Data Security Model for Cloud Computing

Eman M.Mohamed
Department of Computer Science, Menofia University
Faculty of computers and information
Egypt
emanhabib_1987@yahoo.com

Hatem S.Abdelkader
Department of Information Systems, Menofia University
Faculty of computers and information
Egypt
hatem6803@yahoo.com

Sherif El-Etriby
Department of Computer Science, Menofia University
Faculty of computers and information
Egypt
El_etriby100@yahoo.com

***Abstract*— From the perspective of data security, which has always been an important aspect of quality of service, Cloud computing focuses a new challenging security threats. Therefore, a data security model must solve the most challenges of cloud computing security. The proposed data security model provides a single default gateway as a platform. It used to secure sensitive user data across multiple public and private cloud applications, including salesforce, Chatter, Gmail, and Amazon Web Services, without influencing functionality or performance. Default gateway platform encrypts sensitive data automatically in a real time before sending to the cloud storage without breaking cloud application. It did not effect on user functionality and visibility. If an unauthorized person gets data from cloud storage, he only sees encrypted data. If authorized person accesses successfully in his cloud, the data is decrypted in real time for your use. The default gateway platform must contain strong and fast encryption algorithm, file integrity, malware detection, firewall, tokenization and more. This paper interested about authentication, stronger and faster encryption algorithm, and file integrity.**

Keywords- Cloud computing; Data Security model in cloud computing; Randomness testing; Cryptography for cloud computing; One Time Password (OTP).

I. INTRODUCTION

In the traditional model of computing, both data and software are fully contained on the user's computer; in cloud computing, the user's computer may contain almost no software or data (perhaps a minimal operating system and web browser, display terminal for processes occurring on a network).

Cloud computing is based on five attributes: multi-tenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources, it makes new advances in processors, Virtualization technology, disk storage, broadband Internet connection, and fast, inexpensive servers have combined to make the cloud a more compelling solution.

The main attributes of cloud computing are illustrated as follows [1]:

- Multi-tenancy (shared resources): 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.
- Massive scalability: Cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space
- Elasticity: Users can rapidly increase and decrease their computing resources as needed.
- Pay as you used: Users to pay for only the resources they actually use and for only the time they require them.
- Self-provisioning of resources: Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

Cloud computing can be confused with distributed system, grid computing, utility computing, service oriented architecture, web application, web 2.0, broadband network, browser as a platform, Virtualization, and free/open software [2].

Cloud computing is a natural evolution of the widespread adoption of virtualization, service-oriented architecture, autonomic, and utility computing [3]. Details are abstracted from end-users, who no longer have a need for expertise in, or control over, the technology infrastructure "in the cloud" that supports them as shown in figure 1.

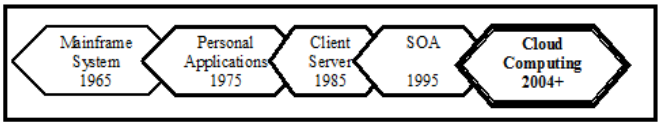

Figure 1. Evolution of cloud computing

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches such as On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured service [4].

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5

Cloud computing often leverages Massive scale, Homogeneity, Virtualization, Resilient computing (no stop computing), Low cost/free software, Geographic distribution, Service orientation Software and Advanced security technologies [4].

The main objective of this paper is to enhance data security model for cloud computing. The proposed data security model solves cloud user security problems, 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 proposed data security model is composed of three-phase defense system structure, in which each floor performs its own duty to ensure that the data security of cloud. The first phase is responsible for strong authentication. It applies the OTP (one time password) 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 modern encryption techniques namely: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish. The evaluation has performed for those encryption algorithms according to randomness testing by using NIST statistical testing. This evaluation uses Pseudo Random Number Generator (PRNG) to determine the most suitable. This evaluation algorithm performed at Amazon EC2 Micro Instance cloud computing environment. 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.

The paper is organized as follows, in section 2 cloud computing architecture is defined. Cloud computing security is discussed in section 3, in section 4 Methodology is described, finally in section 5 interruptions of the results are described.

II. CLOUD COMPUTING ARCHITECTURE

A. *Cloud computing service models*

- Cloud Software as a Service (SaaS): Application and Information clouds, Use provider's applications over a network, cloud provider examples Zoho, Salesforce.com, Google Apps.
- Cloud Platform as a Service (PaaS): Development clouds, Deploy customer-created applications to a cloud, cloud provider examples Windows Azure, Google App Engine, Aptana Cloud.
- Cloud Infrastructure as a Service (IaaS): Infrastructure clouds, Rent processing, storage, network capacity, and other fundamental computing resources, Dropbox, Amazon Web Services, Mozy, Akamai.

