International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

AN EMPIRICAL CRYPTOGRAPHY ALGORITHM FOR CLOUD SECURITY BASED ON HASH ENCRYPTION

Dr. Smith Jones
Malaysia University of Technology
Malaysia

ABSTRACT

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was $16billion in 2008 and will rise to $42billion/year by 2012 . It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications . According to a Gartner press release from June 2008, Cloud Computing will be "no less influential than e-business". Cloud computing evokes different perceptions in different people. To some, it refers to accessing software and storing data in the "cloud" representation of the internet or a network and using associated services. To others, it is seen as nothing new, but just a modernization of time-sharing model that was widely employed in 1960s before the advent of relatively lower-cost computing platforms. This development eventually evolved to the client/server model and to the personal computer, which placed large accounts of computing power at people's desktops and spelled the demise of time-sharing systems. This paper proposes and implement a new algorithmic approach for cloud security using key based cryptography. This work can be enhanced using hybrid approach by integrating multiple cryptography algorithms.

Keywords – Cloud Security, Cryptography, Hash Encryption

INTRODUCTION

There is a lot of discussion of what cloud computing exactly is. The U.S. National Institute of Standards and Technology (NIST) have put an effort in defining cloud computing, and as NIST"s publications are generally accepted, their definition of cloud computing will be used in this thesis. The NIST definition of cloud computing is :

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

Cloud computing is the collective term for a group of IT technologies which in collaboration are

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

changing the landscape of how IT services are provided, accessed and paid for. Some of the supporting technologies have already been available for quite some time, but it is the combination of several technologies which enables a whole new way of using IT .

Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services .

The cloud is a metaphor for the Internet and is an abstraction for the complex infrastructure it conceals. There are some important points in the definition to be discussed regarding Cloud Computing. Cloud Computing differs from traditional computing paradigms as it is scalable, can be encapsulated as an abstract entity which provides different level of services to the clients, driven by economies of scale and the services are dynamically configurable .

To explain the definition in short, “convenient on-demand network access”, together with “minimal management effort or service provider interaction,” stands for easy and fast network access to resources that are ready to use. With a “shared pool of resources,” the available computing resources of a cloud provider are combined as one big collection, to serve all users. The “rapid provisioning and releasing” of computing resources is used to quickly match available resources, with the need for those resources. This rapid provisioning prevents a lack of computing power when the need increases, while rapid release of assigned resources prevents that resources are idle while they may be required elsewhere .

There are many definitions of Cloud computing, a recent study noted more than 22 different definitions of cloud computing where variety of technologies in the Cloud makes the over-all picture confusing.

Multitenancy (shared resources): Unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated to a single user or owner), cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level .

Scalability: cloud computing have property to scale to tens of thousands of system with bandwidth and storage also .

Elasticity: It is the property of increasing and decreasing the resources according to the users’ need, as well as release the resources when they are no longer needed .

Pay as you go: One of the advantage of cloud computing is to pay according to the need or consumption like for one hour, two hour or cost per gigabyte and so on which has large impact on cost or economics. So cloud computing model provides a cheaper way for business to acquire and use the IT – capabilities .

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

Self provisioning of resources: Users self-provision resources like additional system and network resources .

Taking these features into account this thesis provides an encompassing definition of the Cloud. Obviously, the Cloud concept is still changing and these definitions show how the Cloud is conceived today:

"Cloud computing is model that makes reference to the two essential concepts: 'abstraction' and 'virtualization' to increase the capacity and capability of IT by providing on demand network access to shared pool of computing resources without investing in new infrastructure."

THE SOFTWARE- AS- A- SERVICE MODEL

Conventional way of utilising software involved the customer loading the software onto his own hardware after paying license fee (a capital expense, known as CapEx). For other support services the customer could also purchase a maintenance agreement. The customer was afraid with the compatibility of operational systems, patch installations, and compliance with license agreements.

