Sudan University of Science & Technology

College of Graduate of Studies

CLOUD SECURITY

(ENCRYPTION AND AUTHENTICATION MECHANISM FOR CLOUD COMPUTING SECURITY)

أمن الحوسبة السحابية

آلية التشفير و التحقق لتأمين الحوسبة السحابية

A thesis submitted In Partial Fulfillment of The Requirements

For the Degree of Master in Computer Science

BY:

MOHAMMED YOUSIF ELKHIDER IDRES

Supervisor:

Dr. Faisal Mohammed Abdalla Ali

November 2014

بسم الله الرحمن الرحيم

Sudan University of Science & Technology

College of Graduate of Studies

CLOUD SECURITY

(ENCRYPTION AND AUTHENTICATION MECHANISM FOR CLOUD COMPUTING SECURITY)

أمن الحوسبة السحابية

آلية التشفير و التحقق لتأمين الحوسبة السحابية

A thesis submitted In Partial Fulfillment of The Requirements

For the Degree of Master in Computer Science

Prepared by: MOHAMMED YOUSIF ELKHIDER

Supervisor: Dr. Faisal Mohammed Abdalla Ali

November 2014

الآية

بسم الله الرحمن الرحيم

﴿ اقْرَأْ بِاسْمِ رَبّكَ الَّذِي خَلَقَ (1) خَلَقَ الإِنْسَانَ مِنْ عَلَقٍ) 2 (اقْرَأْ
وَرَبُّكَ الأَكْرَمُ (3) الَّذِي عَلَّمَ بِالْقَلَمِ (4) عَلَّمَ الإِنْسَانَ مَا لَمْ يَعْلَمْ ﴾

العلق(1-5)

صدق الله العظيم

Acknowledgement

I would never have been able to finish my dissertation without the guidance of my committee members, help from friends, and support from my family and wife. I would like to express my deepest gratitude to my advisor, **Dr. Faisal Mohammed Abdalla Ali**, for his excellent guidance, caring, patience, and providing me with an excellent atmosphere for doing research, his guidance helped me in all the time of research and writing of this thesis.

ABSTRACT

Cloud computing has emerged as a promising technique that greatly changes the modern Information Technology industry, it depends on sharing resources that were never shared before, demanding a new set of security challenges. There are a variety of information security risks that need to be carefully considered, Risks will vary depending on the sensitivity of the data to be stored or processed.

In this research a proposed method to solve some problems of cloud computing security was introduced form both perspectives client and provider by using encryption technique and EAP-CHAP.

The proposed method was implemented using encryption and authentication technique build inside EAP-CHAP protocol. The implementation using Visual Basic.Net and SQL Server, to simulate the registration and accessing methods.

The proposal is subjected to analysis and optimum result in term of security are obtained.

المستخلص

برزت الحوسبة السحابية في السنوات القليله الماضية بإعتبارها تقنية واعدة وقد ساهمت في تغيير صناعة تكنولوجيا المعلومات الحديثة بصورة واسعة، فهي تعتمد على تشارك الموارد التي لم يتم مشاركتها من قبل، مما فرض مجموعة جديدة من التحديات الأمنية. وهناك مجموعات متنوعة من المخاطر الأمنية المتعلقة بالمعلومات و التي تحتاج إلى النظر فيها بعناية، وتلك المخاطر تختلف تبعاً لحساسية البيانات المراد تخزينها أو معالجتها.

يهدف هذا البحث إلي إيجاد حلول لمعظم تلك المهددات الأمنية والتي تمثل هاجساً وتخوفاً حقيقياً لكل مؤسسه تولدت لديها الرغبة في الإنتقال من النظم التقليدية إلي حلول الحوسبة السحابية, ويتلخص الحل المقدم في هذا البحث علي تأمين البيانات في حالتيها (الإستقرار و الإنتقال) وذلك عن طريق إستخدام تقنيات التشفير, وكذلك علي تأمين الإتصال بين كل من المستخدم(الزبون) ومقدم الخدمة(المزود).

تم تنفيذ الحل المقترح بإستخدام تقنيتي التشفير, والتحقق. حيث تم تصميم تطبيق لمحاكاة عمليتي التسجيل والدخول وتطبيق آخرللقيام بعملية تشفير الملفات قبل إرسالها الي السحابة وذلك بإستخدام لغة ال Visual Basic.Net وال SQL Server.

وفي جانب التحقق تم إستخدام بروتوكول ال EAP-CHAP.

Table of Contents

List of Figures

List of Tables

CHAPTER (1)

INTRODUCTION

Cloud computing has transformed the way organizations approach of Information Technology (**IT**), enabling them to become more agile, introduce new business models, provide more services, and reduce IT costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches.

The cloud computing landscape continues to realize explosive growth. The worldwide public cloud services market was projected to grow nearly 20 percent in 2012, to a total of $109 billion, with 45.6 percent growth for Infrastructure as a Service (IaaS), which is the fastest growing market segment.

Yet for security professionals, the cloud presents a huge dilemma: How to embrace the benefits of the cloud while maintaining security controls over an organizations' assets?

It becomes a question of balance to determine whether the increased risks are truly worth the agility and economic benefits.

Maintaining control over the data is paramount to cloud success. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where one could segregate sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity.

1.1 Cloud Computing Security Challenges

Cloud computing opens up a new world of opportunities for businesses, but mixed in with these opportunities are numerous security challenges that need to be considered and addressed prior to committing to a cloud computing strategy. [1]

Cloud computing security challenges fall into three broad categories:

- **Data Protection**: Securing your data both at rest and in transit.
- **User Authentication**: Limiting access to data and monitoring who accesses the data.
- **Disaster and Data Breach**: Contingency Planning.

Data protection tops the list of cloud concerns today. Vendor security capabilities are key to establishing strategic value.

1.1.1 Data Protection

Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encryption keys. [2]

1.1.2 User Authentication

Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. These access logs and audit trails additionally need to be secured and maintained for as long as the company needs or legal purposes require. As with all cloud computing security challenges, it's the responsibility of the customer to ensure that the cloud provider has taken all necessary security measures to protect the customer's data and the access to that data. [3]

1.1.3 Disaster and Data Breach

With the cloud serving as a single centralized repository for a company's mission-critical data, the risks of having that data compromised due to a data breach or temporarily made unavailable due to a natural disaster are real concerns. Much of the liability for the disruption of data in a cloud ultimately rests with the company whose mission-critical operations depend on that data, although liability can and should be negotiated in a contract with the services provider prior to commitment. A comprehensive security assessment from a neutral third-party is strongly recommended as well.

Companies need to know how their data is being secured and what measures the service provider will be taking to ensure the integrity and availability of that data should the unexpected occur. Additionally, companies should also have contingency plans in place in the event their cloud provider fails or goes bankrupt. Can the data be easily retrieved and migrated to a new service provider or to a non-cloud strategy if this happens? And what happens to the data and the ability to access that data if the provider gets acquired by another company? [4]

1.2 Problem Statement

Users who put their large data files in the cloud storage servers can relieve the burden of storage and computation. At the same time, it is critically important for users to ensure that their data are being stored correctly and safely. So, users should be equipped with certain security means so that they can make sure that their data is safe. The major concern is the security of data at rest and while moving. So to handle this problem it is required that data at both user side and server side must be in encrypted form.

1.3 Objectives

Though IT services from the cloud are becoming increasingly in demand around the world, almost every survey and study shows that there are also many concerns which discourage users away from using Cloud Computing services. A lack of faith in the security of the services provided is frequently cited as being one of the main barriers.

This thesis ensure that the customer's data stored safely in the cloud by:

- Identify and authenticate users before granting access.
- Encrypt sensitive or confidential information,
- Encrypt user's files before sending it to the cloud.

1.4 Method

The two different approaches used for ensuring security in cloud are as follows:

1.4.1 From cloud provider side:

a- **Using the Extensible Authentication Protocol-CHAP.**

An authentication protocol is a type of cryptographic protocol with the purpose of authenticating entities wishing to communicate securely. Extensible Authentication Protocol (**EAP**) will implement on Cloud environment for authentication purpose. It is used for the transport and usage of keying material and parameters generated by EAP methods. In this purposed model the Challenge-Handshake Authentication Protocol (CHAP) was used for authentication.

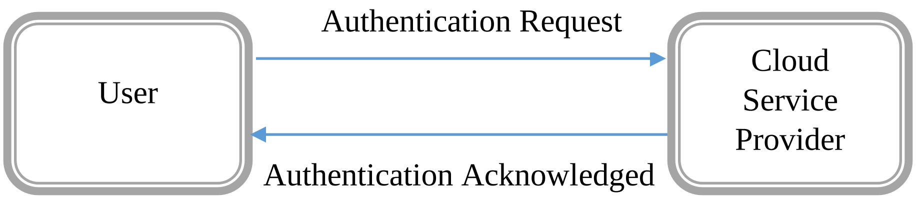


Figure (1.1): CHAP General Process

b- **Keeping user's data in an encrypted form.**

By using **SHA-1** encryption algorithm to encrypt user's credentials before storing it into database.

1.4.2 From cloud user side:

To ensure the data confidentiality and it not exposed by outsiders in the event of a security problem on the provider side, the encryption software designed to encrypt data before it is sent to the cloud.

The User data (files) is encrypted by using Advanced Encryption Standard (AES) encryption algorithm.