B. *Cloud computing deployment models*

- Private cloud : Enterprise owned or leased
- Community cloud: Shared infrastructure for specific community
- Public cloud: Sold to the public, mega-scale infrastructure
- Hybrid cloud: Composition of two or more clouds

C. *Cloud computing sub-services models* [12]

- IaaS: DataBase-as-a-Service (DBaaS): DBaaS allows the access and use of a database management system as a service.
- PaaS: Storage-as-a-Service (STaaS): STaaS involves the delivery of data storage as a service, including database-like services, often billed on a utility computing basis, e.g., per gigabyte per month.
- SaaS: Communications-as-a-Service (CaaS) : CaaS is the delivery of an enterprise communications solution, such as Voice over IP, instant messaging, and video conferencing applications as a service.
- SaaS: SECurity-as-a-Service (SECaaS): SECaaS is the security of business networks and mobile networks through the Internet for events, database, application, transaction, and system incidents.
- SaaS: Monitoring-as-a-Service (MaaS): MaaS refers to the delivery of second-tier infrastructure components, such as log management and asset tracking, as a service.
- PaaS: Desktop-as-a-Service (DTaaS): DTaaS is the decoupling of a user's physical machine from the desktop and software he or she uses to work.
- IaaS: Compute Capacity-as-a-Service (CCaaS) : 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.

D. *Cloud computing benefits*

Lower computer costs, improved performance, reduced software costs, instant software updates, improved document format compatibility, unlimited storage capacity, device independence, and increased data reliability

E. *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.

F. *Cloud computing providers*

Amazon Web Services (AWS) –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 and so on.

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5

III. CLOUD COMPUTING SECURITY

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?

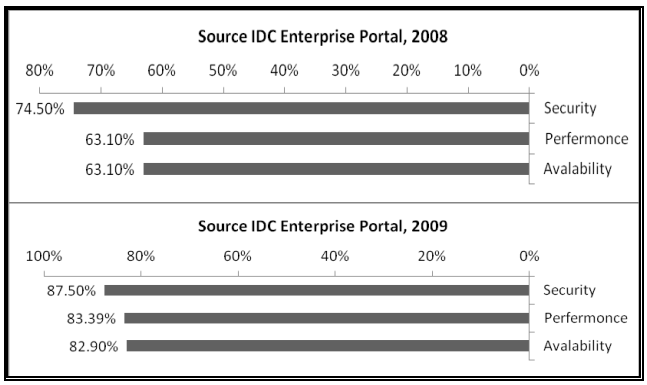

Figure 2. Security is a major concern to cloud computing[28]

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 figure 2.

While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater level of security than the organization would have if the cloud were not used.

There are three types of data in cloud computing. The first type is a data in transit (transmission data), the second data at rest (storage data), and finally data in processing (processing data).

Clouds are massively complex systems can be reduced to simple primitives that are replicated thousands of times and common functional units, These complexities create many issues related to security as well as all aspects of Cloud computing. 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.

TABLE I. DATA SECURITY [ENCRYPTION] IN CLOUD COMPUTING

Storage	Processing	Transmission
Symmetric encryption	***Homomophric encryption***	***Secret socket layer SSL encryption***
AES-DES-3DES-Blowfish-MARS…	Unpadded RSA- ElGamal …	SSL 1.0- SSL 3.0-SSL 3.1-SSL 3.2...

IV. METHODOLOGY

Security of data and trust problem has always been a primary and challenging issue in cloud computing. 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.

A. Proposed data at rest security model

The proposed data security model used three-level defense system structure, in which each floor performs its own duty to ensure that the data security of cloud as shown in figure 3.

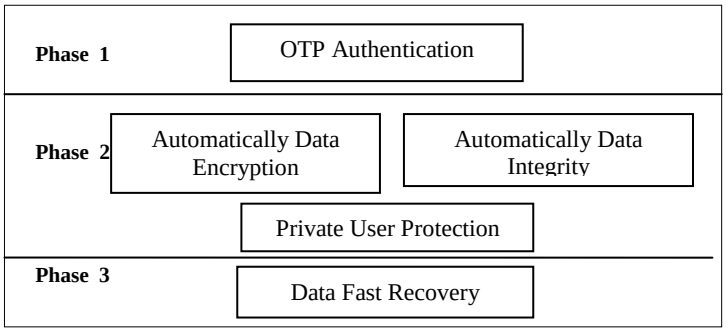

Figure 3. Proposed data security model in cloud computing

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 figure 4. The proposed data security model provides a single default gateway as a platform to secure sensitive customer data across multiple public and private cloud applications, including salesforce, Gmail, and Amazon Web Services, without affecting functionality or performance.

