ISBN: 978-1-948012-16-4

Contemporary Issues in Computing (CIC)

DOI: <http://doi.org/10.26480/cic.01.2020.25.32>

CrossMark

DESIGN AND IMPLEMENTATION TECHNIQUE FOR CLOUD COMPUTING SECURITY IMPROVEMENT

Shipra Yadav^a, Keshao D. Kalaskar^b and Pankaj Dhumane^c^aResearch Scholar, IICC, RTM Nagpur University Nagpur, (MH), India^bAssociate Professor, Dr. Ambedkar College, Chandrapur, (MH), India^cAssistant Professor, Sardar Patel College, Chandrapur, (MH), India*Corresponding Author e-mail: pdhumane@rediffmail.com

This is an open access article distributed under the Creative Commons Attribution License CC BY 4.0, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ARTICLE DETAILS

Article History:

Received 26 October 2020

Accepted 27 November 2020

Available online 03 December 2020

ABSTRACT

Cloud computing focuses on new challenging security threats important in service quality. The most challenging cloud computer security must therefore be solved by a data security model. Without influencing functionality, performance and Sales force, Chatter, Gmail, and Amazon Web Services. Default Gateway System dynamically encrypts confidential data in real time and does not break down the cloud program. They were not affected. If an unauthorized person collects cloud storage data, only the encrypted data can be seen. If authorized individuals access their cloud successfully, the data will be decrypted in real time for your use. A solid and quick encryption calculation, record uprightness, malware, the firewall, and tokenization thus substantially more are required in the default Gateway Platform. This paper was worried about validation, more grounded and quicker encryption and honesty of the document.

KEYWORDS

Cloud-based computing, cloud-based data security model, random testing, cloud cryptography, OTP (a password for one time).

1. INTRODUCTION

Amazon Elastic Computing Cloud (EC2), published in 2006, fired the world at the cloud computing. After this, several technology corporations have developed a cloud computing infrastructure. Dells released its cloud computing solution in 2007 while simultaneously discovering the IBM BlueCloud, the Google Map and the Windows Azure of Microsoft. Numerous assessments show that the distributed computing industry is relied upon to arrive at a phenomenal \$420 billion by 2012. This shows the emergence of cloud computing as an alternative technology that is practical and viable. The development of the cloud system has simplified the implementation by the business companies of large-scale distributed systems. This system allows business enterprises to focus more on functionality and business issues than the underlying framework and implementation features, providing a simple, single interface between software provider providers and the business enterprises that use the service. Software as a service system, transaction processing and Multitenant databases are included in the cloud applications. In response to customers' requests for resource booking and in accordance with customers' quality of service, the Cloud system dynamically assigns computational resources to the user. Risks emerge, and the data security issue becomes a cloud computing bottleneck.

The apparent advantage of the Cloud number of data or computing resources stored and maintained locally. It drastically reduces an organization's initial investment and introduces a pay-as-you-go platform. In practice, cloud computing is not widely adopted because of security and protection worries, regardless of these prominent favorable

circumstances. Also, other conventional IT security issues, for example, respectability, classification, accessibility, dependability, non-denial, proficient recuperation, information sharing, and so on in distributed computing, have a similar essentialness. Information stockpiling precision is one of the key security issues for Cloud (Information Security Briefing Cloud Computing, 2010).

Different methods are used to store the data correctly. Most researchers favour trustworthy third parties like cryptographic co-processors (Foster et al., 2008). It adds additional costs for additional hardware on the part of Cloud users. Another uses open source code as the software application to incorporate the cryptographic co-processor's functionality. With some concession on performance level, it can be proved as a cost-effective solution.

Distributed computing is a characteristic advancement of the far reaching reception of virtualization, administration arranged design, autonomic and utility registering (NIST, 2011). Subtleties are disconnected from end-clients, who never again have a requirement for skill in, or command over, the innovation foundation "in the cloud" that underpins them as shown in Fig. 1.

Figure 1: Evolution of Cloud Computing

Quick Response Code	This paper was presented at	Access this article online	
	International Conference on Contemporary Issues in Computing (ICIC-2020) - Virtual IETE Sector V, Salt Lake, Kolkata From 25th-26th July 2020	Website: www.intelcomp-design.com	DOI: 10.26480/cic.01.2020.25.32

Distributed computing frequently use gigantic scale, homogeneity, virtualization, flexible processing (no quit registering), ease/free programming, geographic dissemination, administration direction programming and propelled security advances (Rittinghouse et al., 2009). The principle target of this paper is to improve information security model for distributed computing. The proposed information security model takes care of cloud client security issues, help cloud provider to select the most suitable encryption algorithm to its cloud. We also help user cloud to select the highest security encryption algorithm. The paper is composed as follows: in Section 2 distributed computing design is characterized; Cloud processing security is talked about in Section 3; in Section 4 system is portrayed lastly in Section 5 interferences of the outcomes are depicted.