The (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption. In December 2001, the National Institute of Standards (NIST) approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies application of the Rijndael algorithm to all sensitive classified data. [5]

1.5 Motivation

With Cloud Computing, as with many new technologies and services, information security and data protection issues are intensely debated, and examined far more critically than is the case with offerings that have been around for a while. Many surveys and studies reveal that potential customers have concerns about information security and data protection which stand in the way of a wider deployment. The required trust still needs to be developed if cloud offerings are to be taken advantage of. [6]

1.6 Thesis structure

This thesis is composed of fives chapters as follows:

Chapter 1: Introduction this chapter contains an overview of cloud computing and cloud computing security challenges, and thesis statement as well as the motivation and objectives of thesis.

Chapter 2: Background and Related Work This chapter explains what cloud computing is, what components comprise a cloud solution, and the different applications you can expect, as well as the cloud reference model and cloud security reference model beside advantages and disadvantage of cloud computing, and takes a closer look at the security concerns and issues with explaining the top threats of cloud computing in the year 2013.

Chapter 3: Proposed Methodology this chapter explains the designed encryption system and how it work to maintain the user's data securely.

Chapter 4: Results and Analysis this chapter contains the results gained when using the proposed system as wel as some security analysis.

Chapter 5: Conclusion and Future Work this chapter contains the thesis conclusion and the future work that should be done in the cloud computing discipline.

References

CHAPTER (2)

BACKGROUND AND RELATED WORK

2.1 Background

2.1.1 Preface

Cloud computing is a relatively novel topic in Information Technology that attracts significant attention from the public and private sectors nowadays [7], and emerged as a new paradigm for on-demand delivery of computing resources to consumers as utilities. It offers unlimited computing resources to its users in **a pay-as-you-go** model with a higher level of quality of service such as availability and reliability in a substantially reduced infrastructure cost. With such an offering, it is not surprising that businesses are considering moving their IT infrastructure to cloud. [8].

Businesses have serious concerns on moving their services and data to a cloud environment. These concerns need to be addressed to realize the vision of delivering IT services as utilities.

The vision of delivering unlimited computing resources, e.g., *compute, network, and storage*, as utilities, as promised by the cloud computing paradigm, has made some of the tasks—that were impossible to achieve a few years back for small and medium size businesses-possible.

Businesses can run sophisticated data analytics tools without investing a big amount on IT infrastructure.

2.1.2 Definition

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., *networks*, *servers*, *storage*, *applications*, and *services*) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [9]

2.1.3 Cloud computing basics

2.1.3.1 The comprises Cloud Computing

The National Institute of Standards and Technology (NIST) defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are summarized in visual form in Figure (2.1) and explained in detail below.

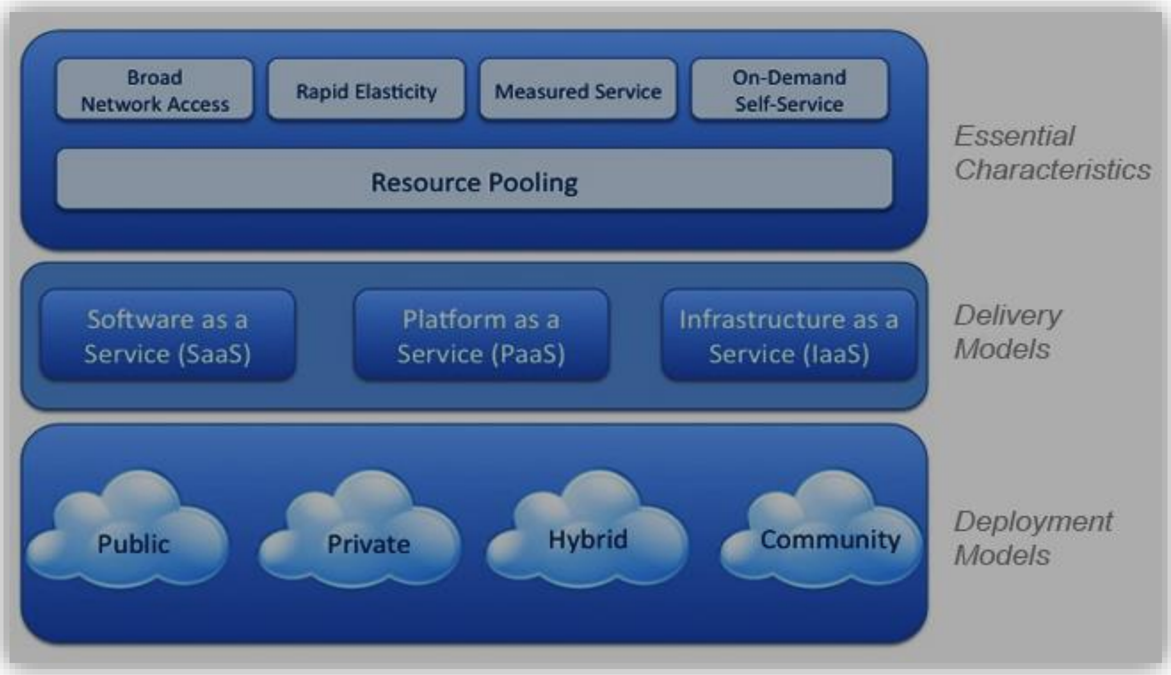


Figure (2.1): NIST Visual Model of Cloud Computing Definition.

2.1.3.2 Cloud Service Models

Based on the delivery type, researchers typically distinguish between the following service models:

Software as a Service (SaaS). Customer can use provider's applications which are running on a cloud infrastructure. Access to an application can be done from various client devices (*PCs, mobile phones, PDAs, etc*.) Examples: *Google Docs, Microsoft Office Live, Salesforce Customer Relationship Management*.

Platform as a Service (PaaS). Customer can use provider's development environment to create applications and deploy them on provider's cloud infrastructure. Examples: *Google App Engine*, *Microsoft Azure*, *Salesforce Force.com*.

Infrastructure as a Service (IaaS). Customer can use provider's computing resources (*processing, storage, networks, etc*.) to deploy and run arbitrary software which can include operating systems and applications. Examples: *Amazon Simple Storage Service (S3), RackSpace Cloud Servers*.

2.1.3.3 Cloud Deployment Models

Regardless of the service model utilized (SaaS, PaaS, or IaaS), there are four deployment models for cloud services with derivative variations that address specific requirements.

It is important to note that there are derivative cloud deployment models emerging due to the maturation of market offerings and customer demand. An example of such is *virtual private clouds* — a way of utilizing public cloud infrastructure in a private or semi-private manner and interconnecting these resources to the internal resources of a consumer's datacenter, usually via virtual private network (VPN) connectivity.

2.1.3.4 Deployment models

- **Public Cloud**. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Private Cloud**. The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or by a third party and may be located on-premise or off-premise.
- **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, or compliance considerations*). It may be managed by the organizations or by a third party and may be located on-premise or off-premise.
- **Hybrid Cloud**. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., *cloud bursting for load-balancing between clouds*).

Depending on the utilized cloud deployment model, organizations have different level of control over the infrastructure and computing resources (private cloud deployment gives greater control than public one) and thus different level of responsibility for applied security measures.

2.1.4 The Characteristics of Cloud Computing

It is important to recognize that cloud services are often but not always utilized in conjunction with, and enabled by, virtualization technologies. There is no requirement, however, that ties the abstraction of resources to virtualization technologies, and in many offerings virtualization by hypervisor or operating system container is not utilized.

Further, it should be noted that multi-tenancy is not called out as an essential cloud characteristic by the **NIST** but is often discussed as such. Although not an essential characteristic of cloud computing in the **NIST** model, Cloud Security Alliance (**CSA**) has identified multi-tenancy as an important element of cloud.

2.1.5 Multi-Tenancy

The multi tenancy is considered an important element, and the following section will outline the **CSA's** understanding/definition as an important element of cloud computing.

Multi-tenancy in its simplest form implies use of same resources or application by multiple consumers that may belong to same organization or different organization. The impact of multi-tenancy is visibility of residual data or trace of operations by other user or tenant.

Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies.

Consumers may choose to utilize a public cloud providers' service offering on an individual user basis or, in the instance of private cloud hosting, an organization may segment users as different business units sharing a common infrastructure.

From a provider's perspective, multi-tenancy suggests an architectural and design approach to enable economies of scale, availability, management, segmentation, isolation, and operational efficiency. These services leverage shared infrastructure, data, metadata, services, and applications across many different consumers.

Multi-tenancy can also take on different definitions depending upon the cloud service model of the provider; inasmuch as it may entail enabling the capabilities described above at the infrastructure, database, or application levels. An example would be the difference between an **IaaS**, **SaaS**, and **PaaS** multi-tenant implementation.

Cloud deployment models place different importance on multi-tenancy. However, even in the case of a private cloud, a single organization may have a multitude of third party consultants and contractors, as well as a desire for a high degree of logical separation between business units. Thus, multi-tenancy concerns should always be considered. [10]

2.1.6 Advantages and Disadvantages of Cloud Computing – Cloud computing pros and cons

2.1.6.1 Advantages of Cloud Computing

Cloud computing offers numerous advantages both to end users and businesses of all sizes. The obvious huge advantage is that you no more have to support the infrastructure or have the knowledge necessary to develop and maintain the infrastructure, development environment or application, as were things up until recently. The burden has been lifted and someone else is taking care of all that. Business are now able to focus on their core business by outsourcing all the hassle of IT infrastructure. Let's visit some of the most important advantages of cloud computing. Those will include both a company's and an end-user's perspective [11].

- **Cost Efficiency**

  This is the biggest advantage of cloud computing, achieved by the elimination of the investment in stand-alone software or servers. By leveraging cloud's capabilities, companies can save on licensing fees and at the same time eliminate overhead charges such as the cost of data storage, software updates, management etc.