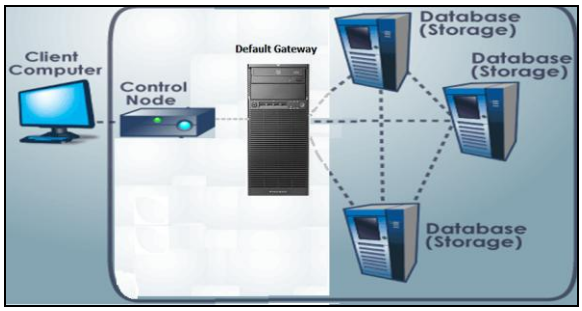

Figure 4. How data stored in the cloud by using the proposed data security model?

Default gateway platform tasks:

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5

- 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.
- If authorized person access success in his cloud, the data is decrypted in real time for your use.
- The default gateway platform must contain Strong/Fast Encryption Algorithm.
- The default gateway platform must contain File integrity.
- The default gateway platform must contain Malware detection, Firewall, Tokenization and more.

Proposed data security model implemented and applied to cloudsim 3.0 by using HDFS architecture and Amazon web services (S3 and EC2).

In this paper, automatically encryption, integrity, fast recovery and private user encryption all are achieved in the proposed data security model.

B. *Implementation details*

1) In first phase, Authentication:

a) The cloud user select company, then create an account

b) Cloud provider upload user information in DB in cloud storage

c) Cloud Provider confirms user with his username and password

d) Cloud user request login page

e) The cloud provider displays login screen

f) Cloud user login with username and password

g) A cloud provider check is valid username and password by searching in DB in cloud storage. If user information not valid display error message else display reserve a PC page.

h) Cloud user reserves your PC

2) OTP authentication steps:

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

b) Cloud user generates an OTP

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

d) Cloud user login with OTP

e) A cloud provider check is valid OTP by searching in temporary DB for OTP in cloud storage. If OTP not valid display error message else display user PC page.

3) In second phase, Private user protection

a) Before adding data, cloud user can encrypt data by using TrueCrypt or CloudCrypt software's.

b) In second phase, Automatic data encryption

c) Cloud user adds data.

d) Cloud server encrypt data automatically by using fast/strong encryption algorithm that selected based on an evaluation algorithm for the cloud company

4) In second phase, Automatic check data integrity

a) The cloud server generates file hash value

b) Cloud server store data with its hash value

c) When a cloud user requests his data, cloud server decrypt data automatically, check integrity by check the hash value.

5) In third phase, fast recovery of data

a) Finally, cloud server retrieves data with message of file integrity.

C. *Proposed Evaluation Algorithm*

We use NIST statistical tests to get the highest security encryption algorithm from eight algorithms namely RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish as shown in figure 6. NIST Developed to test the randomness of binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators.

NIST statistical tests has 16 test namely The Frequency (Mon-obit) Test, Frequency Test within a Block, The Runs Test, Tests for the Longest-Run-of-Ones in a Block, The Binary Matrix Rank Test, The Discrete Fourier Transform (Spectral) Test, The Non-overlapping Template Matching Test, The Overlapping Template Matching Test, Maurer's "Universal Statistical" Test, The Linear Complexity Test, The Serial Test, The Approximate Entropy Test, The Cumulative Sums (Cusums) Test, The Random Excursions Test, and The Random Excursions Variant Test.

We also compare between eight encryption algorithms based on speed of encryption to achieve faster recovery.

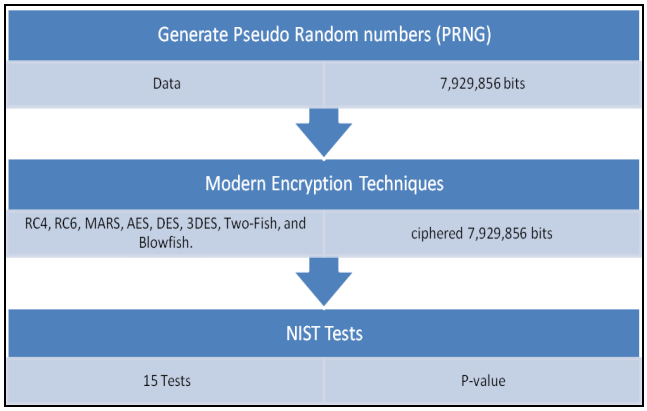

Figure 5. Steps to select the highest encryption algorithm

We use Amazon EC2 as a case study of our software. Amazon EC2 Load your image onto S3 and register it. Boot your image from the Web Service. Open up the required ports for your image. Connect to your image through SSH. And finally execute your application.