In a SaaS model, there is no requirement for purchase software, but rather rents it for use on a pay as you grow model (an operational expense, known as OpEx). In some cases, the service is free for limited use. Typically, the purchased service is complete from a hardware, software, and support perspective. The user accesses the service through any authorized device

THE PLATFORM- AS- A- SERVICE MODEL

Pass is also a variation of saas model where the development environment is offered as a service. In paas solution the development tool is hosted in cloud which is accessed via browser and can built web applications without installing any tool on their own system and can then deploy those applications without any administrative skills .

INFRASTRUCTURE- AS- A- SERVICE MODEL

In the traditional hosted application model, the vendor provides the entire infrastructure for a customer to run his applications. Often, this entails housing dedicated hardware that is purchased or leased for that specific application where as Iaas model offers the various computing services as provided in utility computing. In this model we pay for the processing power, disk space and so on which is actually consumed by us. Iaas is typical a service associated with cloud computing including physical computing resources, location, data partitioning, scaling, security, backup and so on. Examples are Amazon EC2, S3, suns' cloud services etc. Various features that should be available for Iaas system includes:

- **Scalability:** The ability to scale infrastructure requirement.
- **Pay as you go:** The ability to purchase the infrastructure required at any specific time.
- **Best- of- breed technology:** Ability to access the best suitable service and solutions for a fraction of cost

Public Clouds

A public cloud is hosted, operated, and managed by third party vendor from one or more data centres.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

In a public cloud, security management and day-to- day operations are relegated to third party vendor, who is responsible for the public cloud service offering. Hence, the customer of the public cloud service offering has a low degree of control and oversight of the physical and logical security aspects of a private cloud . There are a few challenges listed below that are preventing wide scale adoption of public clouds .

- **Security:** The biggest roadblock is the potential security issues due to multitenant nature of public clouds. There are security and privacy concerns with sharing same physical hardware with unknown parties that need to addressed.

- **Reliability and Performance:** Performance and availability of the applications are important criteria defining the success of an enterprise's business. However, the fact that organizations lose control over IT environment and important success metrics like performance and reliability, and are dependent on factors outside the control of the IT organizations makes it dangerous for some mission critical applications.

- **Vendor Lock-in:** Cloud computing services offered by different vendors are not governed by any standards as of today. Depending on the vendor, the applications have to undergo changes to adapt to the service.

- **Leveraging Existing Investment:** Most large organizations that have already invested in their own data centers would see a need to leverage those investments as an important criterion in adopting cloud computing.

- **Corporate Governance and Auditing:** Performing governance and auditing activities with the corporate data abstracted in the public cloud poses challenges that are yet to be addressed.

- **Maturity of the Solutions:** Some of the PaaS offering like AppEngine offer limited capabilities like only a subset of JDO API.

PRIVATE CLOUDS

To overcome all above challenges enterprises adopt the private clouds which is managed or owned by an organization to provide the high level control over cloud services and infrastructure. In other words private cloud is build specifically to provide the services within an organization for maintaining the security and privacy. As such, a variety of private cloud patterns have emerged :

- **Dedicated:** Private cloud hosted within a customer- owned data center or at a collection facility, and operated by internal IT departments.

- **Community:** Private clouds located at the premises of third party; owned, managed, and operated by a vendor who is bound by customer SLAs and contractual clauses with security and compliance requirements.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

- **Managed:** Private cloud infrastructure owned by customer and managed by a vendor.

HYBRID CLOUDS

This model comprised both the private and public cloud models where organisation might run non-core application in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud

Barriers to Cloud Computing Adoption in Enterprise

Though each cloud computing platform has its own strength, one thing should be noticed is that no matter what kind of platform there is lots unsoloved issues. For example, continuously high availability, dealt mechanisms of cluster failure in cloud environment, consistency guaranty, synchronization in different clusters in cloud platform, interoperation and standarization, the security of cloud platform and data in transmission and so on are all among the issue to be better solved .