2. LITERATURE REVIEW

The proposed information security model is made out of three-stage guard framework structure, in which each floor plays out its own obligation to guarantee the information security of cloud. The principal stage is liable for solid verification. It applies the OTP (once secret phrase) as a two-factor authentication system. OTP provides high security because it used one password in a session and cannot be cracked. The second phase selects the stronger and a faster encryption algorithm by proposing algorithm called "Evaluation algorithm". This algorithm used for selected eight present day encryption systems to be specific: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish. The assessment has performed for those encryption calculations as indicated by arbitrariness testing by utilizing NIST factual testing. This assessment utilizes PRNG (pseudo arbitrary number generator) to decide the most appropriate. This assessment calculation performed at Amazon EC2 Micro Instance distributed computing condition. In addition, this phase checks the integrity of user data. It encourages cloud users to encrypt his data by using "TrueCrypt" software or proposed software called "CloudCrypt V.10". The third phase, ensure fast recovery of user data.

2.1 Cloud Computing Service Models

As per NIST, the cloud model is made out of three help models:

Programming as a Service (SaaS): The applications are open from different customer gadgets through a slight customer interface, for example, an internet browser (e.g., electronic email).

Stage as a Service (PaaS): Applications made utilizing programming dialects, libraries, administrations, and apparatuses bolstered by the supplier.

Framework as a Service (IaaS): The buyer can convey and run self-assertive programming, which can incorporate working frameworks and applications.

2.2 Cloud Computing Deployment Models

Private cloud: The cloud foundation is provisioned for selective use by a solitary association involving numerous customers (e.g., specialty units).

Network cloud: It might be claimed, overseen, and worked by at least one of the associations in the network, an outsider, or a mix of them, and it might exist on or off premises.(e.g Policy and Compliance)

Open cloud: The cloud foundation is provisioned for open use by the overall population

Half and half cloud: The cloud framework is an organization of at least two unmistakable cloud foundations (private, network, or open)

2.3 Cloud Computing Sub-services Models

IaaS: DBaaS (database-as-an administration): DBaaS permits the entrance and utilization of a database the board framework as an assistance.

PaaS: STaaS (stockpiling as-an administration): STaaS includes the conveyance of information stockpiling as a help, including database-like administrations, frequently charged on an utility registering premise, e.g., per gigabyte every month.

SaaS: CaaS (correspondences as-an administration): CaaS is the conveyance of an endeavor interchanges arrangement, for example, Voice over IP, texting, and video conferencing applications as an assistance.

SaaS: SECaaS (security-as-an administration): SECaaS is the security of business systems and portable systems through the Internet for occasions, database, application, exchange, and framework episodes.

SaaS: MaaS (checking as-an administration): MaaS alludes to the conveyance of second-level framework segments, for example, log the executives and resource following, as a help.

PaaS: DTaaS (desktop-as-a-service): DTaaS is the decoupling of a user's physical machine from the desktop and software he or she uses to work.

IaaS: CCaaS (compute capacity-as-a-service): CCaaS is the provision of "raw" computing resource, typically used in the execution of mathematically complex models from either a single "supercomputer" resource or a large number of distributed computing resources where the task performs well (Security Guidance for Critical Areas of Focus in Cloud Computing, 2009).

2.4 Cloud Computing Benefits

Lower computer costs, improved performance, diminished programming costs, moment programming refreshes, improved record design similarity, boundless capacity limit, gadget freedom, and expanded information dependability

2.5 Cloud Computing Drawbacks

Requires a constant Internet connection, does not work well with low-speed connections, can be slow, features might be limited, stored data might not be secure, and stored data can be lost.

2.6 Cloud Computing Providers

AWS (amazon web services)—include Amazon S3, Amazon EC2, Amazon Simple-DB, Amazon SQS, Amazon FPS, and others. Salesforce.com—Delivers businesses over the internet using the software as a service model. Google Apps—Software-as-a-service for business email, information sharing and security. And others providers such as Microsoft Azure Services Platform, Proof-point, Sun Open Cloud Platform, Workday, etc.

3. DATA SECURITY PROBLEM OF CLOUD COMPUTING

With cloud computing, all your data is stored on the cloud. So, cloud users ask some questions like: How secure is the cloud? Can unauthorized users gain access to your confidential data? Cloud computing companies say that data is secure, but it is too early to be completely sure of that. Only time will tell if your data is secure in the cloud. Cloud security concerns arising which both customer data and program are residing in provider premises. Security is always a major concern in Open System Architectures as shown in Fig. 2.

While cost and convenience are two extraordinary advantages of distributed computing, there are huge security worries that should be tended to when thinking about moving basic applications and touchy information to open and shared cloud conditions. To address these worries, the cloud supplier must create adequate controls to give the equivalent or a more prominent degree of security than the association would have if the cloud were not utilized.