For our experiment in a cloud computing environment, we use Micro Instances of this Amazon EC2 family, provide a small amount of consistent CPU resources, they are well

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5

suited for lower throughput applications, 613 MB memory, up to 2 EC2 Compute Units (for short periodic bursts), EBS (Elastic Block Store) storage only from 1GB to 1TB, 64-bit platform, low I/O Performance, t1.micro API name, We use Ubuntu Linux to run NIST Statistical test package [9-11].

D. Selection the highest encryption algorithm steps

Sign up for Amazon web service to create an account. Lunch Micro instance Windows (64 bit) Amazon EC2. Connect to Amazon EC2 windows Micro Instance. Generate 128 plain stream sequences as PRNG, each sequence is 7,929,856 bits in length (991232 bytes in length) and key stream (length of key 128 bits). Apply cryptography algorithms to get ciphers text. Lunch Micro instance Amazon EC2 Ubuntu Linux Connect to Amazon EC2 Ubuntu Linux Micro instance Run NIST statistical tests for each sequence to eight encryption algorithms to get P-value Compare P-value to 0.01, if p-value less than 0.01 then reject the sequence.

We compare between eight encryption methods based on P-value, Rejection rate and finally based on time consuming for each method.

We have 128 sequences (128-cipher text) for each eight-encryption algorithm.

Each sequence has 7,929,856 bits in length (991232 bytes in length). Additionally, the P-values reported in the tables can find in the *results.txt* files for each of the individual test – not in the *finalAnalysisReport.txt* file in NIST package.

The P - value represents the probability of observing the value of the test statistic which is more extreme in the direction of non-randomness. P-value measures the support for the randomness hypothesis on the basis of a particular test Rejection Rate number of rejected sequences (P-value less than significance level α may be equal 0.01 or 0.1 or 0.05). The higher P-Value the better and vice versa with rejection rate, the lower the better [19].

For each statistical test, a set of P-values (corresponding to the set of sequences) is produced. For a fixed significance level α, a certain percentage of P-values are expected to indicate failure. For example, if the significance level is chosen to be 0.01 (i.e., $\alpha \geq 0.01$), then about 1 % of the sequences are expected to fail. A sequence passes a statistical test whenever the P-value $\geq \alpha$ and fails otherwise.

We produce P-value, which small P-value(less than 0.01) support non-randomness. For example, if the sample consists of 128 sequences, the rejection rate should not exceed 4.657, or simply expressed 4 sequences with α = 0.01. The maximum number of rejections was computed using the formula [20]:

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

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

V. SIMULATION RESULTS

In this section, we show and describe the simulation results of the proposed data security model.

A. OTP Authentication

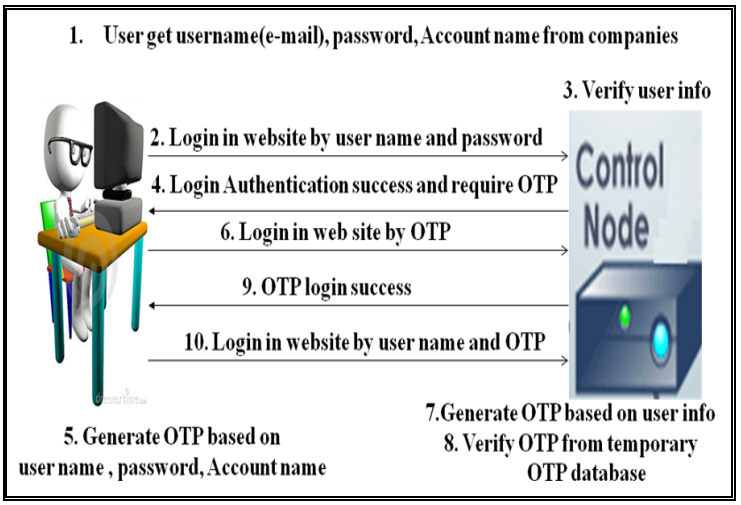

Figure 6. OTP authentication in PDSM

OTP System steps as shown in figure 6.