  The cloud is in general available at much cheaper rates than traditional approaches and can significantly lower the overall IT expenses. At the same time, convenient and scalable charging models have emerged (such as one-time-payment and pay-as-you-go), making the cloud even more attractive.

  If you want to get more technical and analytical, cloud computing delivers a better cash flow by eliminating the capital expense (CAPEX) associated with developing and maintaining the server infrastructure.

  - Convenience and continuous availability
  - Backup and Recovery
  - Cloud is environmentally friendly
  - Resiliency and Redundancy
  - Scalability and Performance
  - Quick deployment and ease of integration

- Increased Storage Capacity
- Device Diversity and Location Independence
- Smaller learning curve

2.1.6.2 Disadvantages of Cloud Computing

- Security and privacy in the Cloud
- Dependency and vendor lock-in
- Technical Difficulties and Downtime
- Limited control and flexibility
- Increased Vulnerability

2.1.7 Cloud Computing Security

Cloud computing Security brings with it all of the traditional computer security threats as well as a host of new ones. The cloud is making security experts' jobs harder than ever before, forcing them to step up with innovative responses.

2.1.8 Cloud Reference Model

"*Understanding the relationships and dependencies between cloud computing models is critical to understanding cloud computing security risks.* ***IaaS*** *is the foundation of all cloud services, with* ***PaaS*** *building upon* ***IaaS****, and* ***SaaS*** *in turn building upon* ***PaaS*** *as described in the Cloud Reference Model diagram. In this way, just as capabilities are inherited, so are information security issues and risk. It is important to note that commercial cloud providers may not neatly fit into the layered service models. Nevertheless, the reference model is important for relating real-*

world services to an architectural framework and understanding that the resources and services require security analysis.

***IaaS** includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the capability to abstract resources (or not), as well as deliver physical and logical connectivity to those resources. Ultimately, **IaaS** provides a set of Application Programming Interface (**API's)**, which allows management and other forms of interaction with the infrastructure by consumers.*

***PaaS** sits on top of **IaaS** and adds an additional layer of integration with application development frameworks, middleware capabilities, and functions such as database, messaging, and queuing. These services allow developers to build applications on the platform with programming languages and tools that are supported by the stack.*

***SaaS** in turn is built upon the underlying **IaaS** and **PaaS** stacks and provides a self-contained operating environment that is used to deliver the entire user experience, including the content, its presentation, the application(s), and management capabilities.*

*It should therefore be clear that there are significant trade-offs to each model in terms of integrated features, complexity versus openness (extensibility), and security. Generally, **SaaS** provides the most integrated functionality built directly into the offering, with the least consumer extensibility, and a relatively high level of integrated security (at least the provider bears a responsibility for security).*

***PaaS** is intended to enable developers to build their own applications on top of the platform. As a result, it tends to be more extensible than **SaaS**, at the expense of customer-ready features. This tradeoff extends to security* *features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security.*

***IaaS** provides few if any application-like features, but enormous extensibility. This generally means less integrated security capabilities and functionality beyond protecting the infrastructure itself. This model requires that operating systems, applications, and content be managed and secured by the cloud consumer.*

The key takeaway for security architecture is that the lower down the stack the cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves.

*Service levels, security, governance, compliance, and liability expectations of the service and provider are contractually stipulated, managed to, and enforced, when a service level agreement (**SLA's)**, is offered to the consumer. There are two types of **SLA's**, negotiable and non-negotiable. In the absence of an **SLA**, the consumer administers all aspects of the cloud under its control. When a non-negotiable **SLA** is offered, the provider administers those portions stipulated in the agreement. In the case of **PaaS** or **IaaS**, it is usually the responsibility of the consumer's system administrators to effectively manage the residual services specified in the **SLA**, with some offset expected by the provider for securing the underlying platform and infrastructure components to ensure basic service availability and security. It should be clear in all cases that one can assign/transfer responsibility but not necessarily accountability.*

Narrowing the scope or specific capabilities and functionality within each of the cloud delivery models, or employing the functional coupling of services and capabilities across them, may yield derivative classifications.

For example "Storage as a Service" is a specific sub-offering within the ***IaaS*** *'family'.*

2.1.8.1 Cloud Security Reference Model

The cloud security reference model addresses the relationships of these classes and places them in context with their relevant security controls and concerns. For organizations and individuals grappling with cloud computing for the first time, it is important to note the following to avoid potential pitfalls and confusion:

- *The notion of how cloud services are deployed is often used interchangeably with where they are provided, which can lead to confusion. Public or private clouds may be described as external or internal, which may not be accurate in all situations.*
- *The manner in which cloud services are consumed is often described relative to the location of an organization's management or security perimeter (usually defined by the presence of a known demarc). While it is still important to understand where security boundaries lie in terms of cloud computing, the notion of a well-demarcated perimeter is an anachronistic concept for most organizations.*
- *The re-perimeterization and the erosion of trust boundaries already happening in the enterprise is amplified and accelerated by cloud computing. Ubiquitous connectivity, the amorphous nature of information interchange, and the ineffectiveness of traditional static security controls which cannot deal with the dynamic nature of cloud services, all require new thinking with regard to cloud computing. The Jericho Forum8 has produced a considerable amount of material on*

the re- perimeterization of enterprise networks, including many case studies.

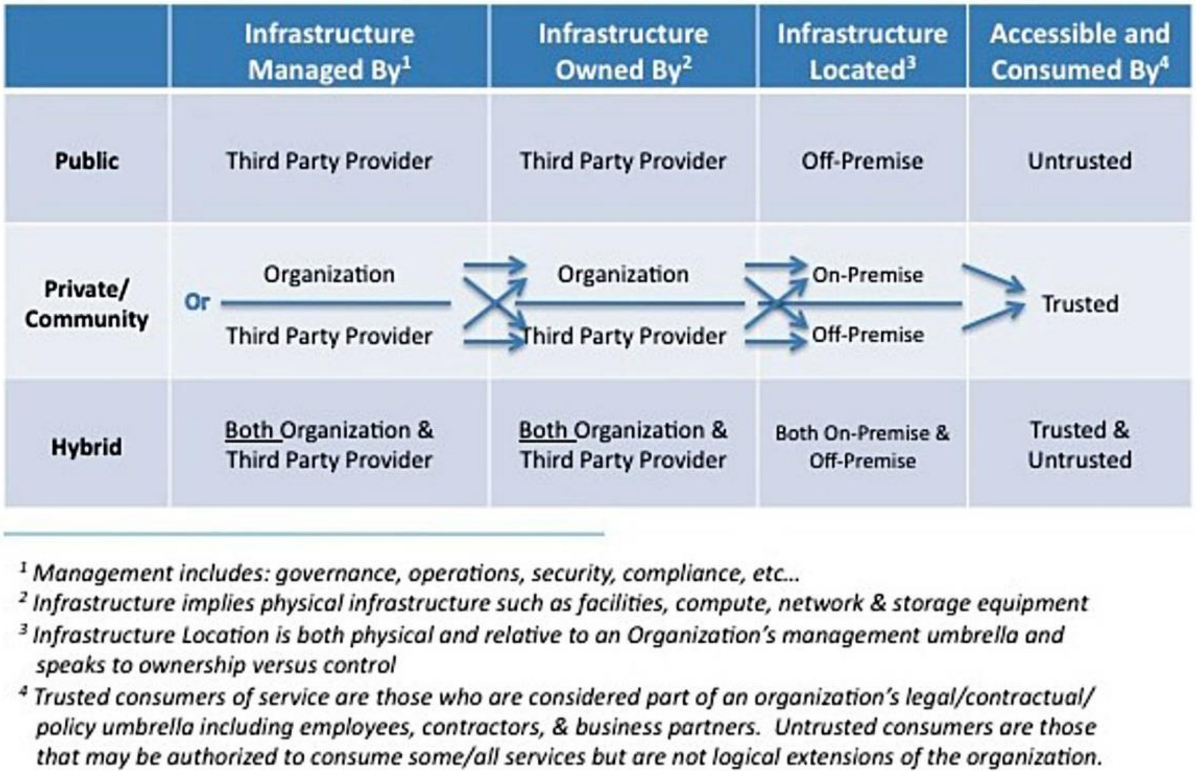
The deployment and consumption modalities of cloud should be thought of not only within the context of 'internal' versus 'external' as they relate to the physical location of assets, resources, and information; but also by whom they are being consumed; and who is responsible for their governance, security, and compliance with policies and standards.

This is not to suggest that the on- or off-premise location of an asset, a resource, or information does not affect the security and risk posture of an organization because they do - but to underscore that risk also depends upon:

- *The types of assets, resources, and information being managed*
- *Who manages them and how*
- *Which controls are selected and how they are integrated*
- *Compliance issues*

Corporation's control, management, and ownership, could be described as a private, on-premise, self-managed ***SaaS*** *solution. Both examples utilize the elastic scaling and self-service capabilities of cloud. "*[12].

The following table summarizes these points:



	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization Or Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] Management includes: governance, operations, security, compliance, etc...

[2] Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

[3] Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control

[4] Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Table (2.1): Cloud Security Reference Model

2.1.8.2 Security for Cloud Computing

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

An organization's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (*physical security*), to the network infrastructure (*network* *security*), to the IT systems (*system security*), all the way to the information, and applications (*application security*). Additionally, controls are implemented at the people and process levels, such as separation of duties and change management, respectively.