There are three kinds of information in distributed computing. The main kind is an information in travel (transmission information), the second information very still (stockpiling information), lastly information in preparing (handling information). Mists are hugely unpredictable frameworks can be decreased to straightforward natives that are reproduced a large number of times and normal utilitarian units. These complexities make numerous issues identified with security just as all parts of Cloud processing. So, users always worry about its data and ask where the data is? And who has access? Every cloud provider encrypts the data in three types according to Table 1.

Figure 2: Security is a major concern to cloud computing

Table 1 Data security (encryption) in cloud computing.

Storage	Processing	Transmission
Symmetric encryption	Homomorphic encryption	Secret socket layer SSL encryption
AES-DES-3DES-Blowfish-MARS	Unpadded RSA-EIGamal	SSL 1.0-SSL 3.0-SSL 3.1-SSL 3.2

4. METHODOLOGY

This area depicts a proposed information security model in distributed computing. Likewise, centers around improving security by using an OTP authentication system, check data integrity by using hashing algorithms, encrypt data automatically with the highest strong/ fast encryption algorithm and finally ensure the fast recovery of data.

4.1 The Existence of Super-user

Most cloud computing providers (Vouk, 2008; Security Guidance for Critical Areas of Focus in Cloud Computing, 2009) in first, authenticates (e.g., Transfer usernames and password) via secure connections and secondly, transfer (e.g., via HTTPS) data securely to/from their servers (so-called "data in transit"), but, as far as I can tell, none finally, encrypts stored data (so-called "data at rest") automatically.

This section describes a proposed data security model in cloud computing. In addition, focuses on enhancing security by using an OTP authentication system, check data integrity by using hashing algorithms, encrypt data automatically with the highest strong/ fast encryption algorithm and finally ensure the fast recovery of data. In cloud computing, to ensure correctness of user data, in first, user must be make authentication. Authentication is the process of validating or confirming that access credentials provided by a user (for instance, a user ID and password) are valid. A client right now be an individual, another application, or a help; all ought to be required to confirm. Numerous undertaking applications necessitate that clients validate previously permitting access. The approval, the way toward allowing access to mentioned assets, is futile without reasonable validation. At the point when associations start to use applications in the cloud, verifying clients in a reliable and sensible way turns into an extra test. Associations must address validation related difficulties, for example, qualification the board, solid verification, designated confirmation, and trust over a wide range of cloud conveyance models (SPI). Two-factor confirmation became answer for any cloud application.

After authentication, cloud user can access data that stored on servers at a remote location and can access it from any device/ anywhere.

So, in the event that you need your information to be secure in the cloud, at that point consider scrambling the put away information. Furthermore, don't store your encryption keys on a similar server. It is unclear whether a cloud computing provider could be compelled by law enforcement agencies to decrypt data that (1) it has encrypted or that (2) users have encrypted, but if the provider has the keys, decryption is at least possible.

4.2 Problem in Existing Data Security Model

The cloud users ask your cloud providers about some problems:

- Are files stored on cloud servers encrypted automatically?
- Can other users boot my machine?
- Have unauthorized users of my machine detected?
- Is my data accessed solely by my virtual machine?
- Is the system should own my key?
- Is my data retrieving fast?

be kept not in cloud system; most of these problems appear in previous data security model (Dai et al., 2009). Clouds typically have a single security architecture. This section provides a detailed overview of the existing data security model, as well as explains the data security model for Amazon web services as shown in Table 2.

Encryption algorithms: AES, Serpent, and Twofish.

Finally, mode of operation is XTS.

TrueCrypt is a computer software program whose primary purposes are to: Secure data by encrypting it before it is written to a disk. Decrypt encrypted data after it is read from the disk. However, TrueCrypt uses only three methods (AES, Serpent and Twofish) to encrypt data as shown in Fig. 3.

Encryption algorithms: AES, Serpent, and Twofish.

Finally, mode of operation is XTS.

TrueCrypt is a computer software program whose primary purposes are to: Secure data by encrypting it before it is written to a disk. Decrypt encrypted data after it is read from the disk. However, TrueCrypt uses only three methods (AES, Serpent and Twofish) to encrypt data as shown in Fig. 3.

Figure 3: TrueCrypt encryption options

Table 2: Data security model in Amazon EC2

Data for processing	Homomorphic encryption algorithm, e.g., RSA.
Data in transit	Secure Sockets Layer, e.g., HTTPS
Data at rest	Depend on the OS used. In windows EFS are used. It is not full encryption. It encrypts individual files. If you need a full encrypted volume, consider using the open-source TrueCrypt product. Linux uses AES, it encrypts individual files. OpenSolaris can take advantage of ZFS Encryption
Key management	The key kept in the cloud as a list but it makes key rotation
Authentication	Two factor authentication (e-mail and password) (account of AWS AMI) X.509 certificates for authentication
User protection	AWS encourages users to encrypt their sensitive data before it upload into Amazon S3.

4.3 Proposed Data at Rest Security Model

The proposed data security model utilized three-level guard framework structure, in which each floor plays out its own obligation to guarantee that the information security of cloud as shown in Fig. 4. The first phase: strong authentication is achieved by using OTP.