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 figure 7.

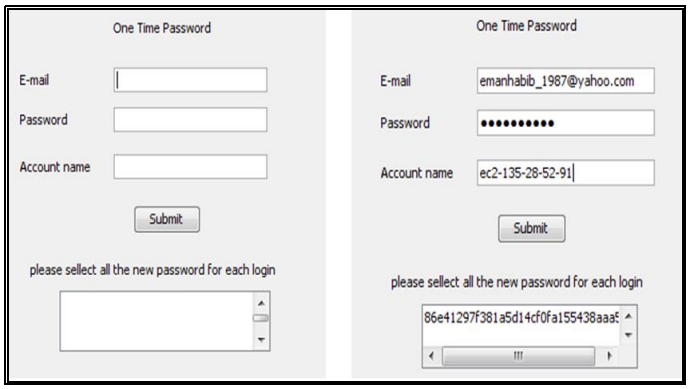

Figure 7. Proposed software for OTP Generation

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 figure 8.

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5

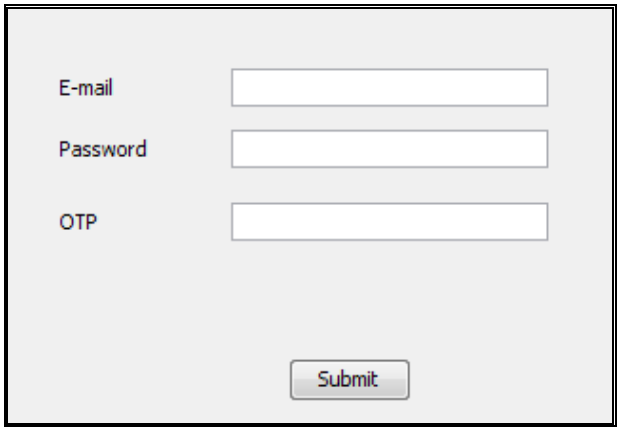

Figure 8. proposed OTP login screen

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.

We have compared password space with different password schemas; we can identify the most secure approaches with respect to brute force attack as shown in table 2. This table shows the comparison of the password space and password length for popular user authentication schemas for cloud computing. The next table shows that the approach presented by us is both more secured and the easiest to remember. At the same time, it is relatively fast to produce during an authentication procedure as shown in figure 9 and figure 10.

TABLE II. PASSWORD SPACE COMPARISON

Authentication System	Alpha bet	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

We must remember that, a one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that, if a potential intruder manages to record an OTP that was already used to log into a service or to conduct a transaction, he or she will not be able to abuse it since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology in order to work.

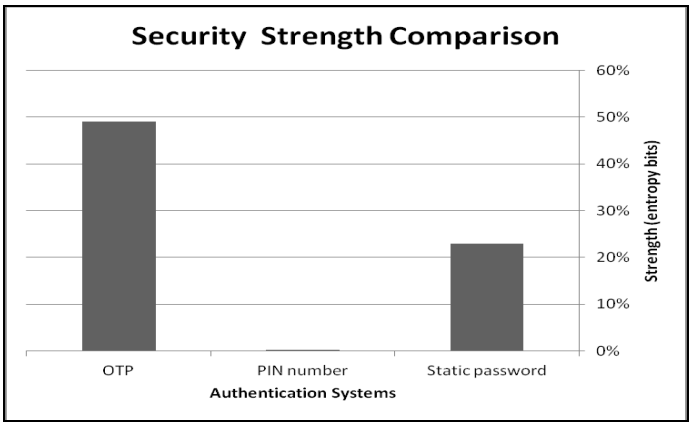

Figure 9. Security strength comparison based on entropy bits

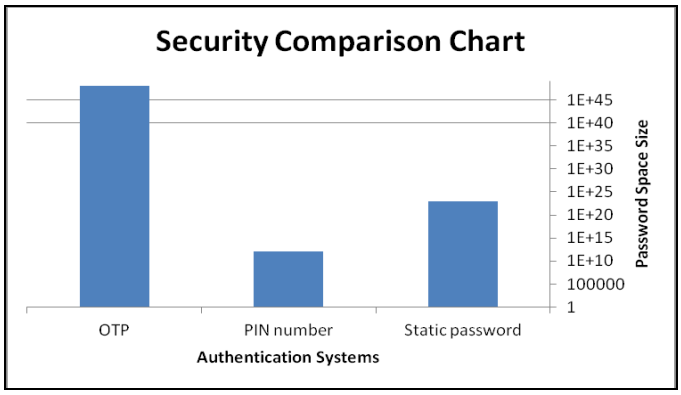

Figure 10. Security strength comparison based on password space size

Benefits of OTP in cloud computing

- OTP offers strong two-factor authentication,
- The OTP is unique to this session and cannot be used again
- OTP offers strong security because they cannot be guessed or hacked
- Provides protection from unauthorized access
- Easier to use for the employee than complex frequently changing passwords
- Easy to deploy for the administrator
- Good first step to strong authentication in an organization
- Low cost way to deploy strong authentication