The security responsibilities of both the provider and the consumer greatly differ between cloud service models. *Amazon's AWS EC2* infrastructure as a service offering, as an example, includes vendor responsibility for security up to the hypervisor, meaning they can only address security controls such as *physical security*, *environmental security*, and *virtualization security*. The consumer, in turn, is responsible for security controls that relate to the **IT** system (instance) including the *operating system, applications,* and *data.*

The inverse is true for Salesforce.com's customer resource management (**CRM**) **SaaS** offering. Because Salesforce.com provides the entire "stack," the provider is not only responsible for the *physical* and *environmental security controls,* but it must also address the *security controls on the infrastructure, the applications,* and *the data*. This alleviates much of the consumer's direct operational responsibility.

There is currently no way for a naive consumer of cloud services to simply understand what exactly he/she is responsible for.

One of the attractions of cloud computing is the *cost efficiencies* afforded by economies of scale, *reuse*, and *standardization*. To bring these efficiencies to bear, cloud providers have to provide services that are flexible enough to serve the largest customer base possible, maximizing their addressable market. Unfortunately, integrating security into these solutions is often perceived as making them more rigid.

This rigidity often manifests in the inability to gain parity in security control deployment in cloud environments compared to traditional IT. This stems mostly from the abstraction of infrastructure, and the lack of visibility and capability to integrate many familiar security controls, especially at the network layer.

The figure below illustrates these issues:

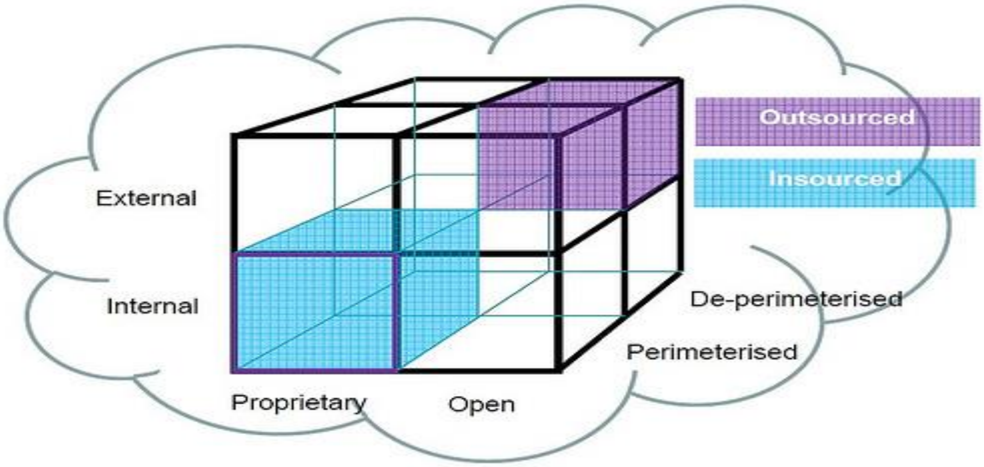


Figure (2.2): Security for Cloud Computing

In **SaaS** environments the security controls and their scope are negotiated into the contracts for service; service levels, privacy, and compliance are all issues to be dealt with legally in contracts.

In an IaaS offering, while the responsibility for securing the underlying infrastructure and abstraction layers belongs to the provider, the remainder of the stack is the consumer’s responsibility.

PaaS offers a balance somewhere in between, where securing the platform falls onto the provider, but both securing the applications developed against the platform and developing them securely, belong to the consumer.

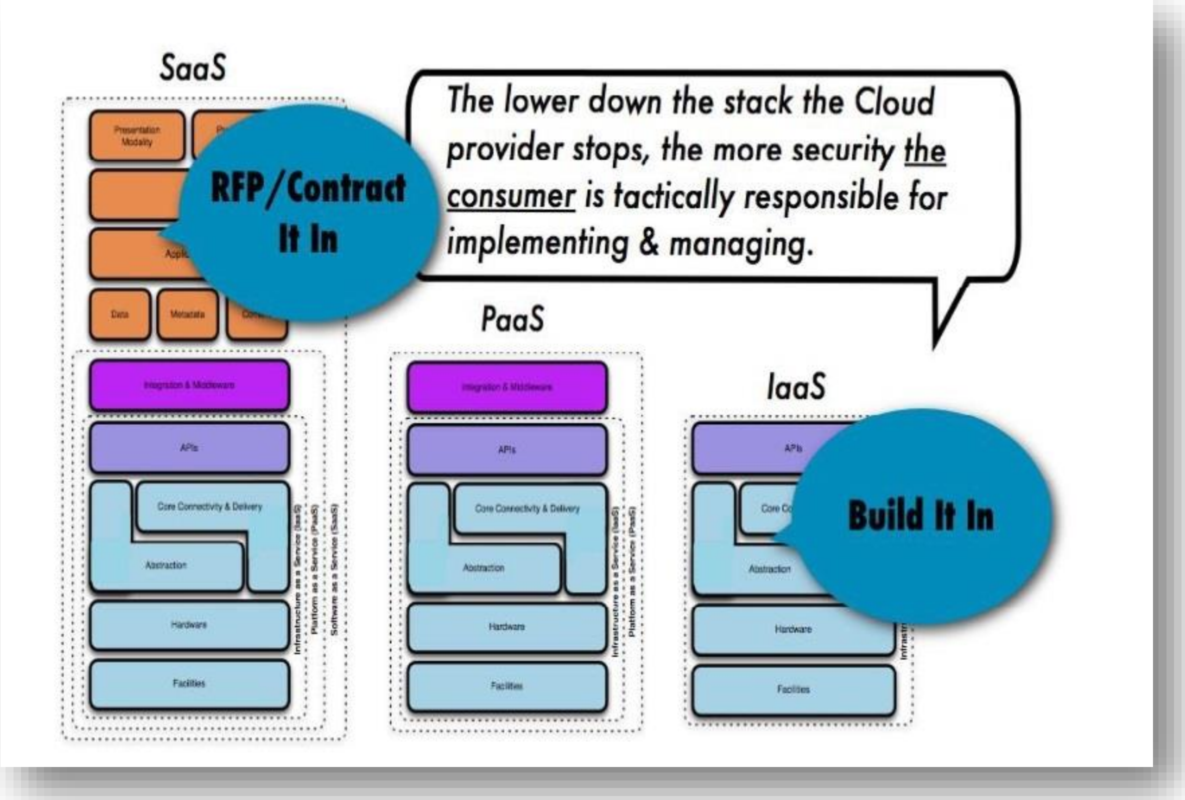

SaaS
Presentation Modality
Appl
Data
Metadata
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
RFP/Contract It In
The lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.
PaaS
IaaS
Build It In

Figure (2.3): Differences between SaaS, PaaS, and IaaS Service Models.

Understanding the impact of these differences between service models and how they are deployed is critical to managing the risk posture of an organization.

2.1.9 The Cloud Computing Top Threats

At an unprecedented pace, cloud computing has simultaneously transformed business and government, and created new security challenges. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Yet these advances have created new security vulnerabilities, including security issues whose full impact is still emerging. [13]

To identify the top threats, CSA conducted a survey of industry experts to compile professional opinion on the greatest vulnerabilities within cloud computing. The Top Threats working group used these survey results alongside their expertise to craft the final 2013 report. The survey methodology validated that the threat listing reflects the most current concerns of the industry. In this most recent edition of this report, experts identified the following nine critical threats to cloud security (ranked in order of severity):

- Data Breaches
- Data Loss
- Account Hijacking
- Insecure APIs
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Issues

4.1.9.1 Data Breaches

It’s every CIO’s (Chief Information Officer) worst nightmare: the organization’s sensitive internal data falls into the hands of their competitors. While this scenario has kept executives awake at night long before the advent of computing, cloud computing introduces significant new avenues of attack. In November 2012, researchers from the University of North Carolina, the University of Wisconsin and RSA Corporation released a paper describing how a virtual machine could use side channel timing information to extract private cryptographic keys being used in other virtual machines on the same physical server. However, in many cases an attacker wouldn’t even need to go to such lengths. If a multitenant cloud service database is not properly designed, a flaw in one client’s application could allow an attacker access not only to that client’s data, but every other client’s data as well.

Unfortunately, while data loss and data leakage are both serious threats to cloud computing, the measures that put in place to mitigate one of these threats can exacerbate the other. Customer may be able to encrypt his data to reduce the impact of a data breach, but if he lose his encryption key, he’ll lose his data as well. Conversely, customer may decide to keep offline backups of his data to reduce the impact of a catastrophic data loss, but this increases his exposure to data breaches.

4.1.9.2 Data Loss

For both consumers and businesses, the prospect of permanently losing one’s data is terrifying.

Of course, data stored in the cloud can be lost due to reasons other than malicious attackers. Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers’ data unless the provider takes adequate measures to backup data. Furthermore, the burden of avoiding data loss does not fall solely on the provider’s shoulders. If a customer encrypts his or her data before uploading it to the cloud, but loses the encryption key, the data will be lost as well.

Under the new EU data protection rules, data destruction and corruption of personal data are considered forms of data breaches and would require appropriate notifications.

Additionally, many compliance policies require organizations to retain audit records or other documentation. If an organization stores this data in the cloud, loss of that data could jeopardize the organization’s compliance status.

4.1.9.3 Account or Service Traffic Hijacking

Account or service hijacking is not new. Attack methods such as *phishing, fraud, and exploitation of software vulnerabilities* still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.

Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

In April 2010, Amazon experienced a Cross-Site Scripting (XSS) bug that allowed attackers to hijack credentials from the site. In 2009, numerous Amazon systems were hijacked to run Zeus botnet nodes.

Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach. Organizations should look to prohibit the sharing of account credentials between users and services, and leverage strong two-factor authentication techniques where possible.