The second phase: data are encrypted automatically by using strong/fast encryption algorithm. In addition to encrypt data, users can encrypt his sensitive data by using TrueCrypt software or proposed software CloudCrypt V.10. CloudCrypt software uses eight modern/strong encryption algorithms. Finally, data integrity is achieved by using hashing algorithms.

The third phase: fast recovery of user data is achieved in this phase. The three phases are implemented in default gateway, as shown in Fig. 5. The proposed information security model gives a solitary default entryway as a stage to verify delicate client information over numerous open and private cloud applications, including Salesforce, Gmail, and Amazon Web Services, without affecting functionality or performance.

Default gateway platform tasks:

Encrypt sensitive data automatically on a real time before sending to the cloud without breaking cloud application;

The default gateway platform did not effect on user functionality and visibility;

If an unauthorized person gets data from cloud storage, he can see the encrypted data;

The default gateway platform must contain Strong/Fast Encryption Algorithm by using one or more of encryption calculations specifically RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish (Burwick et al., 1999; Dawson et al., 2002; Stallings, 2005; Coppersmith, 1994; Daemen et al., 2001; Schneier, 2008; Schneier et al., 1998).

If authorized person access success in his cloud, the data is decrypted in real time for your use;

Figure 4: Proposed data security model in cloud computing

Figure 5: How the cloud data are saved with the data security model proposed

4.4 Implementation Details

4.4.1 First Phase, Authentication

- The cloud client select organization, at that point make a record;
- Cloud supplier transfer client data in DB in distributed storage;
- Cloud Provider affirms client with his username and secret key;
- Cloud client demand login page;
- The cloud supplier shows login screen; Cloud client login with username and secret key;

A cloud supplier check is substantial username and secret key via looking in DB in distributed storage. In the event that client data not substantial showcase mistake message else show save a PC page; Cloud user reserves your PC.

4.4.2 OTP Authentication Steps

Cloud user enters passphrase, challenge and sequence number for OTP authentication;

Cloud user generates an OTP;

The cloud provider generates the OTP temporary DB based on user information;

Cloud user login with OTP;

A cloud supplier check is legitimate OTP via scanning in brief DB for OTP in distributed storage. In the event that OTP not substantial presentation blunder message else display user PC page.

4.5 Proposed Evaluation Algorithm

We use NIST factual tests to get the most noteworthy security encryption calculation from eight calculations in particular RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish as shown in Fig. 6.

Figure 6: Steps to select the highest encryption algorithm

NIST Designed to test the arbitrariness of the parallel groupings produced by arbitrary or pseudorandom number generators dependent on programming or programming.

NIST statistical tests include 16 tests, i.e.: the (Mone-bit) measure frequency, and in-fig frequency test. 6 Steps to select a maximum algorithm for encryption.

Node, The Runs testing, Longest-running Model Matching tests in one node,

The Binary Matrix Rank test, Discrete Fourier Transform test (Spectral) Test, Maurer's 'U'.

We also equate eight encryption algorithms based on encryption speeds in order to recover more easily.

As case trial for our software, we use Amazon EC2. Download and sign your picture on S3. Web Service boots your file. Enable the image's preferred ports. Link via SSH to your image. And finally execute your request.

We have used Micro Instances of this Amazon EC2 family for our cloud trial, have constant small amounts of CPU power, are suitable for lower throughput, 613 MB capacity, up to two EC2 processing units, EBS (elastic block volume) storage from 1 GB to 1 TB, the 64-bit architecture, low I/O performance, t1.micro API name, We use Ubuntu Linux to run NIST Statistical test package (Soto, 1999; Buyya et al., 2009; Rukhin et al., 2010).

4.6 Selection the Highest Encryption Algorithm Steps

Sign up for a web service of Amazon to create a account, select the highest cryptographic algorithm steps. Windows (64 bit) Amazon EC2 Micro instance lunch. Connect to Windows Micro Instance of Amazon EC2 (Amazon EC2 API, 2006; Amazon Web Services, 2006; Amazon Web Services, 2009). Generate a 128 flat stream sequences with an PRNG length and main stream (128 bits in length) of 7,929,856 bits per line. To get text from the ciphers use cryptographic algorithms. Amazon EC2 Ubuntu LinuxConnect toAmazon EC2 Ubuntu Linux Micro instance Execute NIST statistical testing for each sequence to eight cryptographic algorithms, compare P-value at 0,01, and then reject the sequence if P-value below 0,01.

We equate the P value, refusal rate, and finally time usage for each method with eight encryption methods.

For each eight encryption algorithm, we have 128 sequences (128-cipher text). Each sequence has a length of 7,929,856 bits (991,232 bytes). In the results .txt files for each test, the P-values in the tables can be found— not in the final Analysis Report.txt file in the kit of NIST.