B. Evaluation Algorithm Results

In this paper, we select the strongest and a the fastest encryption algorithm by proposing algorithm called "Evaluation algorithm". This algorithm used for selecting eight modern encryption techniques namely: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish. The evaluation has performed for those encryption algorithms according to randomness testing by using NIST statistical testing. This evaluation uses Pseudo Random Number

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5

Generator (PRNG) to determine the most suitable. This evaluation algorithm performed at Amazon EC2 Micro Instance cloud computing environment.

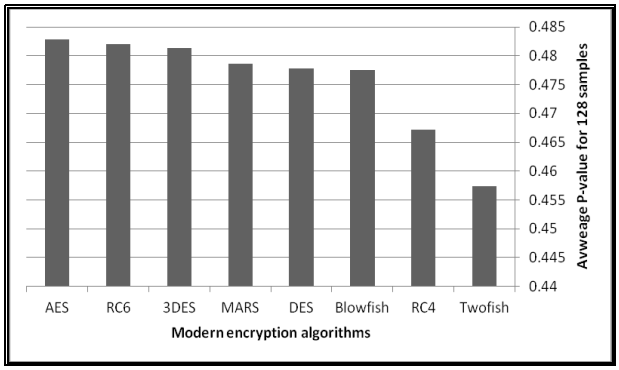

Figure 11. Amazon EC2 Average P-value for eight modern encryption algorithms based on 16 NIST test

Experimental results for this comparison point are shown in figure 11 to indicate the highest security for modern encryption techniques. The results show the superiority of the AES algorithm over other algorithms in terms of the P-value. Another point can be noticed here; that RC6 requires more P-value than all algorithms except AES. A third point can be noticed here; that 3DES has an advantage over other DES, RC4, MARS, 3DES and Twofish in terms of P-value. Finally, it is found that Twofish has low security when compared with other algorithms.

Experimental results for this comparison point are shown Figure 12 to indicate the speed of encryption/decryption. The results show the superiority of the Blowfish algorithm over other algorithms in terms of the processing time. Another point can be noticed here; that AES requires less time than all algorithms except Blowfish. A third point can be noticed here; that RC4 has an advantage over other DES, RC6, MARS, 3DES and Twofish in terms of time consumption . A fourth point can be noticed here; that 3DES has low performance in terms of power consumption when compared with DES. It always requires more time than DES because of its triple phase encryption characteristics. Finally, it is found that Twofish has low performance when compared with other algorithms.

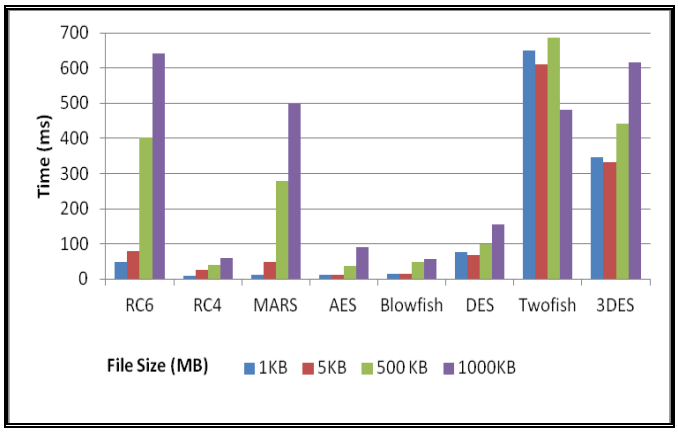

Figure 12. Encryption/decryption comparison with different size in Amazon EC2

C. *Private User protection*

Amazon web services encourage user's to encrypt sensitive data by using TrueCrypt software. A new computer software program is implemented to encrypt data before storing in cloud storage devices. This software enables users to choose from eight encryption techniques namely: AES, DES, 3DES, RC4, RC6, Twofish, Blowfish, and MARS as shown in figure 13.