4.1.9.4 Insecure Interfaces and APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. *Provisioning, management, orchestration,* and *monitoring* are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third-parties in order to enable their agency.

While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

4.1.9.5 Denial of Service

Simply put, denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker (or attackers, as is the case in distributed denial-of-service (DDoS) attacks) causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding.

While DDoS attacks tend to generate a lot of fear and media attention (especially when the perpetrators are acting out of a sense of political "hacktivism"), they are by no means the only form of DoS attack. Asymmetric application-level DoS attacks take advantage of vulnerabilities in web servers, databases, or other cloud resources, allowing a malicious individual to take out an application using a single extremely small attack payload – in some cases less than 100 bytes long.

Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock: there's no way to get to your destination, and nothing you can do about it except sit and wait. As a consumer, service outages not only frustrate you, but also force you to reconsider whether moving your critical data to the cloud to reduce infrastructure costs was really worthwhile after all. Even worse, since cloud providers often bill clients based on the compute cycles and disk space they consume, there's the possibility that an attacker may not be able to completely knock your service off of the net, but may still cause it to consume so much processing time that it becomes too expensive for you to run and you’ll be forced to take it down yourself.

4.1.9.6 Malicious Insiders

The risk of malicious insiders has been debated in the security industry. While the level of threat is left to debate, the fact that the insider threat is a real adversary is not.

Computer Emergency Response Team (CERN) defines an insider threat as such:

A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

A malicious insider, such as a system administrator, in an improperly designed cloud scenario can have access to potentially sensitive information. From **IaaS** to **PaaS** and **SaaS**, the malicious insider has increasing levels of access to more critical systems, and eventually to data. Systems that depend solely on the cloud service provider (CSP) for security are at great risk here. Even if encryption is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack.

4.1.9.7 Abuse of Cloud Services

One of cloud computing’s greatest benefits is that it allows even small organizations access to vast amounts of computing power. It would be difficult for most organizations to purchase and maintain tens of thousands of servers, but renting time on tens of thousands of servers from a cloud computing provider is much more affordable. However, not everyone wants to use this power for good. It might take an attacker years to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes. Alternately, he might use that array of cloud servers to stage a **DDoS** attack, serve malware or distribute pirated software.

This threat is more of an issue for cloud service providers than cloud consumers, but it does raise a number of serious implications for those providers. How will you detect people abusing your service? How will you define abuse? How will you prevent them from doing it again?

4.1.9.8 Insufficient Due Diligence

Cloud computing has brought with it a gold rush of sorts, with many organizations rushing into the promise of cost reductions, operational efficiencies and improved security. While these can be realistic goals for organizations that have the resources to adopt cloud technologies properly, too many enterprises jump into the cloud without understanding the full scope of the undertaking.

Without a complete understanding of the CSP environment, applications or services being pushed to the cloud, and operational responsibilities such as incident response, encryption, and security monitoring, organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks.

An organization that rushes to adopt cloud technologies subjects itself to a number of issues. Contractual issues arise over obligations on liability, response, or transparency by creating mismatched expectations between the **CSP** and the customer. Pushing applications that are dependent on “internal” network-level security controls to the cloud is dangerous when those controls disappear or do not match the customer’s expectation. Unknown operational and architectural issues arise when designers and architects unfamiliar with cloud technologies are designing applications being pushed to the cloud.

The bottom line for enterprises and organizations moving to a cloud technology model is that they must have capable resources, and perform extensive internal and CSP due-diligence to understand the risks it assumes by adopting this new technology model.

4.1.9.9 Shared Technology Vulnerabilities

Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms, and applications. Whether it’s the underlying components that make up this infrastructure (e.g. *CPU caches, GPUs*, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models. A defensive in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider’s cloud.

A compromise of an integral piece of shared technology such as the hypervisor, a shared platform component, or an application in a SaaS environment exposes more than just the compromised customer; rather, it exposes the entire environment to a potential of compromise and breach. This vulnerability is dangerous because it potentially can affect an entire cloud at once.

2.2 Related Work

Cloud security has been in vogue on the literature and industry for a while now. Various international conferences have focused on this subject alone, such as the Association for Computer Machinery (ACM) *Workshop on Cloud Computing Security*, the *International Conference on Cloud Security Management* and the only European conference on the subject, *Secure Cloud*, which already numbers up to three editions. As a result, several scientific contributions have been published, not only in conferences proceedings, but also in international journals and magazines. Thus, there are a few works surveying this area of knowledge that are worthy to describe herein.

The Zhou M et al [14] surveyed security and privacy concerns of cloud providers. **Firstly**, the security topic was discussed while having in mind availability, confidentiality, data integrity, control, and audit properties, concluding that these do not meet current concerns. **Secondly**, the privacy topic was discussed with focus on out-of-date privacy acts that fail to protect information from being disclosed to the government and third-parties. In addition, the multi-location issue of clouds is also included in the study, stating that knowing in which country the data will be kept is a prerequisite for customers, in order to find by which laws the data is governed. It was claimed that new strategies should be put forward to achieve the five aforementioned properties and that privacy acts should be changed accordingly.

Dimitrios Zissis and Dimitrios Lekkas in their paper [15], the confidentiality, privacy, integrity, and availability aspects in clouds were placed under observation. Various issues were discussed so as to present a synthesis of security requirements and threats with respect to the service models. The study ended with the proposal of a trusted third-party solution to eradicate security threats of confidentiality, integrity, authenticity and availability. The solution combined Public Key Infrastructures (PKIs), the Lightweight Directory Access Protocol (LDAP) and Single Sign-On (SSO) with a top-down fashion of the trust tree. The study was concluded with the premise that cloud benefits will outnumber its shortcomings.

Another survey targeting security issues on the cloud service models was presented by Subashini S and Kavitha V [16]. Each model was singularly studied, pointing out some of the most significant security vulnerabilities, threats and risks. It should be noted that the SaaS model was the one with the majority of the issues. An overview of current solutions discussed in the literature is presented afterwards. Yet again, the study was concluded saying that proper solutions should be designed and deployed to allow the cloud industry expand further.

The security and privacy topics were again discussed by Xiao Z and XiaoY [17]. A comprehensive and technical review of security issues was included in the study, in which confidentiality, integrity, availability, accountability and privacy preservability were identified as the most significant attributes. To each property, a few security issues are described, followed by the corresponding defense solutions. In the end, it was claimed that the study might help shaping the future research directions in the security and privacy contexts in terms of clouds.

Chunming Rong et al [18], various security challenges were enumerated as key topics in cloud security.

Those challenges related with resource allocation, system monitoring and logging, computer forensics, virtualization, multi-tenancy, authentication and authorization, availability, and cloud standards. The study particularly focused afterwards on introducing the Service Level Agreements (SLAs), trust, and accountability topics with regard to cloud security. Issues and solutions were dually discussed throughout the study.

The previous works defined the basis of this chapter by providing materials to review the state-of-the-art on the subject. Nonetheless, the review presented in this chapter contains a wider analysis when compared to those studies, allowing to construct a broader taxonomy for cloud security issues, leaving aside a deeper analysis of solutions for such issues. As commonly seen in other works, including the ones above, the chapter also discusses basic cloud and cloud security concepts in order to ease its understanding.

Liliana F. B. Soares et al [19], a paper discussed cloud computing security and how authentication is evolving Secure, and present a work of constructing a model for carrying out authentication securely in cloud computing management interfaces.

The study has shown interest in the importance of authentication on cloud management interfaces, emphasizing some of the related issues and presenting a model that, by resorting to cloud computing technology, may enable the construction of more resilient, securer and backward compatible authentication systems. A prototype using readily available tools shows the feasibility of implementing such a model in practice using smartcard-based authentication, in this case. This approach adheres to the trends discussed herein. The fact that the model offers backward compatibility may help in the process of gradually replacing password-based mechanisms in the future.

Maninder Singh and Sarbjeet Singh [20] proposes a scheme in which authentication process is carried out in two levels or two tiers. First tier uses simple username and password. Second tier is pre-determined series of steps. This schema executing secure financial transactions over Internet and does not require any additional hardware and software. So this can be used and accessed from anywhere across the globe.

Kawser Wazed Nafi et al [21] proposed a security architecture for cloud computing platform. This architecture aims to ensure secure communication system and hiding information from others. AES based file encryption system and asynchronous key system for exchanging information or data is included in the model. The structure can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. The model also includes onetime password system for user authentication process. The proposed architecture mainly deals with the security system of the whole cloud computing platform.

2.3 Summary

The Cloud computing opens up a new world of opportunities for businesses, but mixed in with these opportunities are numerous security challenges that need to be considered and addressed prior to committing to a cloud computing strategy.

The study in [14, 16] the others was surveyed security issues on the cloud. However, the study in [19, 20] discussed the authentication in cloud computing management interface. But study in [21] proposed security architecture for cloud platform to ensure security communication.

It can be argued that the desire to improve one's status is a highly motivation force, and is central to the idea of cloud security motivation.

CHAPTER (3)

METHODOLLOGY

The benefits of cloud adoption are numerous, including improved efficiency, reduced costs, high availability and greater accessibility and flexibility. Cloud computing is one of the fasted evolution in the field of the Information Technology. However, as more information on individuals and companies is placed in the cloud, companies must address cloud computing security issues**.**

Like other major business decisions, an enterprise must evaluate the benefits and be prepared to address any risks and challenges cloud adoption fetch. Moving applications to the cloud and accessing the benefits means first evaluating specific data security issues and cloud security issues.

