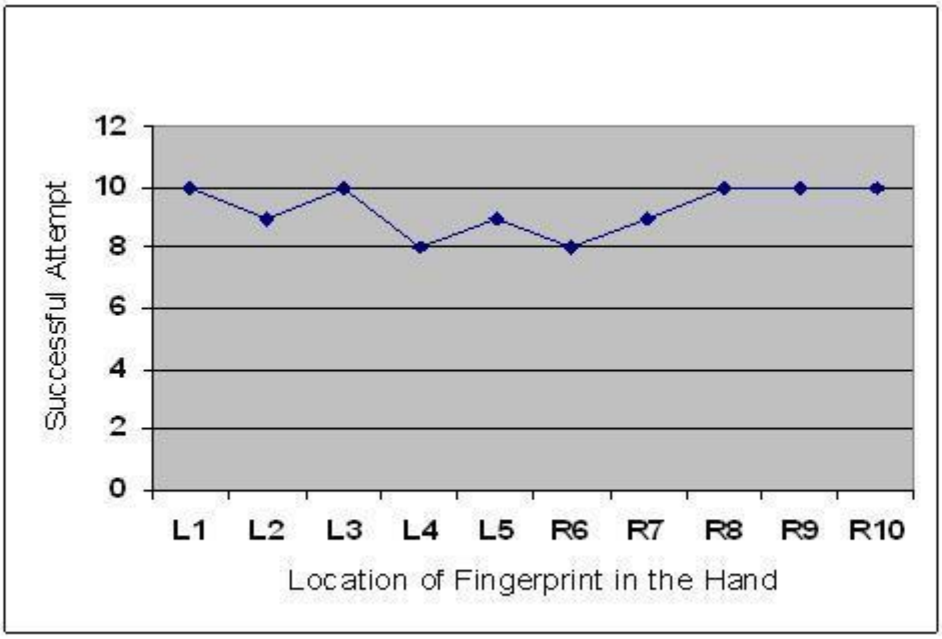


Figure (4-8): The Successful Attempts Results.

Some of the test has failure result due to the unclear pattern for the fingers for the following reasons:
1. Some fingerprints were suffering from the presence of wounds and burns.
2. Some fingerprints smudging paint, dyes, dirt. 3. Smearing fingerprint reader with dust and dirt.

المنارة للاستشارات
www.manaraa.com

Table (4-1) shows the rate of success and failure to read fingerprints, and as shown in the table the success to read fingerprints rate was very high compared to the failure rates.

Fail	Successful	Input
zero	10	left hand(first finger)
1	9	Second
zero	10	Third
2	8	Forth
1	9	Fifth
2	8	Right hand(first finger)
1	9	Second
zero	10	Third
zero	10	Forth
zero	10	Fifth

Table (4-1): Rates of Success and Failure to Read Fingerprints.

Total of successful process=93 Total of fail process=7
Rate of successful process=93%

4.4 Comparison with Previous Works

We have made a comparison between our system and some previous works which handle fingerprint recognition such as: Filter bank-based fingerprint matching [28], A hybrid fingerprint matcher [29] and embedded fingerprint matching on smart card [30]; Table (4-2) shows the results of a comparison with previous works. And as shown in the table below, our system works more efficiently than the Algorithms that are used in previous systems.

المنارة للاستشارات
www.manaraa.com

Matching Accuracy (%)		Algorithm
95.6		Filterbank-based Fingerprint Matching
96.3		A hybrid Fingerprint Matcher
95.51		Embedded Fingerprint Matching On Smart Card
97		Our System

Table (4-2): Comparison with Previous Works.

In this chapter we have provided a practical implementation of our proposed model and we have explained all the interfaces that will be presented to the user in the mobile cloud application that we have designed.

