ENHANCING TRUST IN CLOUD COMPUTING USING MD5 HASHING ALGORITHM AND RSA ENCRYPTION STANDARD

Mr.KATENDE Nicholas, Dr. CHERUIYOT Wilson, Dr. Ann Muthoni Kibe
Jomo Kenyatta University of Agriculture and Technology, Kenya

Abstract: The clients concern about data security, data integrity, and sharing data with specific band of men and women must be addressed. You can find multiple means of achieving this, example encrypting data on client machine and then storing the information to cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. The auditing capabilities of most existing systems focus on one-way auditability. In cloud computing, providers and users may need to demonstrate mutual trustworthiness, in a bilateral or multilateral fashion. This is a proactive measure that is aimed at improving the reliability of the information system applications operation, for both providers and their customers. The security audit of cloud service providers is an essential aspect of the security considerations for cloud consumers. Audits should be carried out by appropriately skilled staff, either belonging to the consumer or to an independent auditing organization. Security audits should be carried out on the basis of one of the established standards for security controls. Consumers need to check that the sets of controls in place meet their security requirement

Key words: cloud computing, mutual auditability, trust management, security transparency, monitoring, detection RSA, MD5.

1.0 Introduction

The cloud consumers have trust issues ranging from the security of the data and who accesses the data when it’s on the cloud provider’s servers and if there are any modification of that data and this therefore leads to an in-depth analysis

The clients concern about data security, data integrity, and sharing data with specific band of men and women must be addressed. You can find multiple means of achieving this, example encrypting data on client machine and then storing the information to cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore, it becomes more tedious for client to keep this information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised. The aforementioned approaches burdens the client by which makes it additionally accountable for securing its data before storing it to the cloud storage.

The security audit of cloud service providers is an essential aspect of the security considerations for cloud consumers. Audits should be carried out by appropriately skilled staff, either belonging to the consumer or to an independent auditing organization. Security audits should be carried out on the basis of one of the established standards for security controls. Consumers need to check that the sets of controls in place meet their security requirements.

2.1 Literature review

Cloud Deployments Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as depicted in figure 2.0. The Cloud Computing model has three main deployment models which are:

Private cloud

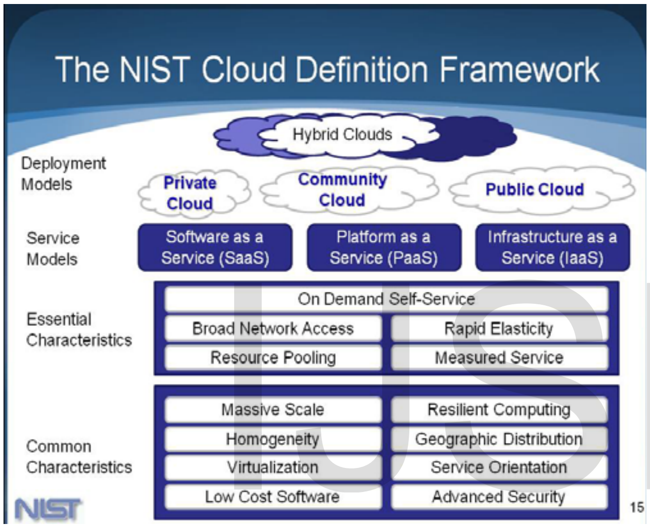
Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud (Kuyoro, Ibikunle and Awodele, 2015).

Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network (Kuyoro, Ibikunle and Awodele, 2015). It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.



The NIST Cloud Definition Framework

FIGURE 1.0: Cloud deployment model (Peter, Timothy, 2015)

Source: csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Cloud Computing Service Delivery Models

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service (Gens, 2009). IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service.

It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers (Kuyoro, Ibikunle and Awodele, 2015). The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore, maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental.

Software as a Service

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the

Internet (Subashini, and Kavitha. 2015). Combining the three types of clouds with the delivery models we get a holistic cloud illustration as seen in Figure 2.0, surrounded by connectivity devices coupled with information security themes. Virtualized physical resources, virtualized infrastructure, as well as virtualized middleware platforms and business applications are being provided and consumed as services in the Cloud.

Cloud vendors and clients' need to maintain Cloud computing security at all interfaces. The next section of the paper introduces challenges faced in the Cloud computing domain.