- **Control**

Some IT departments are concerned because cloud computing providers have a full control of the platforms. Cloud computing providers typically do not design platforms for specific companies and their business practices .

- **Performance**

The major issue in performance can be for some intensive transaction-oriented and other data-intensive applications, in which cloud computing may lack adequate performance. Also, users who are at a long distance from cloud providers may experience high latency and delays .

- **Bandwidth Costs**

With cloud computing, companies can save money on hardware and software; however they could incur higher network bandwidth charges. Bandwidth cost may be low for smaller Internet-based applications, which are not data intensive, but could significantly grow for data-intensive applications .

- **Political Issues Due to Global Boundaries**

In the cloud computing world, there is variability in terms of where the physical data resides, where processing takes place, and from where the data is accessed. Given this variability, different privacy rules and regulations may apply. Because of these varying rules and regulations, by definition politics becomes an element in the adoption of cloud computing, which is effectively multijurisdictional .

- **Reliability**

Cloud computing still does not always offer round-the-clock reliability. There were cases where cloud computing services suffered few-hours outages . In the future, we can expect more cloud computing providers, richer services, established standards, and best practices.

- **Security**

Because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels (e.g.,

network, host, application, and data levels) can be achieved. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing. The subsequent chapters present a detailed examination of those concerns to determine whether they are grounded .

- **Privacy**

The ability of cloud computing to adequately address privacy regulations has been called into question. Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model .

- **Connectivity and Open Access**

The full potential of cloud computing depends on the availability of high-speed access to all.
Such connectivity, rather like electricity availability, globally opens the possibility for industry and a new range of consumer products. Connectivity and open access to computing power and information availability through the cloud promotes another era of industrialization and the need for more sophisticated consumer products .

- **Interoperability**

The interoperability and portability of information between private clouds and public clouds are critical enablers for broad adoption of cloud computing by the enterprise. Many companies have made considerable progress toward standardizing their processes, data, and systems through implementation of ERPs. This process has been enabled by scalable infrastructures to create single instances, or highly integrated connections between instances, to manage the consistency of master and transaction data and produce reliable consolidated information. Even with these improved platforms, the speed at which businesses change may still outpace the ability of IT organizations to respond to these changes. SaaS applications delivered through the cloud provide a low-capital, fast-deployment option. Depending on the application, it is critical to integrate with traditional applications that may be resident in a separate cloud or on traditional technology. The standard for interoperability is either an enabler or a barrier to interoperability, and permits maintenance of the integrity and consistency of a company's information and processes .

Cloud security and Privacy Issues

Security and privacy are indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security.

Dependency among Cloud Layers

The application layer and core layer depends upon VMs layer and physical machine layer which further depend upon virtual network layer and physical network layer so damage at any layer also have great impact on other layers.

Complexity of Security Aspects

When we think about security of organization's core IT infrastructure there is need to provide security at network level, host level, application

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

level and when we talk about data security two aspects are included 'data transmission security and data storage security'.

CLOUD SECURITY ISSUES

In cloud computing the Security issues deals with all the challenges associated with securing an organization's core IT infrastructure at the network, host, and application levels as well as the vulnerabilities and attacks related to the data security including: Data-in-transit, Data-at-rest, Processing of data including multitenancy, Data lineage, Data provenance . To cover all these security issues possible within the cloud, and in-depth, would be herculean task. Existing efforts look to provide a taxonomy over the issues seen. The Cloud Security Alliance is a non-profit organisation that seeks to promote the best practises for providing security assurance within the cloud computing landscape. In Hubbard, Sutton et al. the Cloud Security Alliance identify seven threats to cloud computing that can be interpreted as a classification of security issues found within the cloud. They are:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service and Traffic Hijacking
- Unknown Risk Profile

This thesis analysed the various possible vulnerabilities and attacks that are caused because of above defined security issues found within cloud.