The p-value provides the likelihood that the research results, which is more drastic towards non-randomness, can be found. P-value measures a randomness support hypothesis based on a specific test Rate of refusal number of rejected sequences (P-value below α may be 0.01 or 0.1 or 0.05). The better the higher the P value, and conversely the lower the better the lower the rejection rate (Soto, 1999).

A series of P values (equivalent to the sequence set) is generated for each statistical test. A certain proportion of P-values would imply a loss for a fixed level of importance α . For examples, if the value amount is 0,01 (i.e. α to 0,01), only 1 percent of the sequences would fail. Whenever the p-value is α and otherwise fails, a sequence passes a statistical test. We produce a P-value that does not randomly support small P-value (less than 0.01). For eg, where the sample consists of 128 sequences the rejection rate is not more than 4.657, or 4 sequences of $\alpha = 0.01$ can clearly be defined. The formula calculates maximum number of refusals:

$$\text{Rejection rate \#} = s \left(\alpha + 3 \sqrt{\frac{\alpha(1-\alpha)}{s}} \right)$$

where s is the sample size and α is the significance level is chosen to be 0.01.

5. SIMULATION RESULTS

As shown in Fig.7, system steps for OTP (Prakash et al., 2010). The users connect to the provider of the cloud. Then the user will get the username, password, and email of the account.

Users link via e-mail, password and the password of a server on the Cloud Provider website.

By logging user name, the paCloud Node Controller verifies the user info, users login to the website of the cloud provider

5.1 OTP Authentication:

OTP [23] System steps as shown in Fig. 7.

The users connect to the cloud provider. Then the user gets the username (e-mail), password and finally account password.

Users login to the cloud provider website by getting username (e-mail), password and account password.

Cloud node controller verifies user info. If user info is true, controller-node send that login authentication success and require OTP.

OTP generation software used to generate OTP as shown in Fig. 8.

Users generate OTP by using MD5 hash function and sequence number based on user name, password and account password.

Then users login to cloud website with OTP as shown in Fig. 9.

The cloud controller node generates 1000 OTP based on user info by using the MD5 hash function. Then the cloud controller saves 1000 OTP in the temporary OTP database.

The cloud controller verifies user OTP from the temporary OTP database.

If OTP is true, send OTP login success.

Secret word Space is an element of the size of the letter set and the quantity of characters from that letters in order that are utilized to make passwords. To decide the base size of the secret phrase space expected to fulfill the security necessities for an operational domain. In the content based secret word, a secret word space is figured as [23]:

$S = A \cdot M$ (2) Password length and letter set size are factors in registering the greatest secret phrase space prerequisites. Eq. 2 communicates the connection between

S, An, and M where:

S = secret phrase space;

A = number of letters in order images; M = secret phrase length.

To delineate: If passwords comprising of 4 digits utilizing a letter set of 10 digits (e.g., 0-9) are to be created: $S = 10^4$

That is, 10,000 special 4-digit passwords could be created. In like manner, to create irregular 6-character passwords from a letters in order of 26 characters (e.g., A-Z): $S = 26^6$

Secret phrase entropy is typically used to gauge the security of a created secret phrase which mean how hard to indiscriminately figure out the secret key.

Secret word Space is an element of the size of the letter set and the quantity of characters from that letters in order that are utilized to make passwords. To decide the base size of the secret phrase space expected to fulfill the security necessities for an operational domain. In the content based secret word, a secret word space is figured as [23]:

$S = A \cdot M$ (2) Password length and letter set size are factors in registering the greatest secret phrase space prerequisites. Eq. 2 communicates the connection between

S, An, and M where:

S = secret phrase space;

A = number of letters in order images; M = secret phrase length.

To delineate: If passwords comprising of 4 digits utilizing a letter set of 10 digits (e.g., 0-9) are to be created: $S = 10^4$

That is, 10,000 special 4-digit passwords could be created. In like manner, to create irregular 6-character passwords from a letters in order of 26 characters (e.g., A-Z): $S = 26^6$

Secret phrase entropy is typically used to gauge the security of a created secret phrase which mean how hard to indiscriminately figure out the secret key.

$$\text{Entropy} = M \times \log_2(A). \quad (3)$$

Figure 7: OTP authentication in PDSM **Figure 8:** Proposed software for OTP generation

As it were, entropy endeavor to gauge the likelihood of the attacker accepting the right secret phrase. For examples, a 6-character text message with Capital and small alphabets then the number of entropy bits = $6 \times \log_2(52) = 34.32$ [23].

Figure 9: Proposed OTP login screen

We have compared the password space with various password schemes to identify the fastest approaches to brute force attacks as shown in Table 3. This table shows a comparison of the space and password length of the popular cloud authentication schemes. It shows that we are both safer and easier to remember in our approach. At the same time, during the authentication process as shown in the figures, 10 and 11.

Table 3 Password space comparison.