المنارة للاستشارات
www.manaraa.com

CHAPTER FIVE:CONCLUSION AND FUTURE WORKS

المنارة للاستشارات
www.manaraa.com

CHAPTER FIVE:Conclusion and Future Works

5.1 Introduction

Cloud computing is new paradigm shift and mobile cloud computing means using cloud computing thought mobile phone device. Mobile cloud computing provides many services for both organization and individuals encouraging them to migrate for using cloud computing, from these services store the files, using the software and the applications and the platforms…est. all these services the users can access it thorough the mobile phone device from any where and any time easily.

Because mobile cloud computing is hot topic, there are many researchers wrote in this area, these articles talked about mobile cloud computing concepts, benefits, services, deployment, characteristics of cloud computing, challenges are facing the mobile cloud computing and proposed solutions to address these issues.

The mobile phone device has become indispensable because of the many services it provides, since individuals are doing most of their daily work through their mobile phone devices, and because it is small in size, it is therefore easy to lose and easy to be stolen. Thus, it is necessary to use the identity authentication procedure to prevent intruders from accessing to the important files stored in the device or benefiting from the services provided by it.

The most important challenge facing mobile cloud computing is the problem of security, especially the problem of authentication. In mobile cloud computing it is important to detect whether the user is authorized or not. In this thesis, we designed new efficient model to provide authentication to mobile cloud computing.

In this chapter we have included conclusions and future works, illustrations the result of the implementation of the proposed solution to solve the authentication issue on mobile cloud computing, then the suggested future works related to this research project.

المنارة للاستشارات
www.manaraa.com

5.2 Conclusion

In this thesis we have explained the concepts of mobile cloud computing,and we have presented the benefits, services, deployment, properties and characteristics of cloud computing and security issue related to it. Furthermore, we have clarified the concepts of mobile phone device, phone service, benefits and mobile security of mobile phone device. On the other hand, we have explained the concept of authentication and the methods of authentication. Also, we have cleared the concepts of fingerprint authentications and Fingerprint image preprocessing.

And in this thesis we have designed a new efficient model for mobile cloud computing based on fingerprint, the implemented model works on storage all the user's fingerprints with their password on cloud server, when them want to access the cloud computing through mobile phone device they most scan any one of their fingerprints and its password. We find the following results in this thesis:-

1. Applicable security is excellent because using many passwords.

2. Flexibility in the use of any fingerprint to prove personal.

3. Intruders will not be able to take advantage of mobile cloud

computing service because of the use of several layers of security.

5.3 Future Works

Mobile cloud computing is considered a new technology, and as previously known, a new technology brings new threats and because perfect security does not exist, we suggest a group of ideas for future works on mobile cloud computing.

1. Use eye iris recognition to identify the authorized user, because this method is more rigid.

المنارة للاستشارات
www.manaraa.com

2. Improve the detection process for fingerprint through raising the ability to read the low resolution fingerprints.

3. Enhance the detection process through recognize the cuts, paints,or any obstacle for recognition.

4. Make the completion of the process of matching fingerprints inside Mobile phone device instead of cloud computing server.

المنارة للاستشارات

www.manaraa.com

References

[1]http://www.quaintise.com/in-2014-physician-marketing-will-be-all-about-mobile, Retrieved on 1/4/2014.

[2] http://www. ewikipedia.org, Retrieved on 5/4/2014.

[3] http://ttimobileinstitute.in, Retrieved on 6/4/2014.

[4]http://www.portaldomontadordemoveis.com.br/2014_04_01_archive.h tml, Retrieved on 9/4/2014.

[5] Rodriguez F, Jose R, Roth M, “The Mobile Technology Era: Potential Benefits and the Challenging Quest to Ensure Patient Privacy and Confidentiality”, PRS Jornal, May 2012.

[6] Stefan C, “The Future of Mobile Security “, CS Network Solutions Limited, June 2013.

[7] Ronnie D C and Sunguk L,” Security Considerations for Public Mobile Cloud Computing”, International Journal of Advanced Science and Technology Vol. 44, July 2012.

[8]http://www.readwriteweb.com/archives/why_cloud_computing_is_the _future_of_mobile.php, Retrieved on 12/4/2014.