Network level attacks

During resource pooling process all data or services flow over the network needs to be secured from following attacks to prevent the leakage of sensitive information or other vulnerabilities :

- **Denial of service/distributed denial of service attack**

  This attack can overwhelm target's resources so that authorised user is abstained from getting the normal services of cloud. DDOS is also based on DOS attack which can be distributed for more significant effects. This attack is a cause of failure of availability.

- **Eavesdropping**

  Eavesdropping is an interception of network traffic to gain unauthorized access. It can results in failure of confidentiality .

- **Man in the Middle attack**

  It is also a category of eavesdropping. The attack set up the connection with both victims that makes conversation and making them believe that they talk directly but infect the conversation between them is controlled by attack.

- **Replay attack**

  The attacker intercepts and save the old messages and then send them later as one of

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

participants to gain access to unauthorized resources.

- **Back Door**

The attacker gain access to network through bypassing the control mechanisms using "back door" such as modem and asynchronous external connections .

- **Impersonation**

It is vulnerability in which malicious node modify the data flow route and lure the node to wrong positions.

- **Sybil attack**

In *Sybil attack* a malicious user pretends to be distinct users after acquiring multiple identities and tries to create relationship with honest user if malicious user is successful to compromise one of the honest user then attack gain unauthorized privileges that helps in attacking process.

- **Byzantine failure**

It is a malicious activity which compromised a server or a set of server to degrade the performance of cloud.

Attacks and Vulnerabilities Based on Security Techniques

If any security technique has weakness in implementation it can cause various vulnerabilities:

- Inside channel attack gain the information from physical implementation of cryptosystem to break the security. The information is like technical knowledge on which encryption implement, time information, power consumption and others.
- SSL/SSH/TLS use the cryptography techniques to secure the data but any crucial flow in implementation of cryptography algorithm can make stronger cryptography technique to weak technique which is a main target of hackers .

Language and Malicious Program Injection Based Attack:

One of the most frequently discovered vulnerabilities in cloud are a direct result of language and programmes that are as follow .

- **Buffer overflow**

It is a favourite exploit for hacker which takes the advantage of programme that is waiting for user's input. But in place of user the hacker would enter the input which results to move the control to attack code.

- **Trojan horses/Malware**

They are the unauthorized program that are contained or injected by malicious user within legitimate program to perform unknown and unwanted function.

- **XML Signature wrapping Attack**

It is well known attack on protocols like SOAP that use XML format to transfer the request for services. In this, attack moves the original body of SOAP message to newly inserted wrapping element writing within SOAP header and create a new body which

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

contains the operation that an attack wants to perform .

Web Application Attacks

Web browser is one of the way of providing the web application virtually to users but at the same time they also creates vulnerabilities that has detrimental impact on customers as well as on cloud system .

- **Weak authentication or weak username- password**

  It is one of the main target of malicious users to gain unauthorized access to the services.

- **SQL injection flaws**

  In which malicious SQL code is erroneously executed in database backend.

- **Cross-site-scripting (XSS)**

  In which the malicious java script code is executed erroneously by browser.

Virtual Machine Based Vulnerabilities

Following are the various VM based vulnerabilities create challenges and issues for service providers.

- Any malicious programme in VM also transferred between other VMs using shared clipboard technology which is an issue for security.
- Many VMs co-exist on same server share CPU, memory, I/O have virtual boundaries. So securing the virtual boundaries is also a challenge for service provider.
- Hypervisor is main controller that maps the physical resources to virtual resources. So if any hypervisor is compromised, it is possible to trace the VMs operations unencrypted .

Problem definition and Directions for proposed solution

Over the preceding chapters the notion of data security and privacy within the cloud was discussed. In Cloud Computing there is rapid expansion in security and privacy challenges because the storage, processing and accessing of sensitive data is all done through remote machines (CSP) that are not owned or even managed by data owner themselves. As there is storage and accessing of data from cloud servers, the concerns about data confidentiality, authentication and integrity are being increased. Besides these issues there would also be chance of using a part of data or whole by cloud server for their financial gain which results the economic losses to data owner. The main reason behind the above defined issues is that the cloud servers are very likely to be the outside from trusted boundaries of data owner.