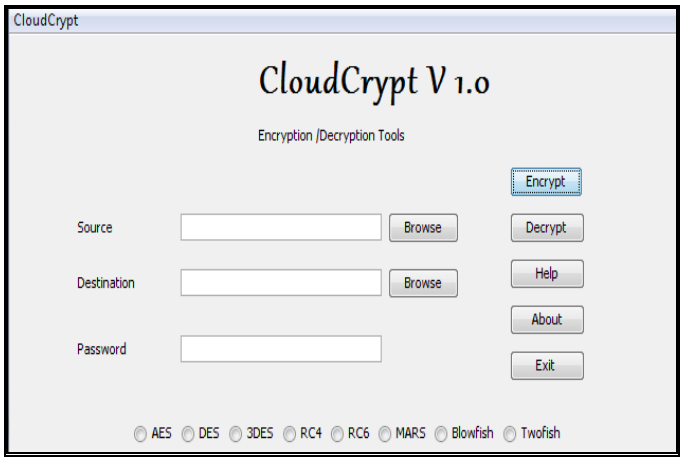

Figure 13. Proposed encryption software CloudCrypt at runtime in Amazon EC2

D. *Ensuring Integrity*

This is an extra concern for customers that now they have to worry about how to keep data hidden from auditors. The actual problem of "trust" remains the same. In order to avoid third party auditors in this chain, this paper propose that the integrity check of data stored in the cloud can be checked on customer's side. This integrity check can be done by using cryptographic hash functions.

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

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5

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 figure 14. This figure presents the overview of the scheme

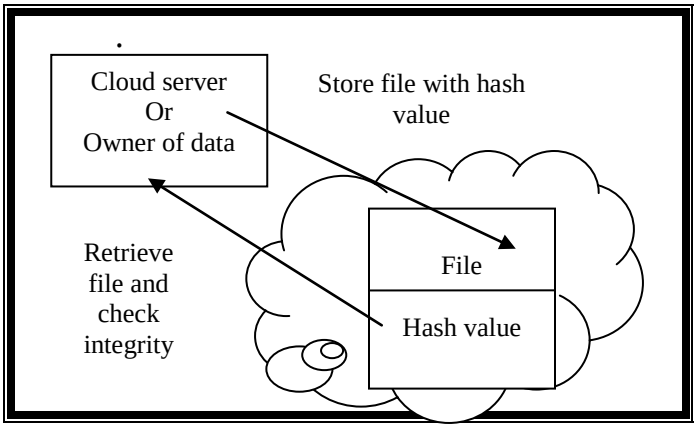

Figure 14. Overview of integrity check with hash functions

Integrity Check using Hash Function steps

- The program takes file path that as shown in figure 15.
- The program computes a four-hash values in this file based on the four hash functions (MD4, MD5, SHA-1, and SHA-2) as shown in figure 16.

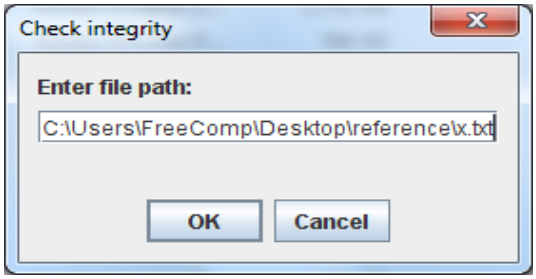

Figure 15. Screen shot of Check integrity program

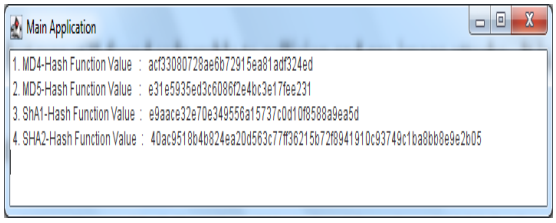

Figure 16. Check integrity program calculating hash values

- When users store data in cloud storage devices, server store filled with four hash values.
- When a user retrieve data file, server generate four hash values
- Server check integrity by comparing new four hash values with stored four hash values.

The following are the advantages of using the utility:

- Not much implementation effort required.
- Cost effective and more secured.
- Does not require much time to compute the hash values.
- Flexible enough to change the security level as required.
- Not much space required to store the hash values.

VI. CONCLUSION

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 Ubunto Amazon Micro Instance EC2, and from randomness and performance evaluation to eight modern encryption algorithms AES is the best encryption algorithm in Ubunto 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 3.