Cloud computing entities

Cloud providers and consumers are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world. These are discussed as follows

Cloud Providers:

Includes Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media (Internet connections) or infrastructure (hosted data centers) that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centers hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers (Kresimir and Zeljko, 2015).

Cloud Service Brokers:

Includes technology consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.

Cloud Resellers:

Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as "resellers" for their Cloud-based products in a particular region. Cloud Consumers: End users belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller. In the next section, key benefits of and possible threats and risks for Cloud Computing are listed (Grobauer, Walloschek and Stöcker, 2015).

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth (Peter and Timothy, 2015).

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

2.2 Architectural design and method for enforcing mutual auditability and security transparency

Because security transparency and mutual auditability imply the possibility for the cloud service consumer (CSC) or its auditors to probe the security of the cloud service provider (CSP). The area of event computing Moussa et al (2015) offers some potential that could be exploited in that context. In fact, events provide a powerful construct to capture current state of a system (service) and deviations from expectation and to predict future security or quality of service (QoS) related issues.

Additionally, a well-defined architecture can support event based monitoring in ensuring the prompt dissemination of events' occurrence to the interested parties who would subsequently make judgment on the course of action to adopt. Amongst others, it may be a way to hold cloud providers accountable for a security breach that may have stemmed from a weakness in their security; a breach of service level agreement (SLA) or other escrows between the two parties. The set of patterns and the detection algorithms associated could also constitute a powerful tool for a cloud provider concerned with abusive and nefarious use of its service by clients. Efficiently leveraging the power of events for the purpose of Security Transparency and Mutual Audit (STMA) in the cloud will entail further investigation in mainly three areas as depicted in Figure:

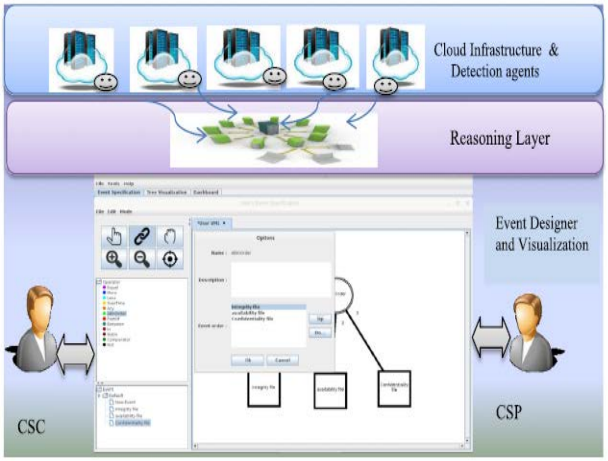

Cloud Infrastructure & Detection agents
Reasoning Layer
Event Designer and Visualization
CSC
CSP

Figure. 2 High level Architecture for STMA enforcement

Source: Journal of Cloud Computing 2015: Advances, Systems and Applications

2.3 Keyless Signature Infrastructure (KSI)

This a technology developed by Guardtime that generates digital signatures for electronic data on a massive scale but uses only cryptographic hash functions, meaning there are no keys to be compromised or trusted humans in sight.KSI uses only hash-function cryptography, allowing verification to rely only on the security of hash-functions and the availability of a public ledger commonly referred to as a blockchain. A blockchain is a distributed public ledger; a database of transactions such that there is a set of pre-defined rules as to how the ledger gets appended, achieved by distributed consensus of participants in the system.The KSI blockchain overcomes two major weaknesses of traditional blockchains, making it usable at industrial scale(Guardtime, 2015).

Scalability: One of the most significant challenges with traditional blockchain approaches is scalability – they scale at O(n) complexity i.e. they grow linearly with the number of transactions. In contrast the KSI blockchain scales at O(t) complexity – it grows linearly with time and independently from the number of transactions.

Settlement time: In contrast to the widely distributed crypto-currency approach, the number of participants in KSI blockchain distributed consensus protocol is limited. By limiting the number of participants it becomes possible to achieve consensus synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second.