One of the related issue is also the unwanted exposure of data as result of a software malfunction or malicious CSP. When entrusting data to the cloud the data creators i.e. service users need assurances over access to their data. In essence data creators need to regain control over this access i.e. data creators need to become empowered.

Directions for proposed solution/Objectives

- **Need for data privacy and user empowerment**

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

Within computer security the protection of one's data can be seen as being synonymous with the protection of one's privacy. The `right to privacy' is a fundamental right and is enshrined in many a countries constitution. A user empowered over the privacy of their data can be seen as being empowered over the protection of their data. A thorough grasp of this notion of data privacy is fundamental when building a solution to empower users. As such a better solution can thus be designed. Data privacy in cloud can be maintained by using three existing solutions: None of Your Business (NOYB) ; Privacy Manager ; and Content Cloaking (CoClo) . Each of these three solutions each have a different take on how to protect the privacy of data.

- **Encryption.** The CoClo solution dictated the encryption of data prior to its insertion into the cloud. Data was hidden completely from unauthorised users and the CSP.

- **Obfuscation.** With Privacy Manager data was obfuscated. While `obfuscation' does not necessarily imply the encryption of data, obfuscated data can still nonetheless be operated upon by a CSP with the CSP not learning anything about the underlying data. Examples of obfuscation techniques can be found in Kantarcioglu.

- **Contextual Integrity.** The NOYB solution sought to destroy the link between the data and its creator, as well as hide the data itself.

The Proposed Algorithm

When ensuring the confidentiality over one's data the aim should be for the data creator to gain control over how the data is being used. This will include the data creator being in a position to dictate to whom access to their data should be granted.

Systems perform one or more of the following tasks on data, each with its own concerns regarding privacy .

- **Transfer**

Disclosure of sensitive data during transfer from one party to the other is a concern that has been addressed quite extensively with the use of encryption. Encryption of data during transport is a well known concept and is sufficient, on the presumption both sender and receiver are trusted parties. In the article of Spiekermann et al, the authors are more concerned about the difference between transfers with and without explicit user involvement. Sending sensitive information with the users‟ involvement, such as filling a form with private information, in order to gain access to a service, has lower privacy concerns than information that is transferred without users‟ involvement, such as cookies and other information requested by the receiver.

When we translate these privacy concerns to the cloud computing paradigm, one can make a difference between information-*push* to the cloud and information-*pull* from local resources to the cloud, where the latter has more concern. Information-pull is initiated by the cloud service provider, and depending on the service, with or without user involvement.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

- **Storage**

Storage of data can occur inside or outside the user's or corporation's direct control. When the data is stored outside the direct control, the data owner can exercise *separation of duties*, by encrypting the data before storing it externally, while keeping the means of decryption in the owner's control. This separation of duties does not work when stored data needs to be processed externally.

It may be useful to distinguish between persistent and transient storage. *Persistent* storage stores data on a long-term basis, like normal hard disks. Persistent storage brings more data retention concerns than *transient* storage, where data is deleted when the initial purpose of the data has been completed. The notion of transient storage can be implemented by preventing software to store the data on hard disks and only keep the data in memory, which is done in one of the products of cloud service provider Gigaspaces.com.

- **Processing**

Processing refers to any use or transformation of data. In the context of personal privacy, privacy concerns are raised when data is used for purposes not foreseen by users. Under European privacy laws, users must be informed up front of all secondary uses of data and given an opportunity to provide or withhold their consent . In the US, sector-specific legal requirements regulate secondary use of data . When processing needs to take place within the cloud, data cannot be protected by the same means as data at rest and data in transit (e.g. encryption). Data needs to be in readable form in order to be processed. As such, proper data access controls need to be in place to preserve the confidentiality of data being processed externally.