Authentication system	Alphabet	Password length	Password space size	Entropy bits
Static password	82	12	92.4×1021	22.96
PIN number	10	12	1×1012	12
OTP	40	30	1.15×1048	48.06

Fig. 10 Security strength comparison based on entropy bits.

Fig. 11 Security strength comparison based on password space size.

We should remember that an OTP (once secret word) is a substantial secret phrase for just a one login session or exchange. An assortment of vulnerabilities of normal (static) passwords is secured by OTPs. The key disadvantage talked about by OTPs is that they are not helpless against replay assaults, in contrast with static passwords. In the event that a potential gatecrasher can record an OTP previously utilized for signing into assistance or leading an exchange, it can't mishandle it, since it is never again substantial. Then again, OTPs are difficult to remember for individuals. They in this manner need extra innovation to work.

Benefits of OTP in distributed computing

- OTP offers solid two-factor validation;
- OTP gives a solid security, since they are not expected to be bargained,
- OTP is restrictive to this session.
- Provides security from unapproved get to;
- Employee simpler to use than complex passwords that as often as possible change;
- Easy to convey for the director;
- Good initial step to solid hierarchical confirmation;
- Significant confirmation is more affordable.

5.2 Evaluation Algorithm Results

In this paper, the algorithm called "Evaluation algorithm" is chosen to be

the strongest and fastest encryption algorithm. This algorithm has the following functions: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish and Blowfish, for the option of eight modern encryption techniques. The review was done on the basis of randomness tests and NIST mathematical validation for those encryption algorithms. This calculation uses PRNG to decide the most appropriate. This evaluation algorithm performed at Amazon EC2 Micro Instance cloud computing environment.

Table 4 shows simulation results for the eight-encryption rejection rate algorithms selected for Amazon EC2. The table shows the results of Amazon EC2 rejection rates.

It can be seen that the results show no significant statistical shortcomings about Amazon EC2 rejections and the rejection rate does not surpass the maximum number of rejection rates for selected modern encryption techniques (expected 4) expect two tests. The first test number is 11: Random trips and the second test number is 12: Random trips.

Table 4 Amazon EC2 rejection rate for modern encryption algorithms.

Nist tests	RC6		RC4		DES		MARS		Two-Fish		Blowfish		3DES		AES	
	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept
1	127	1	127	1	127	1	127	1	127	1	127	0	128	0	128	0
2	127	2	126	3	125	4	124	1	127	1	127	1	127	2	126	0
3	127	2	126	0	128	1	127	1	127	1	127	2	126	0	128	0
4	125	1	127	1	127	1	127	0	128	2	126	1	127	0	128	0
5	126	0	128	1	127	1	127	3	125	1	127	3	125	1	127	0
6	127	1	127	0	128	1	127	0	128	3	125	1	127	0	128	0
7	0	128	0	128	1	127	2	126	1	127	2	126	3	125	125	0
8	0	128	1	127	2	126	2	126	2	126	1	127	0	128	1	127
9	1	127	2	126	1	127	1	127	0	128	1	127	1	127	1	127
10	1	127	1	127	2	126	1	127	3	125	2	126	1	127	2	126
11	51	77	51	77	52	76	62	66	50	78	51	77	54	74	48	80
12	53	75	50	78	51	77	59	69	48	80	52	76	56	72	47	81
13	2	126	2	126	0	128	0	128	3	125	0	128	2	126	1	127
14	1	127	2	126	1	127	1	127	3	125	1	127	0	128	2	126
15	0	128	2	126	0	128	1	127	1	127	1	127	2	126	1	127
16	4	124	0	128	1	127	3	125	2	126	2	126	1	127	1	127

Only if the number of cycles exceeds 500, the random excursion test and the random excursion variant test apply. If a sample has period sequences of less than 500, the number of valid sequences will be decreased (by 42 per cent) and the random excursion checks will not be tested. Any divergence from randomness could be wrongly indicated by a small sample size. It is important to remember that for each algorithm and data category only one sample was constructed.

The random hike test and random hike test depend on Eq. (4) the following:

$$j < \max(0.005\sqrt{n} \ 500) \dots (4)$$

Where J applies the cumulative number of cycles in the string and when the P values are too small, the randomness theory is dismissed. The outcome is shown in the NIST test 11 and test 12 files stats.tx, as shown in the Figs. 12 and 13

The most adequate encryption algorithm for Amazon EC2 is shown in Table 5 with experimental results for this comparison point. The results show the superiority of AES in terms of highest safety and faster encryption algorithms over other algorithms. There is another point that Blowfish and DES need less time and greater security than any algorithm other than AES. Another point is that Finally, two fish is considered to have low performance relative to other algorithms. All these results are from the 11.10 micro Instance of Amazon EC2 Ubuntu. All cloud companies with different operating systems should receive this evaluation. This point of comparison is shown in Figure.14 to provide the best protection for advanced rejection-based encryption techniques. In terms of rejection (small number), the results show the dominance of the AES algorithm over other algorithms.