2.4 Trusting a Third Party

Technically in Cloud Computing environment, trust among the user of the cloud service, the provider of the cloud service and third parties who provide or receive service from either user or provider is very crucial. Provider with good reputation and unquestionable service would be most trustworthy. Trust in cloud computing is more complex than in a traditional IT scenario where the information owner owns his own computers (Monoj. and Smriti, 2015). Most of the infamous Cloud products provide some basic security, privacy, and trust mechanism, which often cannot be customized. Security, privacy and trust are related in the context of computing. For strong Cloud privacy and security are prerequisite and trust can be built on the top only when consumer's data will remain private and secure.

Trust can be seen as an outcome of betterment of security or privacy objectives.

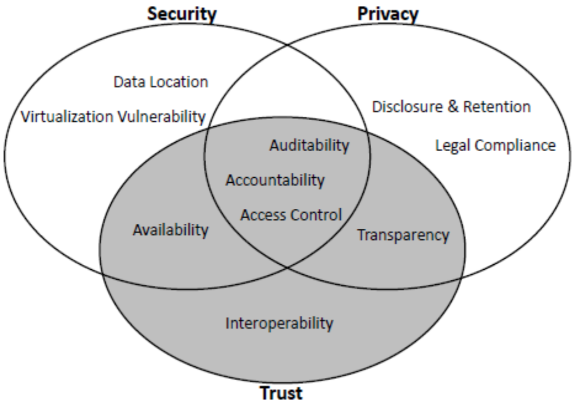


Figure. 3. Correlation among Security, Privacy and Trust

Source: (Monoj. and Smriti, 2015) A Survey on Web Services and Trust in Cloud Computing Environment

The trust circle incorporates some common issues of both security and privacy. Tackling issues of security and privacy like auditability, accountability, access control, availability, transparency etc., can lead to building of trustworthy Cloud.

Trusting a Third Party, which assures security characteristics while realizing trust. Using a Trusted Third Party (TTP) within a cloud environment by enabling trust and using cryptography ensures the confidentiality, integrity and authenticity of data and communications. Cryptographic protocols such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) using both symmetric and asymmetric cryptography are believed to be necessary to provide secure transmission of data between the service provider and client. In cryptography, a Trusted Third Party is an entity which facilitates secure interactions between two parties who both trust this third party. TTPs are operationally connected through chains of trust (usually called certificate paths) in order to provide a web of trust forming the notion of a Public Key Infrastructure (PKI). For service provider trust, it is the responsibility of service provider to publish the platform configurations and provide attestation signatures so that configuration can be verified(Monoj. and Smriti, 2015).

2.5 Existing Algorithms for Security

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using “the key” and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption. Fig 2.2 shows some of the symmetric & asymmetric algorithms (Abdul et al. 2009).

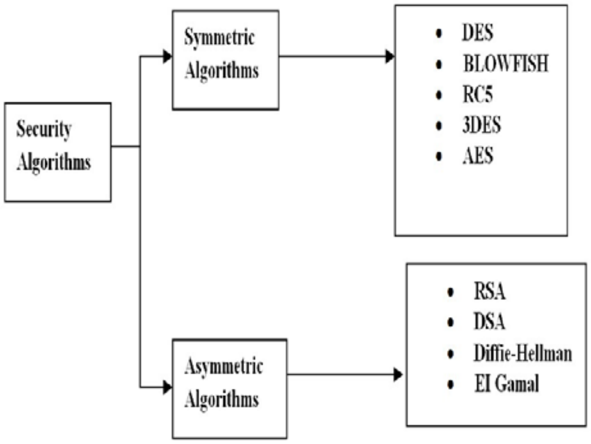


Figure 4: Security Algorithms

Symmetric Algorithms:

The Data Encryption Standard (DES) Neha J and Gurpreet K, (2012) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56-bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds (Devi , M. and Pramod K,2012). Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm as shown in figure 2.3.