There is ongoing research on the possibility of processing data in encrypted form, which is called *homomorphic* encryption . Homomorphic encryption enables data owners to have their encrypted data processed by another entity, while preventing the processing party to find out what the data is in unencrypted form. This theory is very interesting for the cloud computing paradigm, but the researcher Craig Gentry admits that it may take up to 40 years before the theory becomes practical .

A. Data owner and consumer Authentication

This module involves the authentication of data owner and consumer by carrying out the username and password verification. There are two types logging on cloud server:

1. **New user** In which both data owner and user firstly register their username and password that will be added to database on server side.
2. **Existing user** verify themselves by providing their unique username and password.

B. View, Delete and Upload the Files

After authentication the data owner can view and delete the previously stored files from forensic analyser storage and CSP storage respectively. They can also upload the new files in cloud storage.

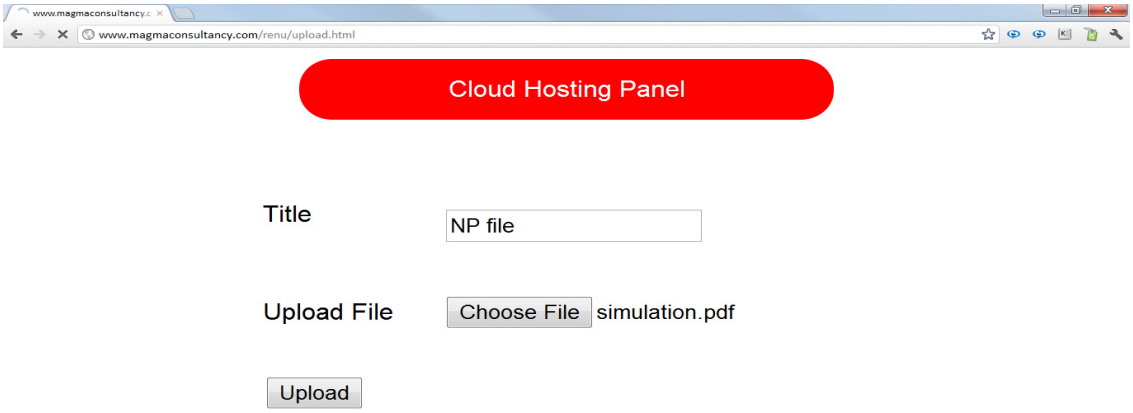
International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

S.no	Encrypted Filename	Actual Filename	Random Key	File Type	File Size	Creation Time	Query Execution Time	Hits
1	BBoSUVxGR0wBEBI=	ptp (2).pdf	tnbqt	application/pdf	992.4423828125kb	05/14/2012 07:46:43 pm	0.0046	0
2	fdp.ypoC -)1(PTNP	PNTP (1) - Copy.pdf	Reversed	application/pdf	806.6318359375kb	05/14/2012 07:48:06 pm	0.0033	0
3	fdp.ypoC -)2(PTNP	PNTP (2) - Copy.pdf	Reversed	application/pdf	992.4423828125kb	05/14/2012 07:48:38 pm	0.0043	0
4	fdp.ypoC -)3(PTNP	PNTP (3) - Copy.pdf	Reversed	application/pdf	497.982421875kb	05/14/2012 07:58:39 pm	0.0027	0
5	Fg4DSkBVU10aDAA=	ptp (3).pdf	fzsjh	application/pdf	497.982421875kb	05/14/2012 08:04:14 pm	0.0029	0
6	ABYfTkRBS0EeCBY=	ptp (1).pdf	pbonl	application/pdf	806.6318359375kb	06/02/2012 09:22:32 pm	0.0038	0