The methodology used in this research depend on the idea of securing data in its both situation (at the rest, and while its transfer), to achieve this goal, the system has been proposed depending on the following:

- Securing data from cloud provider’s side.
- Securing data from cloud user’s side.

3.1 Securing data from cloud provider’s side

3.1.1 Implementing Authentication Protocol

From cloud provider side, the purposed system implemented the EAP-CHAP authentication protocol on the Cloud environment for authentication purpose. The EAP-CHAP authentication protocol is a type of cryptographic protocol with the purpose of authenticating entities wishing to communicate securely.

It is used for the transport and usage of keying material and parameters generated by EAP methods. The purposed model used Challenge-Handshake Authentication Protocol (CHAP) for authentication.

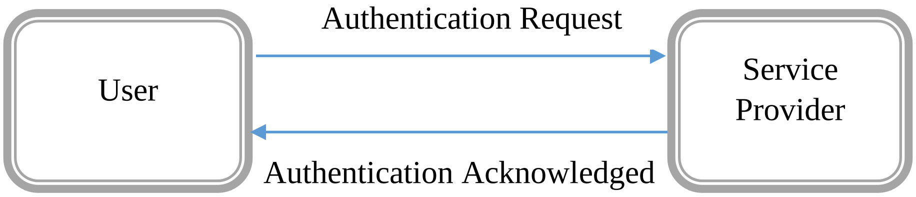


Figure (3.1): authentication Process in general

3.1.1 Keeping user’s data in an encrypted form

By using **SHA-1** encryption algorithm to encrypt user’s credentials before storing it into database.

To achieve this goal, the database contains the encrypted user’s credential was designed using MS-SQL Server. And the website that represents the interface between the cloud user’s and the cloud provider was designed using MS-Visual Basic.

3.2 Securing data from cloud user’s side

To ensure the data confidentiality and it not exposed by outsiders in the event of a security problem on the provider side, the encryption software designed to encrypt data before it is sent to the cloud.

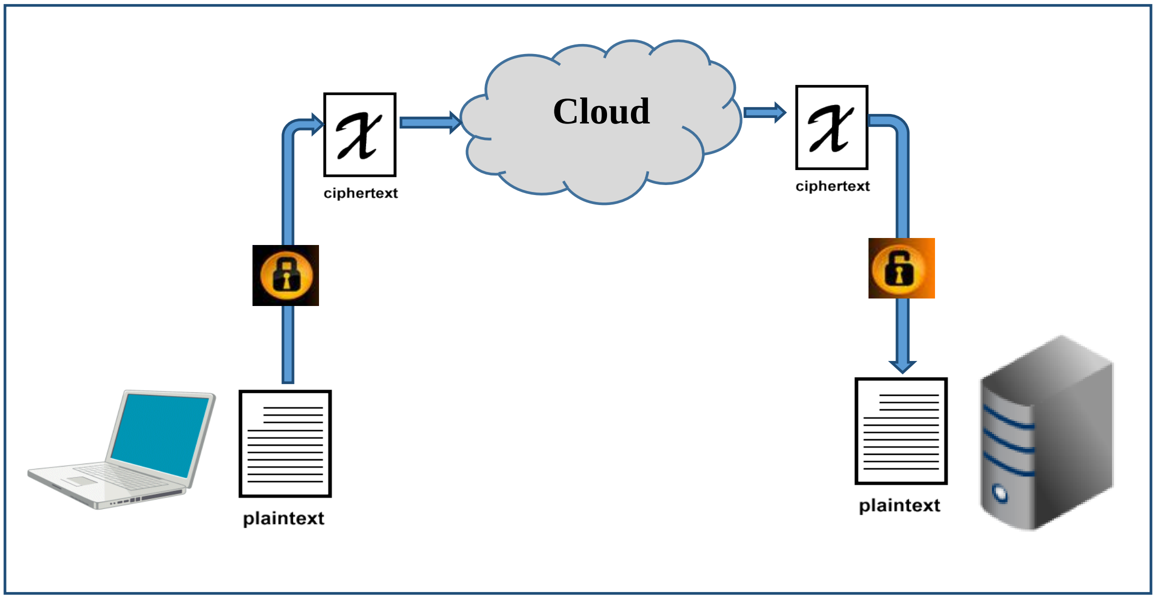


Figure (3.2): Encryption Process

CHAPTER (4)

IMPLEMENTATION

4.1 The Proposed Method

The proposed method depend on two different phases used for ensuring security in cloud.

4.1.1 Phase 1: Using the Extensible Authentication Protocol-CHAP

Extensible Authentication Protocol (EAP) is an authentication framework frequently used in wireless networks and point-to-point connections.

EAP provide the transport and usage of keying material and parameters generated by EAP methods. There are many methods, here we will implemented the EAP on the environment of the cloud for authentication purpose, and using the Challenge-Handshake Authentication Protocol (CHAP) for authentication.

When the supplicant needs data or any service of cloud computing, the Service Provider Authenticator (SPA) first requests for client identity. The whole process between client and Cloud provider explain in a figure (4.1) given below.

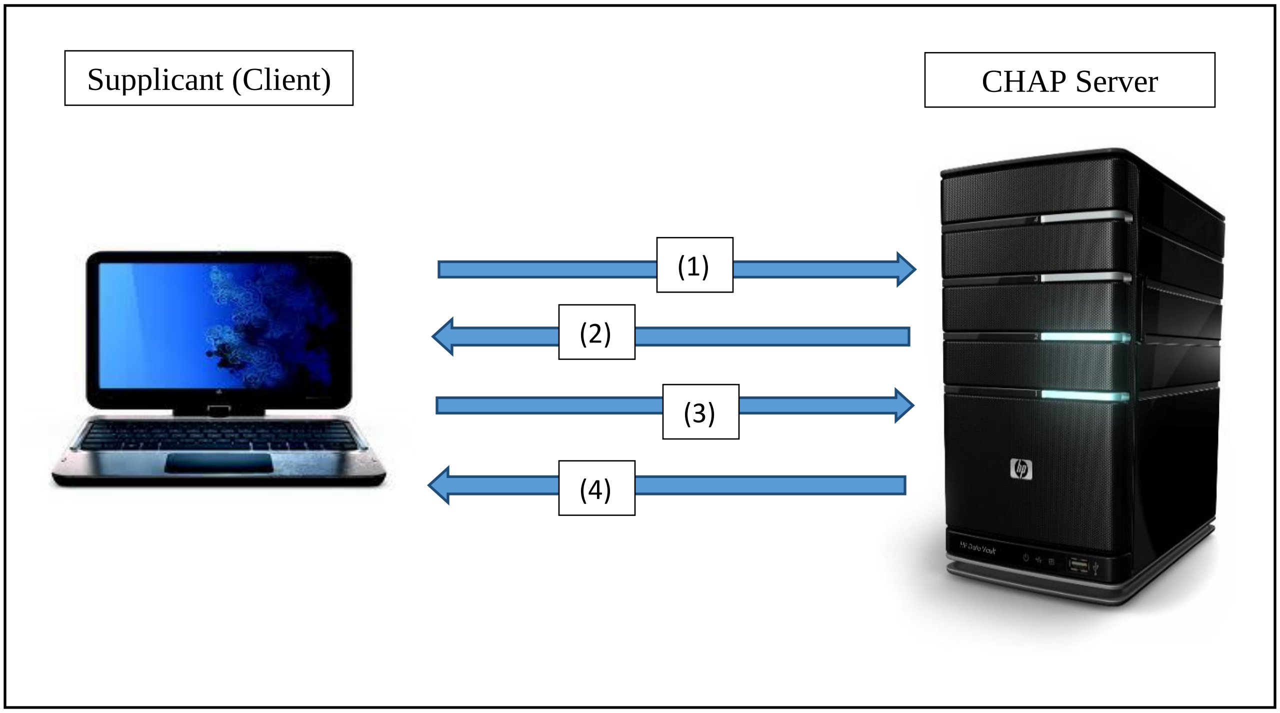


Figure (4.1): CHAP Authentication Process

4.1.1.1 The steps of CHAP authentication

1. When client demands a service, Service Provider Authentication sends a "challenge" message to client, (Send user ID in plaintext).
2. The CHAP server send a random string (calculate hash value of string and password).
3. Client responds with a value that is calculated by using one way hash function on the challenge, (return hash value of random string and password).
4. Authenticator verifies the response value against its own calculated hash value. If the values match, the Cloud provider will give service, otherwise it should terminate the connection.

Implementation of EAP-CHAP in Cloud Computing will solve the authentication and authorization problems.

4.1.2 Phase 2: Keeps the user's data in an encrypted form

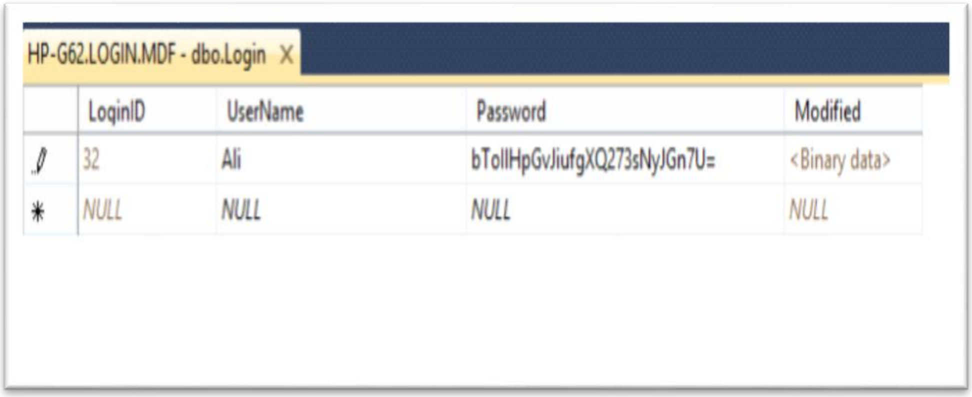
In this phase the database that keeps users credentials in an encrypted form was developed, and the website thet is used to access the cloud was developed with certain security criteria.