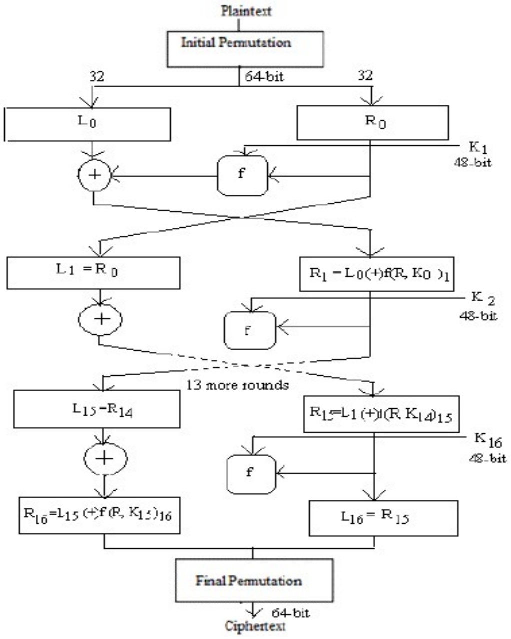


Figure. 5. Encryption with DES

DES performs an initial permutation on the entire 64-bit block of data. It is then split into two, 32 bit sub-blocks, L_0 and R_0 which are then passed into what is known as Feistel rounds (Devi, M. and Pramod K,2012). Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. At the end of the 16th round, the 32 bit L_{15} and R_{15} output quantities are swapped to create what is known as the pre-output. This [R_{15}, L_{15}] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64-bit cipher text.

The function f is made up of four sections:

- Expansion P-box
- A whitener (that adds key)

A group of S-boxes and A Straight P-box.

BLOWFISH: This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption (Gurpreet S and Supriya K 2013).

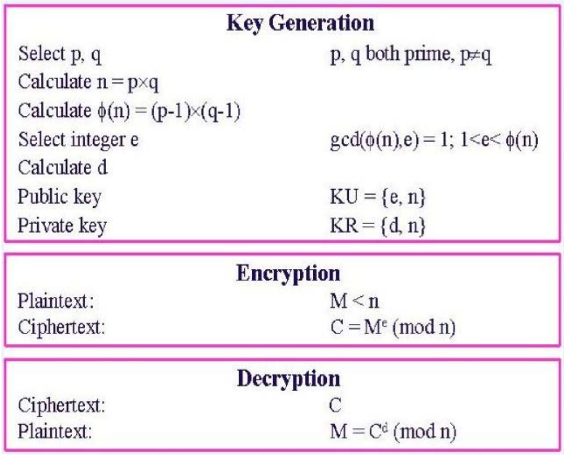
RC5: It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow (Uma S, 2010)

3DES: This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods.This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics(Gurpreet S and Supriya K 2013).

AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters' combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications (Uma S, 2010).

Asymmetric Algorithms:

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The process is shown in figure 2.4.



Key Generation

Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure. 6. RSA Algorithm

RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at encryption

$C = M^e \bmod n$

And at decryption side

$M = C^d \bmod n.$

Where n is a very large number, created during key generation process.

Rashmi N et.al (2013), uses DES algorithm and RSA algorithm for providing security to cloud storage.

DSA:The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013. With DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA (Uma S, 2010).

Diffie-Hellman Key Exchange (D-H): Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

EI Gamel: In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1984. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. ElGamal encryption can be defined over any cyclic group G. Its security depends upon the difficulty of a certain problem in G related to computing discrete logarithms

2.6 Improving Data Security in Cloud Computing Using MD5 Algorithm

MD5 (Message Digest 5)

MD5 is a message digest algorithm developed by Ron Rivest. MD5 is quite fast and produces 128-bit message digests. After some initial processing, the input text is processed in 512-bit blocks (which are further divided into 16 32-bit blocks). The output of the algorithm is a set of four 32-bit blocks which make up the 128-bit message digest (Priyanka and Vivek 2014). It contains various steps which includes Padding, append length, Divide the input into 512-bit blocks, initialize chaining variables, and Process blocks.

One MD5 operation

- A process P is first performed on b, c and d. This process is different in all the four rounds.
- The variable a is added to the output of the process P (i.e. to the register abcd).
- The message sub-block M[i] is added to the output of step2(i.e. to the register abcd).
- The constant t[k] is added to the output of step 3 (i.e. to the register abcd).
- The output of step 4 (i.e. the contents of register abcd) is circular-left shifted by s bits.(The value of s keep changing)
- The variable b is added to the output of step 5 (i.e. to the register abcd).
- The output of step 6 becomes the new abcd for the next step (Priyanka and Vivek 2014).

All the above steps are shown in the following figure 3 i.e. it shows the process of one MD5 operation. As it contains the process P, variables a, b, c, d, message sub-block M[i], constant t[k] for the operation of MD5 algorithm.