[9] ABI Research. http://www.abiresearch.com, Retrieved on 15/4/2014.

[10] NIST (National Institute of Standards and Technology). http://csrc.nist.gov/groups/SNS/cloud-computing, Retrieved on 17/4/2014.

[11] http://www.atomrain.com/it/technology/cloud-deployment-models, Retrieved on 21/4/2014.

[12] http://www.gvsu.edu/e-hr/biometrics, Retrieved on 27/4/2014.

المنارة للاستشارات
www.manaraa.com

[13] Jain A K, Hong L, Pankanti S and Bolle R, "An Identity Authentication System Using Fingerprints", Proc. IEEE, vol. 85, no. 9, pp. 1365-1388, 1997.

[14] http://www.zhihu.com/question/22258379, Retrieved on 1/5/2014.

[15] Sachin D, Shrey S, Vishwa M and Khatana A, "Fingerprint, Retina and Facial Recognition Based Multimodal Systems", International Journal of Engineering and Computer Science ISSN: 2319-7242, May 2013.

[16] Amira S Supervised Dr. Abdel-Moneim. A, Dr. Ayman M, "Enhanced Secure Algorithm for Fingerprint Recognition", Ain Shams University Egypt, 2011.

[17] Michał S, Ireneusz J, " Biometric Security Systems for Mobile Devices based on Fingerprint Recognition Algorithm", The Second International Conference on Advanced Communications and Computation, 2012.

[18] Marius T, Pauli K, "Fingerprint Matching Using an Orientation-Based Minutia Descriptor, IEEE, August 2003.

[19] Weiwei J H Z, Zhenfu C, Lifei W and Xiaodong L, "SDSM: A secure data service mechanism in mobile cloud computing", Computer Communications Workshops (INFOCOM WKSHPS)IEEE, April 2011. Journal of Computer Science and Mobile Computing, volume 2, Issue 6, (2013).

[20] Akhil K, Hari O A, Kirtika G and Sakshi G, " Secure Authentication with Encryption Technique for Mobile on Cloud Computing", International Journal of Scientific Research Engineering & Technology (IJSRET), August 2012.

[21] Bhargava N, Bhargava R , Mathuria M, Daima R, "Performance Analysis of Cloud Computing for Distributed Client", International Journal of Computer Science and Mobile Computing, volume 2, Issue 6, (2013).

المنارة للاستشارات

[22] Soeung k and Sung W K, "Mobile Cloud Computing Security Considerations", journal of security engineering, April 2012.

[23] Nithiavathy R, Suresh J, "Verification of Data Reliability and Secure Service for Dynamic Data in Cloud Storage", International Journal of Advanced Computer Research, Volume 3, No. 1, Issue 8, (2013).

[24] Jaejung K and Seng-phil H, "A Consolidated Authentication Model in Cloud Computing Environments", International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 3, July201.

[25] Mrs. Yogita D M and Prof. Kailas K D, "Protection concern in Mobile Cloud Computing- A Survey", IOSR Journal of Computer Engineering (IOSR-JCE), 2009.

[26] Thamba M W and Suresh B K, "Secured and Efficient Authentication Scheme for Mobile Cloud", International Journal of Innovations in Engineering and Technology (IJIET), February, 2013.

[27] Swati P R, Priya S K, Golait S S, "Privacy Preserving & Access Control to Intrusion Detection in Cloud System", International Journal of Innovative Research in Computer and Communication Engineering, Volume1, Issue 1, (2013).

[28] Jain A K, Prabhakar S, Hong L, and Pankanti S, "Filterbank-based Fingerprint Matching", IEEE, vol. 9, no. 5, pp.846–859, May 2000.

[29] Ross A, Jain A, and Reisman J, "A hybrid Fingerprint Matcher", Pattern Recognition., vol. 36, No. 7, pp. 1661–1673, November 2003.

[30] Farid B H and Kadda B B," Embedded Fingerprint Matching on Smart Card", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 27, No. 2, April 2013.

المنارة للاستشارات

www.manaraa.com