4.1.2.1 The login database

By using SQL Server 2012 the database that included user's credentials was developed, the developed database containing two tables named **Login, Salt**.

The Login table stored users credential as encrypted form by using SHA-1 hashing algorithm.

The figure (4.2) below show the Login table in edit preview



HP-G62.LOGIN.MDF - dbo.Login X

	LoginID	UserName	Password	Modified
✎	32	Ali	bTollHpGvJiufgXQ273sNyJGn7U=	<Binary data>
*	NULL	NULL	NULL	NULL

Figure (4.2): Login table

The login table contains the flowing fields:

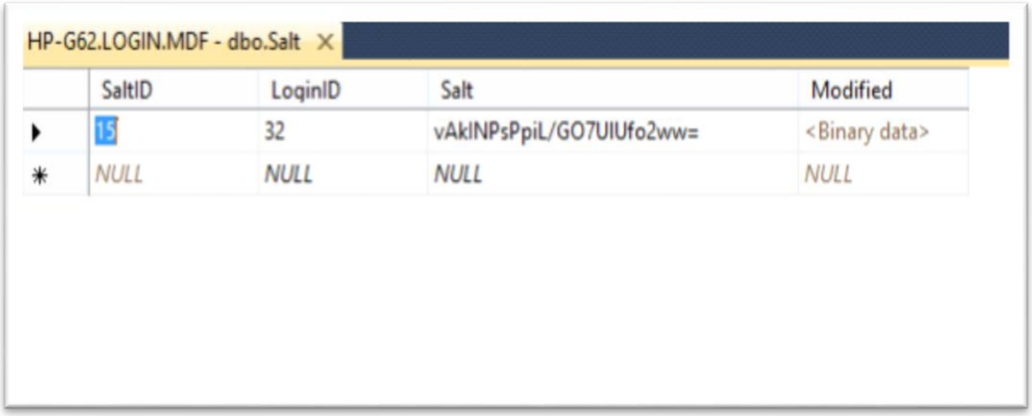
1- LoginID: Login Identification is a unique number and it represent the number of the user name, this field is a primary key for this table.

2- UserName: User Name, this field contain the user's names.

3- Password: This field contain the user's passwords in encrypted form (hashed).

4- Modified: This field is working to record the date and time of the amendment which was implemented on the record automatically

The figure (4.3) below show the Salt table in edit preview.



	SaltID	LoginID	Salt	Modified
▶	15	32	vAkINPsPpiL/GO7UIUfo2ww=	<Binary data>
✱	NULL	NULL	NULL	NULL

Figure (4.3): Salt table

The figure (4.4) below show the relation between Login table and Salt table.

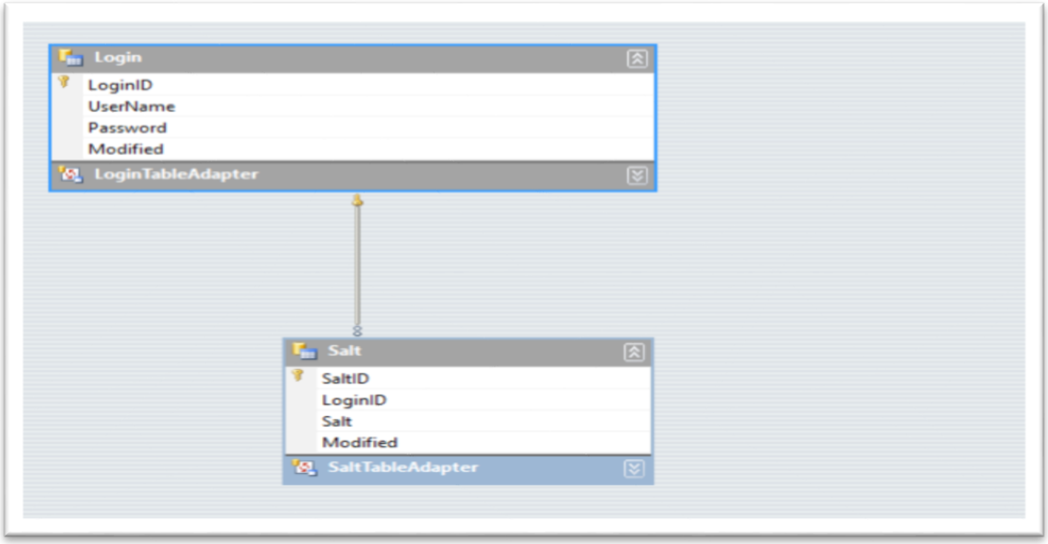
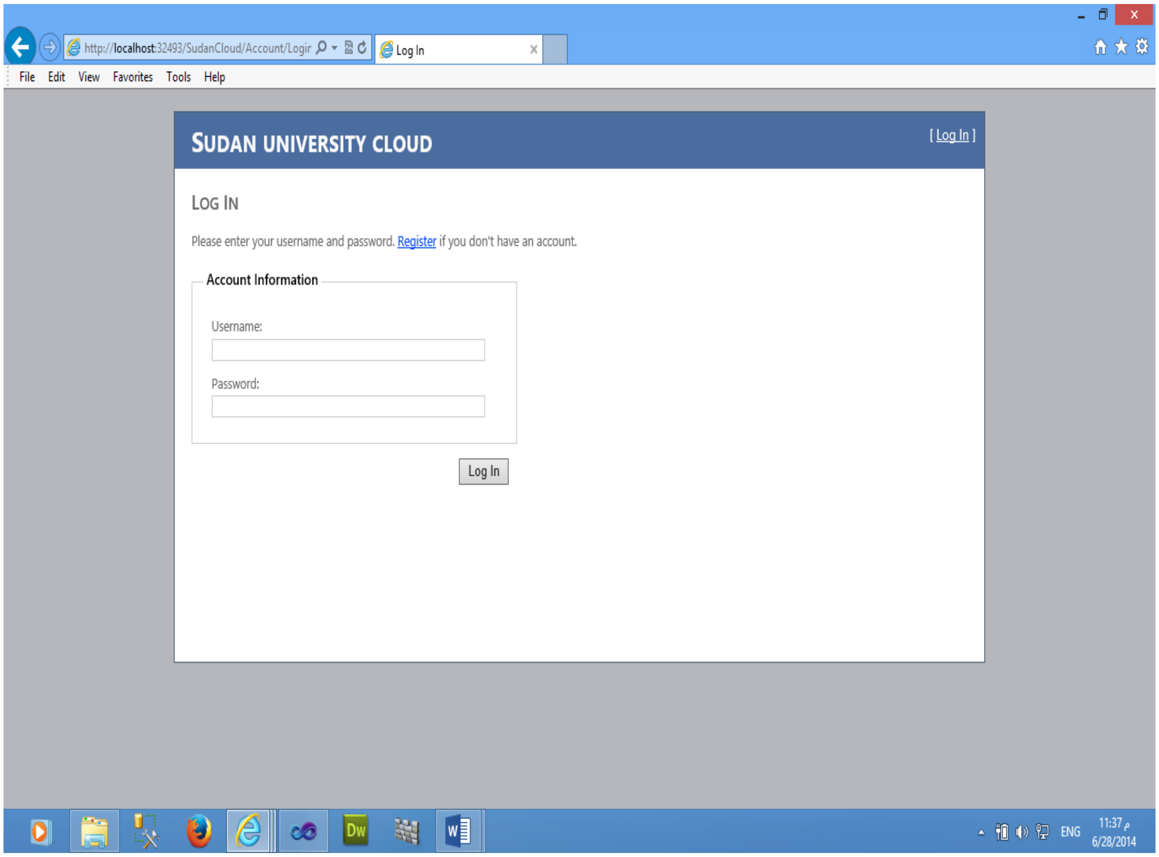


Figure (4.4): Relation between Login table and Salt table

4.1.2.2 The login Page

The figure (4.5) below show the login page that developed to access to the cloud services.



Please enter your username and password. Register if you don't have an account.

Figure (4.5): Login Page

The login page of the website was designed using Visual basic.net 2010.

The general workflow for account registration and authentication in a hash-based account system is as follows:

1. The user creates an account.

2. His password is hashed and stored in the database. At no point is the plain-text (unencrypted) password ever written to the hard drive.
3. When the user attempts to login, the hash of the password he entered is checked against the hash of their real password (retrieved from the database).
4. If the hashes match, the user is granted access. If not, the user is told he entered invalid login credentials.
5. Steps 3 and 4 repeat every time someone tries to login to their account.

In step 4, never tell the user if it was the username or password they got wrong. Always display a generic message like "Invalid username or password." This prevents attackers from enumerating valid usernames without knowing their passwords.

4.1.2.3 Encrypt the user’s files before sending it to the cloud

Encryption is the method of scrambling or locking the contents of a file and makes the files unreadable with an encryption key or pass phrase so that even if somebody gains access to cloud – it doesn’t matter because the only thing an intruder sees is gibberish. Only by using the key, the contents of the file can properly displayed.

4.1.2.3.1 The developed package

for these purpose the package that encrypt files before sending it to the cloud was developed using Visual Basic .Net, this package has two functions are:

1- Encrypt file before uploading it to the cloud.
2- Decrypt file after download it from the cloud.