S.no	Encrypted Filename	Actual Filename	Random Key	File Type	File Size	Creation Time	Query Execution Time	Hits	Action
1	BBoSUVxGR0wBEBI=	ptp (2).pdf	tnbqt	application/pdf	992.4423828125kb	05/14/2012 07:46:43 pm	0.0046	0	Delete
2	fdp.ypoC -)1(PTNP	PNTP (1) - Copy.pdf	Reversed	application/pdf	806.6318359375kb	05/14/2012 07:48:06 pm	0.0033	0	Delete
3	fdp.ypoC -)2(PTNP	PNTP (2) - Copy.pdf	Reversed	application/pdf	992.4423828125kb	05/14/2012 07:48:38 pm	0.0043	0	Delete
4	fdp.ypoC -)3(PTNP	PNTP (3) - Copy.pdf	Reversed	application/pdf	497.982421875kb	05/14/2012 07:58:39 pm	0.0027	0	Delete
5	Fg4DSkBVU10aDAA=	ptp (3).pdf	fzsjh	application/pdf	497.982421875kb	05/14/2012 08:04:14 pm	0.0029	0	Delete
6	ABYfTkRBS0EeCBY=	ptp (1).pdf	pbonl	application/pdf	806.6318359375kb	06/02/2012 09:22:32 pm	0.0038	0	Delete

For uploading the files there are three cases:

1. Data owner stores the NP category data directly on Cloud storage without performing encryption on data.

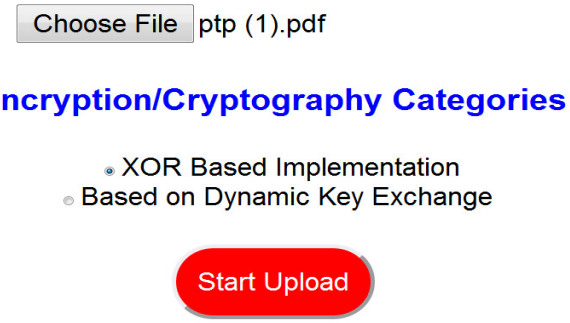


For PTP and PNTP categorised data, data owners firstly choose encryption category i.e. weather to perform XOR based encryption or dynamic key based encryption and then upload the files:

(i) For XOR based encryption, the CSP encrypts the file using XOR based encryption technique [4] and stores it into PTP storage pool.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

(ii) For dynamic key based encryption, the trusted module provides the key to data owner who further encrypts the file and stores it into PNTP storage pool of CSP server.



C. Files downloading

For downloading the files, the customer or user firstly authenticate at CSP and then downloads the files according to their privacy category:

1. **NP categorised file:** The user directly download the original data file from NP storage pool.

1. **PTP categorised file:**The user gets decrypting key for XOR based encrypting files and downloads the encrypted file from PTP storage pool and then decrypt it using XOR based decrypting techniqueFor original file ptp (2).pdf XORED filename is **BBoSUVxGR0wBEBI=** and decrypting key: **tnbqt**

2. **PNTP categorised file:** Here the user firstly gets the dynamic key from trusted module and encrypted PNTP file from PNTP storage pool and then apply the reverse procedure of encryption for getting the original data. The encrypted file name and decrypting keys for PNTP categorised encrypted file i.e. For original file PNTP (2)-copy.pdf the encrypted filename is **fdp.ypoc -)2(PNTP** and random key is **Reversed**

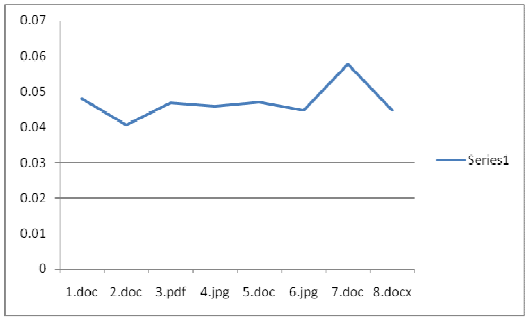
International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-43