The comparison point is shown in Figure. 15 to signify maximum safety for advanced P-value encryption techniques. The results show that the AES algorithm is equivalent to other P-value algorithms. The argument is that RC6 is more P than all algorithms except AES. It is not appropriate to use this form. A third point is that 3DES has an advantage in terms of p-value over other DES, RC4, MARS, 3DES and two fish. In contrast to other algorithms, it was also found that two fish has low reliability.

RANDOM EXCURSIONS TEST	
COMPUTATIONAL INFORMATION:	
(a) Number Of Cycles (J) = 0346	
(b) Sequence Length (n) = 991232	
WARNING: TEST NOT APPLICABLE. THERE ARE AN INSUFFICIENT NUMBER OF CYCLES.	

Figure 12: Screenshot of stats.txt file in NIST for random excursion test at Amazon EC2

RANDOM EXCURSIONS VARIANT TEST	
COMPUTATIONAL INFORMATION:	
(a) Number Of Cycles (J) = 32	
(b) Sequence Length (n) = 991232	
WARNING: TEST NOT APPLICABLE. THERE ARE AN INSUFFICIENT NUMBER OF CYCLES.	

Figure 13: Stats.txt file screenshot in NIST for the Amazon EC2 random excursion variant testing

Table 5 Modern encryption algorithms evaluation in Amazon EC2.

Evaluation parameters	1	2	3	4	5	6
Rejection Rate	AES	DES	Blowfish	RC4	TwoFish	RC6
P-value	AES	RC6	3DES	MARS	DES	Blowfish
Enc/Dec speed	Blowfish	AES	RC4	DES	RC6	MARS

Figure 14: Amazon EC2 average rejection rate for eight modern encryption algorithms

Figure 15: Amazon EC2 Average P-value for eight modern encryption algorithms based on 16 NIST test

This comparison point is shown in the figure 16 to specify encryption / decoding speed. The results demonstrate the dominance in processing time of the Blowfish algorithm over other algorithms. The point is that AES takes less time than all algorithms except Blowfish. A third point is that the RC4 is more advantageous in terms of time consumption than other DES, RC6, MARS, 3DES and two fish. A fourth point is that 3DES has low power consumption relative to DES. A fourth point can be seen here. Thanks to its triple-phase encryption property, it always takes longer than DES. Ultimately, Two fish has low performance compared to other algorithms.

Figure 16: Encryption/decryption comparison with different size in Amazon EC2

5.3 Security Desktop vs. Cloud

We notice from results that, the Desktop rejection rate more than Amazon EC2 Furthermore, In addition Desktop P- value is less than the Amazon EC2 P- value. Cloud computing requires advanced security capabilities than desktop computing. Cloud computing has less P-value numbers (under than 0.1 thresholds) than the mobile value (under 0.1 thresholds). This statement makes sure that cloud computing security is better than traditional desktop security as demonstrated in Fig. 17.

5.4 Private User Protection

Web services from Amazon encourage users to encrypt sensitive data with software True Crypt. A new software computer program is introduced before loading on cloud storage systems to encrypt records. This software allows users to select the AES, DES, 3DES, RC4, RC6, Twofish, Blowfish & MARS methods shown in the Fig. 18

5.5 Ensuring Integrity

This is an additional concern for customers to be worried about keeping the data hidden from auditors. The real issue of "confidence" remains the same. This paper proposes that the integrity control of information stored in the cloud may be monitored at a customer's side to avoid third parties' auditors in this chain. Such completeness test is feasible using the hash functions of a cryptograph.

Figure 17: Desktop and Amazon EC2 P-value comparison

Figure 18: Proposed encryption software CloudCrypt at runtime in Amazon EC2

For integrity check, we have to think about a simple solution that is feasible and easy to implement for a common user. The trust problem between Cloud storage and customer can be solved, if users can check the integrity of data themselves instead of renting an auditing service to do the same. This can be achieved by hashing the data on user's side and storing the hash values in the cloud with the original data. As shown in Fig. 19. This figure presents the overview of the scheme.

- (1) The program takes file path that as shown in Fig. 20;
- (2) This file is based on four Hash Functions in the system (MD4, MD5, SHA-1 and SHA-which are shown in Figure. 21;
- (3) If users are storing information in cloud storage systems, the data database has four hash values;
- (4) When a user retrieve data file, server generate four hash values;

Figure 19: Overview of integrity check with hash functions

Figure 20: Screen shot of check integrity program

Figure 21: Check integrity program calculating hash values

Table 6: Summarized results of the proposed data security model in cloud computing

Features	Description
Authentication	OTP Authentication System (mathematical generation).
Provider encryption	Software implemented to select the highest security and faster encryption algorithm based on NIST statistical tests.
Private user encryption	This software select AES algorithm to Micro Instance ubuntu Amazon EC2 with Amazon S3.
Data integrity	TrueCrypt system or proposed software CloudCrypt v.1.0.
Data fast recovery	Hashing-MD5-MD4-SHA-1-SHA-2.
Key management	Based on decryption algorithm speed.
	User keys not stored in provider control domain.