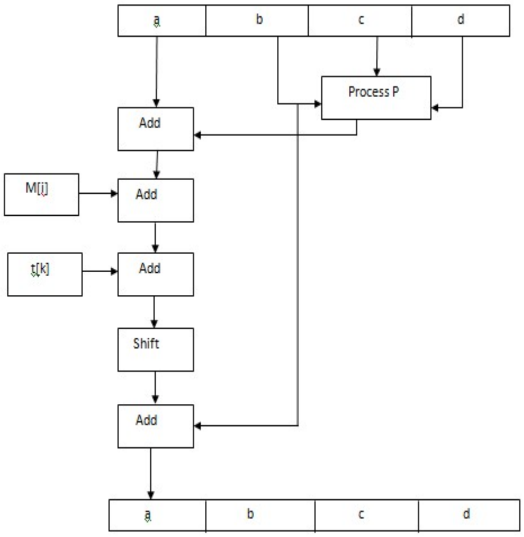


Figure 7: One MD5 operation

Source: Shreya and Neeraj, 2015

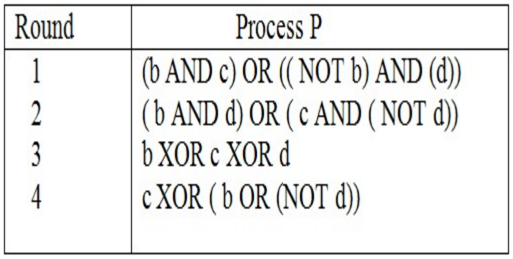
We can mathematically express a single MD5 operation as follows:

a = b + ((a + Process P (b, c, d) + M[i] + t[k]) <<< s) where

<<< s = Circular left shift by s bits

Understanding the process P

As we can see, the most crucial aspect here is to understand the process P, as it is different in the four rounds. In simple terms process P is nothing but some Boolean operations on b, c and d as shown in the following table (Priyanka and Vivek 2014).



Round	Process P
1	(b AND c) OR ((NOT b) AND (d))
2	(b AND d) OR (c AND (NOT d))
3	b XOR c XOR d
4	c XOR (b OR (NOT d))

Table 1.0: Process P in each round

Secure Hash Algorithm (SHA)

The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993; a revised version was issued as FIPS 180-1 in 1995 and is generally referred to as SHA-1. The actual standards document is entitled Secure Hash Standard. SHA is based on the hash function MD4 and its design closely models MD4. SHA-1 is also specified in RFC 3174, which essentially duplicates the material in FIPS 180-1, but adds a C code implementation (William 2010).

Steps in SHA Algorithm:

Step 1: Append padding bits.

The message is padded so that its length is congruent to 896 modulo 1024 [length 896(mod 1024)]. Padding is always added, even if the message is already of the desired length. Thus, the number of padding bitsis in the range of 1 to 1024. The padding consists of a single 1-bit followed by the necessary number of 0-bits.

Step 2: Append padded length:

A block of 128 bits is appended to the message. This block is treated as an unsigned 128-bit integer (most significant byte first) and contains the length of the original message (before the padding) (Fadi, Syed, and Wassim. 2009)

Step 3: Initialize hash buffer:

A 512-bit buffer is used to hold intermediate and final results of the hash function. The buffercan be represented as eight 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialized to the following 64-bit integers.

a = 6A09E667F3BCC908

b = BB67AE8584CAA73B

c = 3C6EF372FE94F82B

d = A54FF53A5F1D36F1

e = 510E527FADE682D1

f = 9B05688C2B3E6C1F

g = 1F83D9ABFB41BD6B

h = 5BE0CDI9137E2179

Step 4: Process blocks:

The heart of the algorithm is a module that consists of 80 rounds.