S.no	Xored Filename	Actual Filename	Random Key	File Type	File Size	Creation Time	Query Execution Time	Hits	Action
1	BBoSUVxGR0wBEBI=	ptp (2).pdf	tnbqt	application/pdf	992.4423828125kb	05/14/2012 07:46:43 pm	0.0046	0	Download
2	fdp.ypoC -)1(PTNP	PNTP (1) - Copy.pdf	Reversed	application/pdf	806.6318359375kb	05/14/2012 07:48:06 pm	0.0033	0	Download
3	fdp.ypoC -)2(PTNP	PNTP (2) - Copy.pdf	Reversed	application/pdf	992.4423828125kb	05/14/2012 07:48:38 pm	0.0043	0	Download
4	fdp.ypoC -)3(PTNP	PNTP (3) - Copy.pdf	Reversed	application/pdf	497.982421875kb	05/14/2012 07:58:39 pm	0.0027	0	Download
5	Fg4DSkBVU10aDAA=	ptp (3).pdf	fzsjh	application/pdf	497.98242̃1875kb	05/14/2012 08:04:14 pm	0.0029	0	Download
6	ABYfTkRBS0EeCBY=	ptp (1).pdf	pbonl	application/pdf	806.6318359375kb	06/02/2012 09:22:32 pm	0.0038	0	Download

The XOR based cryptography technique (PTP) always has more computational as well as time complexity than dynamic/symmetric key based cryptographic technique used for PNTP because in XOR based cryptography technique as the file size increases the key size also increases and the second reason is that the binary operations performed during XOR based cryptographic technique are always be very time consuming processes.

COMPARISON TABLE - EXECUTION TIME

FileName	Execution Time Proposed Approach (In Microseconds) WITH MD5 AND SHA-1 ON INDIVIDUAL LEVELS
1.doc	0.048059
2.doc	0.040584
3.pdf	0.046836
4.jpg	0.045792
5.doc	0.047025
6.jpg	0.044696
7.doc	0.057807
8.docx	0.044718



In the simulation, it is found that the MD5 and SHA-1 is rapidly used in the cloud infrastructure security.

Future Scope

The cryptographic techniques are essential, but not the only one, method to protect private data against

partially trustworthy cloud server. Therefore, future work of this research might include:

- Multiple Algorithms including RSA, MD5, SHA1 can be included and integrated for better security of the Cloud Platforms.
- The hybrid approach with multiple algorithms can be deployed on the Live Servers for analyzing the performance and integrity.
- The results fetched from MD5 and SHA-1 can be reduced further using the hybrid approach in parallel.

REFERENCES

[1] Aiiad Albeshri and William caelli, "Mutual Protection in cloud computing Environment", 2010 IEEE international conference on high performance computing and communications, IEEE computer society, 978-0-7695-4214-01/10 © 2010 IEEE, pp. 641-647.

[2] Alok Tripathi, Abhinav Mishra, "cloud computing security consideration", 2011 IEEE International Conference on signal processing, communication and computing, 27 October2011, pp. 1-5.

[3] Bernd Grobauer, Tobias Walloschek and Elmer Stoker Siemens, "Understanding cloud computing Vulnerabilities", co-published by IEEE computer and reliability society, 1540-7993/11 © 2011 IEEE, March/April 2011, pp. 50-58

[4] Borko Furth, Flordia Atlantic, "Cloud computing fundamentals", springer Ist edition, 2010, ISBN 978-1-44 19-6523-3.

[5] Brian Hayes. `Cloud computing'. In: Commun. ACM 51.7 (2008), pp. 9-11. issn: 0001-0782. doi: http://doi.acm.org/10.1145/1364782.1364786.

[6] Charlie Kaufman and Ramanathan Venkatapathy, "Windows Azure™ Security Overview", http://www.windowsazure.com/en-us/develop/overview/

[7] Chenguang Wang, Huaizhi Yan, "Study of Cloud Computing Security Based on Private Face Recognition", 2010 International Conference on Computational Intelligence and Software Engineering (CISE), 978-1-4244-5392-4 ©2010 IEEE, pp. 1-5.