(5) Server integrity is checked by comparing four new hash values with four hash values stored.

The advantages of using the utility are as follows:

- Not much effort required for implementation.
- Cost effective and more secured.
- Do not take long to determine hash values.
- Sufficient to make changes to the level of security as necessary.
- Not much space is needed for hash values to be stored

6. CONCLUSIONS

According to the simulation results, in the authentication phase in the proposed data security model, OTP is used as two-factor authentication software. OTP archived more password strength security than other authentication systems (BIN and static password). This appears by comparing between OTP, BIN, and static password authentication systems based on the space time size and entropy bits. From the simulation results of the second phase in the proposed data security model, test the proposed system in Ubuntu Amazon Micro Instance EC2, and from randomness and performance evaluation to eight modern encryption algorithms AES is the best encryption algorithm in Ubuntu Amazon Micro Instance EC2. In addition to the randomness and performance evaluation, data integrity must be ensured. Moreover, the proposed data security model encourages users to use true-crypt to encrypt his/her sensitive data. From the comparison and performance evaluation, fast recovery of data achieved to the user. These appear in the proposed data security model third phase. From the comparison and performance evaluation, cloud computing depend on some condition, however it has advanced security technologies rather than traditional desktop. The summarized results of proposed data security model are shown in Table 6.

REFERENCES

- Amazon EC2 API. 2006. Amazon Elastic Compute Cloud Developer Guide [Online], Oct., <http://docs.amazonwebservices.com/AWSEC2/2006-10-01/DeveloperGuide/>.
- Amazon Web Services. 2006. Amazon Simple Storage Service Developer Guide [Online], Mar.
- Amazon Web Services. 2009. Overview of Security Processes [Online], Sep. <http://aws.typepad.com/aws/2009/08/introducing-amazon-virtual-private-cloud-vpc.html>.
- Burwick, C., D. Coppersmith. 1999. The MARS Encryption Algorithm, 27.
- Buyya, R., C.S. Yeo, S. Venugopal. 2009. Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities, in: 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, CCGRID'09, Shanghai, May 18-21.
- Coppersmith, D. 1994. The Data Encryption Standard (DES) and Its Strength Against Attacks, IBM Journal of Research and Development, 38, 243-250.
- Daemen, J., V. Rijmen. 2001. Rijndael: The advanced encryption standard,

- D r. Dobb's Journal, 26, 137-139.
- Dai, Y.F., B. Wu, Y.Q. Gu, Q. Zhang, C.J Tang. 2009. Data security model for cloud computing, in: Proceedings of The 2009 International Workshop on Information Security and Application IWISA 2009, Qingdao, China. 21-22.
- Dawson, E., H. Gustafson, M. Henricksen, B. Millan. 2002. Evaluation of RC4 Stream Cipher, Information Security Research Centre Queensland University of Technology, Jul. 31,
- Foster, L., Y. Zhao, I. Raicu, S.Y. Lu. 2008. Cloud computing and grid computing 360-degree compared, in: Grid Computing Environments Workshop, GCE'08, Austin, TX, 12-16, 1-10.
- Information Security Briefing Cloud Computing. 2010. Center of The Protection of National Infrastructure CPNI by Deloitte, 1, 71.
- Prakash, V., A. Infant, J. Shobana. 2010. Eliminating vulnerable attacks using One-Time Password and PassText—Analytical study of blended schema, Universal Journal of Computer Science and Engineering Technology, 1, 133-140.
- Rittinghouse, J.W., J.F. Ransome. 2009. Cloud Computing Implementation, Management, and Security, CRC Press, Boca Raton.
- Rukhin, A., J. Soto, J. Nechvatal, M. Smid. 2010. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication, Apr.
- Schneier, B. 2008. The Blowfish Encryption Algorithm [Online], <http://www.schneier.com/blowfish.html> (accessed: Oct. 25).
- Schneier, B., J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson. 1998. Twofish: A 128-bit block cipher, Jun. 15.
- Security Guidance for Critical Areas of Focus in Cloud Computing V1.0 [Online], Apr. 2009, Cloud Security Alliance Guidance, [www.cloudsecurityalliance.org/guidance/csaguide.v1.0.p df](http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf).
- Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 [Online]. 2009Dec., Cloud Security Alliance Guidance.
- Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 [Online]. 2009. Cloud Security Alliance Guidance.
- Soto, J. 1999. Randomness Testing of the Advanced Encryption Standard Candidate Algorithms, U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.
- Stallings, W. 2005. Cryptography and Network Security, 4th ed., Prentice Hall, N.J, 58-309.
- The NIST Definition of Cloud Computing. 2011. National Institute of Science and Technology, 7. Retrieved July 24.
- Vouk, M.A. 2008. Cloud computing-issues, research and implementations, Journal of Computing and Information Technology, 16, 235-246