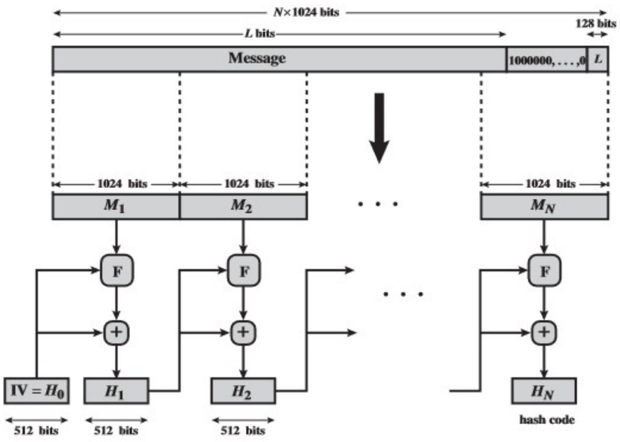


Figure 8 SHA producing Message Digest

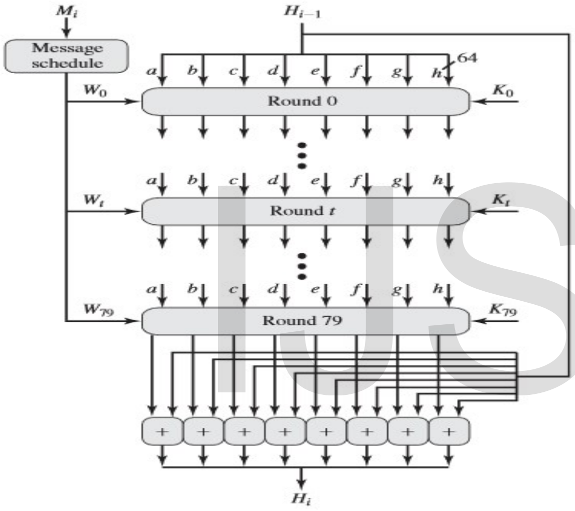


Figure 9 Processing of Single Block

Adopted from Neelima et al 2016, Enhancement of Data Security in Cloud Computing by Generating OTP

Step 5: Output

After all *N* 1024-bit blocks have been processed, the output from the *N*th stage is the 512-bit message digest.

We can summarize the behaviour of SHA-512 as follows.

*H*0 = IV

Hi = SUM64 (*Hi*-1, abcdefgh*i*) *MD* = *HN* where

IV = initial value of the abcdefgh buffer, defined in step 3 abcdefgh*i*= the output of the last round of processing of the *i*th message block

N = the number of blocks in the message (including

padding and length fields)

SUM64 = Addition modulo 2^64 performed separately oneach word of the pair of inputs

MD = final message digest value (William 2010).

Operation:

The algorithm can be described in 3 steps:

Step 1: Generate the SHA-1 value Let digest = SHA-

1(Key, M) digest is a 20-byte string

Step 2: Generate a hex code of the digest. Hex digest=ToDec (digest)

Step 3: Extract the 6-digit OTP value from the string

OTP = subString (digest)

The substring function in Step 3 does the dynamic truncation and reduces the OTP to 6-digit

Here we are going to generate a hash value by massing the message and key as the parameters to the hash function.

Later the hash value obtained is converted to the decimal format from the hexadecimal form.

Later by using the substring function we are to choose our OTP length i.e., 4 digits or 6 digits etc. (Lin, Shen, and Hwang, 2003).

2.7 The summary and The research gaps

Following the literature review, it can be noted that most systems were designed using one or two methods of encryption and hashing and has been used as a measure of the integrity of data by the cloud consumer. This therefore means that the security audits are carried out on one side either on the side of the cloud consumer or the cloud provider. This also means that there is no mutual auditability agreed upon by both parties in the cloud.

This research is going to be carried out to design a model that can keep track the security at both the consumer and the provider of the cloud using MD5 hashing algorithm andRSA encryption standard. This will help to maintain the security of the data and integrity at all time since you will be notified in case of any change in the MD5 hash value due to modifications.

3.0 Conceptual Model

As shown in Figure 1.0 is an overview of the architecture where storage and encryption/decryption/hash services (security services) are separated. For example, a small or medium scale business who wish to store all its account related data in cloud storage, will first calculate the hash of the data, encrypt the data using encryption service and then store the data in storage provided by separate provider.