The figure (4.6) below show the developed package

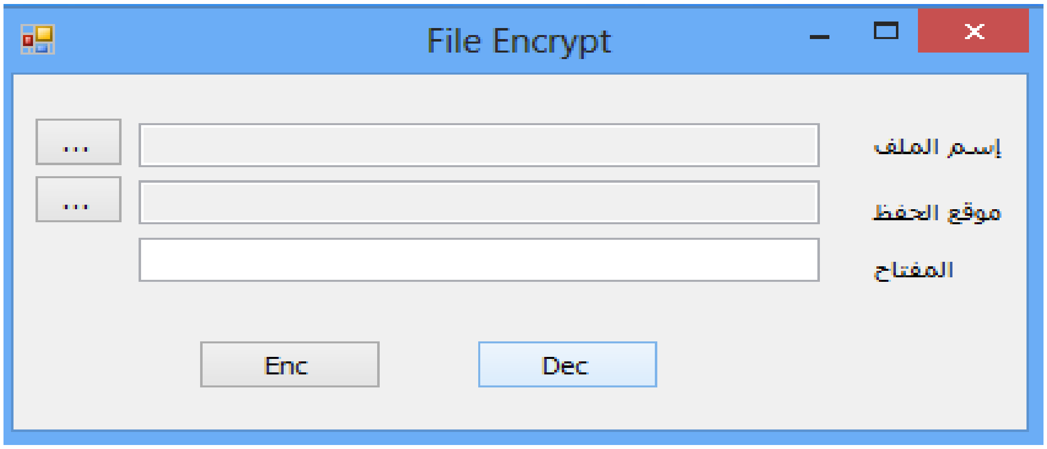


Figure (4.6): Encrypt/ Decrypt Package

4.1.2.4 The encryption algorithm

The encryption algorithm used in developed package is Advance Encryption Standard AES-256.

The AES is a symmetric-key block cipher algorithm, and it has a fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits, based on finite field calculations.

4.1.2.4 .1 The AES features:

- Block encryption implementation.
- 128-bit group encryption with 128, 192 and 256-bit key lengths.
- Symmetric algorithm requiring only one encryption and decryption key.
- Data security for 20-30 years.
- Worldwide access.
- No royalties.
- Easy overall implementation.

The encryption process in this section performed in the user side, by user local machine (offline).

4.2 Results

By used the proposed system it was able to add more secured techniques in the client and provider sides, as well as securing the connection.

The proposed system provide protection against many attacks such as:

- Man-in-the-middle attack (MITM).
- Brute-force or dictionary attack.
- Replay or playback attack.
- Server attack.
- Eavesdropping attack.
- Provide protection against data theft.
- Acts as identity theft prevention.

4.3 Analysis

4.3.1 Securing the Connection

The proposed system using an Extensible Authentication Protocol, or EAP.

EAP is an authentication framework frequently used in wireless networks and point-to-point connections. EAP is an authentication framework providing for the transport and usage of keying material and parameters generated by EAP methods, designed to work as a link layer authentication protocol and many different authentication protocols can be used over it. EAP is not a wire protocol; instead it only defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages.

EAP has addition support for a variety of authentication schemes including smart card it’s often used with VPNs to add security against brute-force or dictionary attacks.

4.3.1.1 Challenge-Handshake Authentication Protocol

The Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake.
This is done upon initial link establishment, and may be repeated any time after the link has been established.

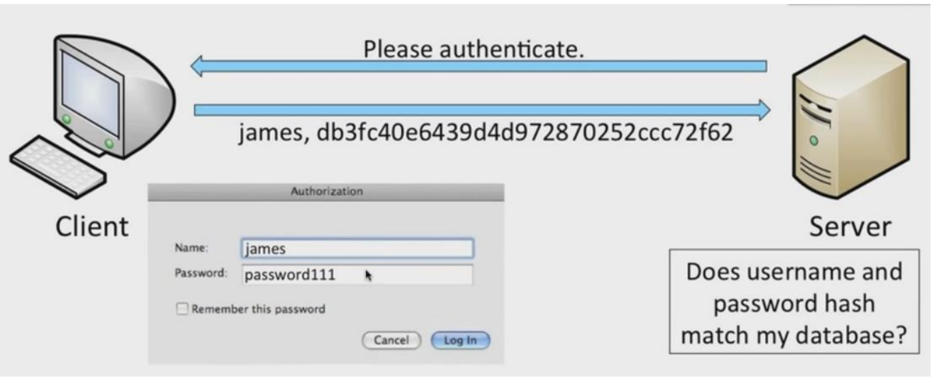
1. After the Link Establishment phase is complete, the authenticator sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a "one-way hash" function.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection SHOULD be terminated.
4. At random intervals, the authenticator sends a new challenge to the peer, and repeats steps 1 to 3.

4.3.1.2 CHAP Advantages

CHAP provides protection against playback attack by the peer through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges.

This authentication method depends upon a "secret" known only to the authenticator and that peer. The secret is not sent over the link.
Although the authentication is only one-way, by negotiating CHAP in both directions the same secret set may easily be used for mutual authentication.
Thus, CHAP provides better security as compared to Password Authentication Protocol (PAP) which is vulnerable for both these reasons.

Since CHAP may be used to authenticate many different systems, name fields may be used as an index to locate the proper secret in a large table of secrets. This also makes it possible to support more than one name/secret pair per system, and to change the secret in use at any time during the session.



Please authenticate.
james, db3fc40e6439d4d972870252ccc72f62
Client
Server
Authorization
Does username and password hash match my database?
Cancel
Log In

Name: james
Password: password111
□ Remember this password

Figure (4.8) Hashing user’s credentials and send it to cloud provider

4.3.2 Security measures in the database

Identity theft remains one of the highest priorities for fraudsters today. Encrypting the data ensures that your identity is protected in the event that it is lost or stolen. Thus Storing user’s sensitive data with encrypted form in database provide protection against potential threats such as lost or stolen data, and acts as identity theft prevention.

4.3.3 Security measures in the Login Page

The login page contain a form that is sending user’s credentials in a hashed form which provide protection against data theft, Man-in-the-middle attack, and other eavesdropping attack mechanisms.

4.3.4 Security measures in the encryption files package

The encryption of cloud user’s file before sending and sending it to the cloud provider in an encrypted form that provide protection against data theft. If a hacker gained access to the cloud platform he couldn’t read or modify any user’s files.

CHAPTER (5)

CONCLSION AND FUTURE WORK

5-1 Conclusion

Cloud computing offers many businesses a new way of accessing computing services. This can also expose organizations to a range of risks which they were unaware of. Thus data security has become the vital issue of cloud computing security.

From the consumer's perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services.

So in this we focused on client side and provider side security in our proposed system, only the authorized user can access the data. Even if some intruder (Unauthorized user) gets access of the data accidentally or intentionally, he will not be able to decrypt it. Also it is proposed that encryption must be done by the user to provide better security.

5-2 Future Work

More research should be funded to find ways to mitigate existing and new security risks in the cloud computing environment.

This thesis suggested that in the near future, the IT discipline needs to shift to using or developing **Security as a Service** to adapt to new threat scenarios in both public cloud computing and virtualization of their IT infrastructure.

References

[1] [2] [3] [4] “Cloud Computing Security Challenges,” in http://www.webopedia.com/DidYouKnow/Hardware_Software/cloud_computing_security_challenges.html, 2011.

[5]http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

[6] Michael Hange,” Security Recommendations for Cloud Computing Providers,” in www.bsi.bund.de.2013.

[7] Rostyslav Slipetskyy,” Security Issues in OpenStack,” M.S. thesis, Norwegian University of Science and Technology-Department of Telematics, 2011.

[8] Surya Nepal and Mukaddim Pathan, *Security, Privacy and Trust in Cloud Systems*. Springer Press, 2014.

[9] Peter Mell, “The NIST Definition of Cloud Computing,” National Institute of Standards and Technology, NIST Special Publication 800-145, September 2011.

[10] [12] Jerry Archer et al, “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,” Cloud Security Alliance, 2011.

[11] Ilias Tsagklis. (2013, April). Advantages and Disadvantages of Cloud Computing – Cloud computing pros and cons. Available: http://www.javacodegeeks.com/2013/04/advantages-and-disadvantages-of-cloud-computing-cloud-computing-pros-and-cons.html.

[13] Aaron Alva et al, “The Notorious Nine: Cloud Computing Top Threats in 2013,” Cloud Security Alliance. 2013.

[14] Zhou M, Zhang R, XieW, QianW, Zhou A (2010) Security and privacy in cloud computing: a survey. In: *6th international conference on semantics knowledge and grid*, Ningbo, China, 2010, pp 105–112.

[15] ZissisD, LekkasD, “Addressing cloud computing security issues,” in *FutureGener Comput Sys* 2012, pp 583–592.

[16] Subashini S, Kavitha V, “A survey on security issues in service delivery models of cloud computing,” in *Journal of Network and Computer Applications*, 2011, pp 1–11.

[17] Xiao Z, XiaoY, “Security and privacy in cloud computing,” in *IEEECommunSurvTutorials*, 2012, pp 1–17.

[18] Chunming Rong et al, “A survey on security challenges in cloud computing,” in *Computers and Electrical Engineering*, 2013, pp 47-54.

[19] Liliana F. B. Soares et al. “Secure User Authentication in Cloud Computing Management Interfaces”, *ipccc.org/ipccc2013.*

[20] Maninder Singh and Sarbjeet Singh, “Design and Implementation of Multi-tier Authentication Scheme in Cloud”, in *International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012*.

[21] Kawser Wazed Nafi et al, “ A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture”, *International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012*.