TABLE III. 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. This software select AES algorithm to Micro Instance ubunto Amazon EC2 with Amazon S3.
Private user Encryption	TrueCrypt system or proposed software CloudCrypt v.10
Data integrity	Hashing- MD5- MD4-SHA-1-SHA-2
Data fast recovery	Based on decryption algorithm speed
Key management	User keys not stored in provider control domain

REFERENCES

[1] Center Of The Protection Of National Infrastructure CPNI by Deloitte "Information Security Briefing 01/2010 Cloud Computing", p.71 , Published March 2010.

[2] lan Foster, Yong Zhao, Ioan Raicu, Shiyong Lu, " Cloud Computing and Grid Computing 360-Degree Compared " Grid Computing Environments Workshop, 2008. GCE '08 p.10, published 16 Nov 2008.

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5

[3] Jeremy Geelan, "Twenty-One Experts Define Cloud Computing", cloud computing journal, published january 24, 2009.

[4] National Institute of Science and Technology."The NIST Definition of Cloud Computing".p.7. Retrieved July 24 2011.

[5] Ngongang Guy Mollet, "Cloud Computing Security" Thesis, p. 34 + 2 appendices Published April 11, 2011.

[6] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal, " Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities" Department of Computer Science and Software Engineering, University of Melbourne, Australia. p. 9. Retrieved July 31 2008.

[7] Mladen A. Vouk "Cloud Computing- Issues, Research and mplementations" Journal of Computing and Information Technology -CIT 16, 2008, 4, 235–246

[8] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing"Data Security Model for Cloud Computing"Proceedings of the 2009 international Workshop on Information Security and Application IWISA 2009) Qingdao, China, November 21-22, 2009.

[9] Amazon EC2 API ," Amazon Elastic Compute Cloud Developer Guide " http://docs.amazonwebservices.com/AWSEC2/2006-10-01/DeveloperGuide/Amazon Elastic Compute Cloud Developer Guide, published 2006-10-01

[10] Amazon Web Services, "Amazon Simple Storage Service Developer Guide , " http://docs.amazonwebservices.com/AmazonS3/2006-03-01/ Amazon Simple Storage Service Developer Guide , published 2006-03-01

[11] Amazon Web Services," Overview of Security Processes" http://aws.typepad.com/aws/2009/08/introducing-amazon-virtual-private-cloud-vpc.html, September 2009.

[12] Cloud Security Alliance Guidance, "Security Guidance For Critical Areas of Focus In Cloud Computing V1.0", www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf, published April 2009

[13] Cloud Security Alliance Guidance," Security Guidance For Critical Areas of Focus In Cloud Computing V2.1", www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, published Dec 2009

[14] Cloud Security Alliance Guidance, "Security Guidance For Critical Areas of Focus In Cloud Computing V3.0 , www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf published 11/14/2011

[15] Luis M. Vaquero1, Luis Rodero-Merino1 , Juan Caceres1, Maik Lindner2 "A Break in the Clouds: Towards a Cloud Definition ", ACM SIGCOMM Computer Communication Review, Vol 39, Number 1, published January 2009

[16] John W. Rittinghouse James F. Ransome "Cloud Computing Implementation, Management, and Security" book, published 17 Aug 2009.

[17] Mark Baker, "An Introduction and Overview of Cloud Computing",43 slides, published 19th May, 09 . http://acet.rdg.ac.uk/~mab/Talks/Clouds-La-Coruna09/Talk.ppt

[18] Cloud Security Alliance "Top Threats to Cloud Computing V1.0" , March 2010.

[19] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid,: "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", April 2010 .

[20] Affiliation Juan Soto, National Institute of Standards and Technology 100 Bureau Drive, Stop 8930 Gaithersburg "Randomness Testing of the Advanced Encryption Standard Candidate Algorithms".

[21] Carolynn Burwick c , Don Coppersmith "The MARS Encryption Algorithm " , published August 27, 1999

[22] Dawson, Helen Gustafson, Matt Henricksen, Bill Millan. " Evaluation of RC4 Stream Cipher , Information Security Research Centre Queensland University of Technology", July 31, 2002

[23] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

[24] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks."I BM Journal of Research and Development, May 1994,pp. 243 -250.

[25] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, March 2001,PP. 137-139.

[26] Bruce Schneier. "The Blowfish Encryption Algorithm Retrieved ",October 25, 2008,

[27] John Kelseyy Doug Whitingz David Wagnerx Chris Hall, "Two_sh: A 128-Bit Block Cipher" , Niels Ferguson k , 15 June 1998

[28] http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt.

Copyright (c) The Government of Egypt, 2013. Used by permission to IARIA. ISBN: 978-1-61208-245-5