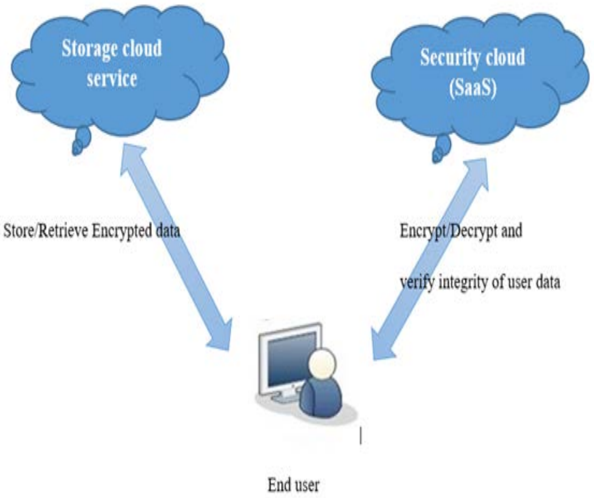

Storage cloud service
Security cloud (SaaS)
Store/Retrieve Encrypted data
Encrypt/Decrypt and verify integrity of user data
End user

Figure 1.0 Conceptual Model for security audit.

The system also provides functionality where other users from small scale business Company will be able to access data which is stored in cloud storage. The sessions between client and security server is secured using RSA as the encryption algorithm. MD5 is used for calculating the hash of the data, and RSA is used as an encryption/decryption algorithm for computing cipher at security server end.

References

Abdul D. S. Elminaam, Abdul Kader H. M. and Hadhoud M. M. (2009),“ Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA Volume 8, 2009.

Balachandra R. K., Ramakrishna P. V. and Rakshit A.. “Cloud Security Issues.” In PROC ‘09 IEEE International Conference on Services Computing, 2015, pp 517-520.

Beynon-Davies D. (2013). *Business Information Systems*. Basingstoke UK, Palgrave Macmillan

Broad, J. (2013). *Risk Management Framework: A Lab-Based Approach to Securing Information Systems*. Newness. Elsevier Science

Brodkin J.. (2015, September.). “Gartner: Seven cloud-computing security risks.” *Infoworld*, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1> [September. 5, 2015].

Carlos C. (June 2013). The Four Keys of Cloud Security: Mutual Auditability

Chen Y, Paxson V, Katz RH (2010). What’s New About Cloud Computing Security? Report EECS Department, University of California, Berkeley. Accessed june 13, 2016 from http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version September. 5, 2015.

Cloud Security Alliance (2015), CSA STAR: The Future of Cloud Trust and Assurance, Available: https://cloudsecurityalliance.org/star/, accessed (September 9, 2015)

Davendranath G. H. (2013). *Computer concepts and management information systems*. Patparganj, New Delhi. PHI Learning Pvt. Ltd

Devi G., Pramod Kumar, (2012) “Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm” International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596,2012.

Diana.s, (April 25 2016). Cloud security frame work audit methods. Retrieved https://www.sans.org/reading-room/whitepapers/cloud/cloud-security-framework-audit-methods-36922

ENISA. (September, 2015) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk- assessment [September. 5, 2015].

FadiAloul, Syed Zahidi, Wassim El-Hajj. 2009. Two Factor Authentication UsingMobilePhones. Digital Library Telkom Institute of Technology (IEEE).

Federal Information Processing Standard (FIPS) (april,2009)140-2, Security Requirements for Cryptographic Modules.

Grobauer B, Walloschek T and Stöcker E, 2015 "Understanding Cloud Computing

Gens F. (Feb, 2009). “New IDC IT Cloud Services Survey: Top Benefits and Challenges”, *IDC eXchange*, Available: <http://blogs.idc.com/ie/?p=730> [September. 5, 2015].

Grace T. R. Lin, Chih-Chieh Lin, C. James Chou, and Yen-Chun Lee (*December* 2014), Fuzzy Modeling for Information Security Management Issues in Cloud Computing

Guardtime. (2015) KSI Technology, Available: https://guardtime.com/ksi-technology accessed (September 9, 2015)

Gurjeevan Singh, , Ashwani Singla and K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011

Gurpreet Singh, Supriya Kinger (2013)"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

http://istqbexamcertification.com

http://m.globallegalpost.com/corporate-counsel/shadow-it-the-loomingcybersecurity-

Kanchana,M, Nazar Hussain, sk, kumar, Praveen.c, (2013). Preserving Audit of secure data storage services in cloud computing.

Kashish Goyal, Supriya Kinger" Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.

Kresimir P. and Zeljko H. (2015)"Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized