Mansoura Journal of Computers and Information Sciences

# Data Security Evaluation Based on Trend Line Rules Model

Nazar.K. Khorsheed
Faculty of Computers and Information
Mansoura University, Egypt.
nizarkhorshd@yahoo.com

Mohammad.A.El-Dosuky.
Faculty of Computers and Information
Mansoura University, Egypt.
mouh_sal_010@mans.edu.eg

Taher.T.Hamza
Faculty of Computers and Information
Mansoura University, Egypt.
taher_hamza@yahoo.com

Magdi.Z. Rashad
Faculty of Computers and Information
Mansoura University, Egypt.
magdi_z2011@yahoo.com

## Abstract

With the rise in demand for cloud services, most companies attempt to provide a lot of cloud services and benefit from them, one of the most important services is accounting the cost of data ciphering in the clouds market. This proposed work proved that the cryptographic keys are variable as evident mathematically, which in turn makes it difficult to guess the decoding of the data, and extends the cloud security model by generating both private and public keys based on local cost and trend line rules respectively. Due to the increased decoding time as evident from the proof results, the suitable security level is implemented and tested using Symmetric and Asymmetric encryption algorithms.

**Keywords::**Cloud Computing; trend line Models, Symmetric and Asymmetric Algorithms.

## Introduction:

Cloud computing, whatever it is, is a phenomenon that has turned the case of traditional business and economic plans and expectations. This new technology has provided users with the wide range to store, download, manage and maintain their data quickly, efficiently and inexpensively. There are many different definitions for the interpretation of this phenomenon and the definition of NIST makes this phenomenon more obvious [1].

Cloud computing provides a comprehensive customer service. Data cost calculation is the most important relationship between service providers and customers. Big competition among computing service providers to provide the best customer service at the lowest cost is the main concern. Calculating the cost, storage, transmission, management and coding of data has a significant impact for cloud-equipped companies as it affects the relationship of customers and organizations directly with these companies, as well as the cost of data which has a great economic impact. The data cost calculation model is flexible as opposed to traditional models. As the vendors compete to provide services to customers and each has its own price and that it seems appropriate for customers. The calculation of cost in cloud computing is based primarily on business and IT services. This varies according to business estimates and processes provided by cloud computing. The main problem is how to measure these costs and in what way. Also, there are many models that can be used to calculate and explain the cost of data within cloud computing [2].

This study extends a recently proposed cloud security model, based on generating both private and public keys based on local cost and trend line rules respectively. The proposed approach is to introduce a new security concept in cloud computing by measuring the performance of a set of symmetric and asymmetric algorithms, computing the cost of computational coding, decoding data using multiple keys, and evaluating the efficiency of these algorithms in protecting and securing systems data for different sizes of data [2]. The new method is based on the trend line rules model, and the data is saved as a top priority.

## 2. Related Works:

The cost issue in the cloud and The relationship between cloud service providers and customers from the perspective of many authors, who read different ideas and carried out some theoretical models and simulation process using several different programs.

**Sharma et al.,** [3] provided an economic model capable of providing quality services to customers. The idea of financial choices as assets for managing cloud resources has been developed at a typical price and is considered the best price that covers the service provider's initial costs. They indirectly used Moore's law to determine the cost of resources in the cloud and the Blacksmith Merton model, which read cloud resources as public assets. The value of initial investments, the period of impact of the contract, and the impact of resources on life and prices were analyzed. It is where the focus is only the initial price but does not affect the maintenance cost.

**Btel and Shah,**[4] studied price values within data centers, which focused on three things: energy, space and cooling using the cost model. An analysis of the cost of prices for each of the three cases and the total cost of the services, as compared to the actions taken within the data centers.

**Bal and Hui,**[5] studied economic solutions and resource costs using the idea of the game and presented an economic model. The first model is about the quality of service provided by the cloud service provider. It is predetermined and competitors can compete others on prices. The other model is the quality of service applications provided by the cloud service provider and compete for the prices of specific applications.

**Wang et al.** [6] They offered ideal solutions to increase net profits of data centers with a data table that works on the deadline by increasing revenues and reducing electricity. The researchers have demonstrated these solutions through using an algorithm and simulation work for the algorithm first (to dry). The authors looked only at achieving access to established jobs and then leaving. Servers in all data centers are also considered homogeneous, not realistic.

**Yeoa et al.**[7] They evaluated the difference between fixed and variable prices. Where fixed prices are understood and presented directly to

customers, fixed prices are not suitable for all customers because everyone does not have the same orders. It was proposed to add variable prices with pre-booking, in which case customers will know the calculated fees and the booking time even though was based on variable prices.

**Macias and Guitart,** [8] proposed the genetics model of pricing and arithmetic in cloud computing. The selection of the good cost model is done by making the genetic algorithm and has three steps: First determine the chromosome, then evaluate it, and choose the best pairs of chromosomes suitable for reproduction neglecting others with bad results. The results showed that the cost of the genetic algorithm took on the highest revenue among many of the proposals. Providers of this service model using genetic cost have achieved revenues of up to 100% more than other dynamic cost models, which are up to 1000% more than fixed cost models.

**Li et al.** [9] algorithm was introduced to calculate cost in cloud computing. The authors proposed the cloud bank commission model as resources from a global perspective and provided detailed guidance to all customers. The model evaluates the utilization rate of resources, constantly reiterates the current price ratio, and obtains availability and continuity of resources each time, where the final price is expected to be calculated for customers. But this proposed model was not able to accommodate the rapid changes taking place in the market.

## 3. Proposed System:

There are many models and businesses which contain applications that provide different services through which the cost value of services is set in the cloud. As an example, there is an example of a cost accounting model for cloud computing which addresses how costs are calculated in the production and delivery of cloud services [10].

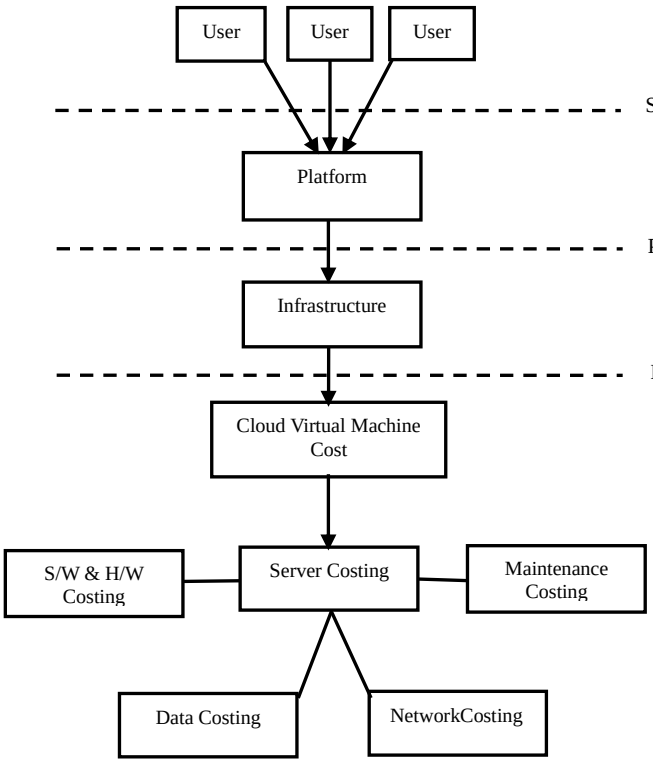


Figure.1. General Diagram of Cloud Computing Cost Model[11].

### 3.1 Data Costing Method:

Basically, data can be cross-sectional or time series data. Treatment of time series econometrics has some issues concerning trends, persistence, dynamics, and seasonality. The Econometric linear Regression analysis is mentioned in the in reference [12].

### 3.2 Trend Line Rules Model:

Trend lines are the lines connecting the peaks that represent the highest price or bottoms that represent the lowest price within a trend line extending into the future. There are two types of trend lines: the ascending trend line and the descending trend line. The upward trend line (descending trend) is created if the line connecting the (bottoms) and (tops) is pointing upwards and downwards [13].

More clearly, let $pk_{i1}^{(n)}$ and $pk_{i2}^{(n)}$, be the two lowest, highest (peaks), in the time interval [t-n, t-1] with t1<t2, i.e., Where the minimum cost be:

$$\min = \{p_{k-1} < p_{k-1}, p_{k+1}\} \quad (1)$$

And the maximum cost be:

$$\max = \{p_k > p_{k-1}, p_{k+1}\} \quad (2)$$

where min, max, means "collect the two smallest or (largest)", and t1, t2 (t1< t2) be the time points at these two lowest or (highest) cost are located.

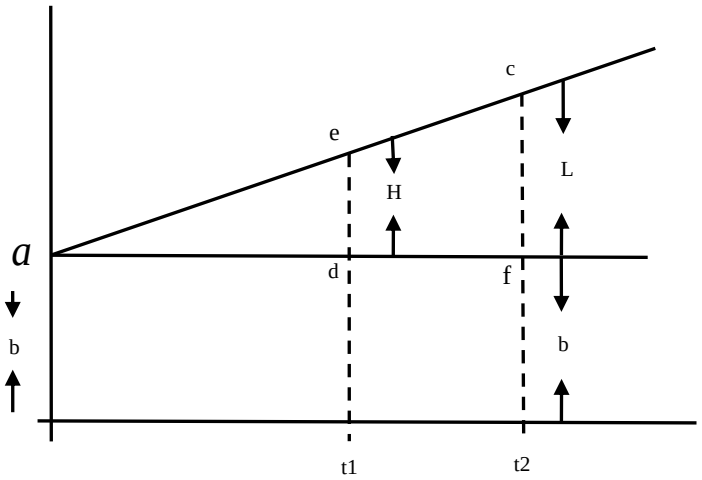


Figure.2.Example of Trend Line Method.

Let the Trend line Rules Equation be:

$$Y = at + b \quad (3)$$

Where

$$a = slop = \frac{dy}{dx} = \frac{\mathrm{p\,k}_{t2}^{(n)} - pk_{t1}^{(n)}}{\mathrm{t}_2 - t_1} \quad (4)$$

b = value of Y. From similarity of the two triangle we can see from the figure2.

$$\therefore \frac{H}{L} = \frac{t_2}{t_1} \quad (5)$$

$$\because H = pk_{t1}^{(n)} - \mathrm{b} \quad (6)$$

$$\therefore \frac{pk_{t1}^{(n)} - \mathrm{b}}{L} = \frac{\mathrm{t}_2}{\mathrm{t}_1} \quad (7)$$

$$pk_{t1}^{(n)} - \mathrm{b} = L\left(\frac{\mathrm{t}_2}{\mathrm{t}_1}\right) \quad (8)$$

By arranging the equation:

$$b = pk_{t1}^{(n)} - L\left(\frac{\mathrm{t}_2}{\mathrm{t}_1}\right) \quad (9)$$

$$\therefore L = pk_{t1}^{(n)} - b \quad (10)$$

$$\therefore b = pk_{t1}^{(n)} - b(\ pk_{t1}^{(n)} - b)\left(\frac{t_2}{t_1}\right) \quad (11)$$

Rearrange

$$b\left(1 - \frac{t_2}{t_1}\right) = pk_{t1}^{(n)} - pk_{t2}^{(n)}\frac{t_2}{t_1} \quad (12)$$

Where

$$b(t_1 - t_2) = pk_{t1}^{(n)} - pk_{t2}^{(n)} \quad (13)$$

$$b = \frac{pk_{t1}^{(n)} - pk_{t2}^{(n)}}{t_1 - t_2} \quad (14)$$

$$\therefore Y = \left(\frac{pk_{t2}^{(n)} - pk_{t1}^{(n)}}{t_2 - t_1}\right)\mathrm{t} + \left(\frac{pk_{t1}^{(n)}\mathrm{t}_1 - pk_{t2}^{(n)}t_2}{t_1 - t_2}\right) \quad (15)$$

Where :

$pk_{i1}^{(n)}$ and $pk_{i2}^{(n)}$ represent the max-min, lowest (highest) price and lowest (highest) cost are located value of product.

$t$ : represent the time in period.

$Y$ : the price in real time denoted as *Pt*.

## 4. Symmetric & Asymmetric Algorithms:

### 4.1 Symmetric Cryptography:

Encryption is symmetric and has a single key format known only by authorized parties to use it.The same suggested key is used for both encryption and decryption during the symmetric data encryption process.

- Similar cryptographic algorithms are still in use and the most common are DES, 3DES, AES, and RC4. 3DES and AES are used in IPsec and many other types of VPNs.
- Encryption algorithms Symmetric are fast, efficient, relatively uncomplicated, and easy to implement on non-expensive computers.
- However, they require all participants in the encryption process to actually create the secret key through actual participation in the implementation[14-16].

### 4.2 Asymmetric Cryptography:

In the asymmetric encryption process, a pair of keys is used. First, a public key called "public key" and the second key called "private key" or "secret key" approved only by the public key.

- In the asymmetric encryption process, the key used to encrypt and a different key is used to decrypt. If the owner is the one who encrypts, the user uses the encryption key and the recipient uses the public key in return to decrypt the message. If the owner is the recipient, the sender uses the public key for encryption, and the owner / recipient uses his own key to decrypt.The most common asymmetric encryption algorithm is RSA.
- Compared with symmetric encryption, asymmetric encryption has a large computational burden and is much slower. Therefore, it is not normally used to protect and maintain transferred data. Instead, it is powerful, since its ability to create a secure channel through an insecure satellite (for example, the Internet). This is done by switching public keys, which are used only for data encryption. The complementary private key, which was never shared, is used to decrypt [14-16].

## 5. Experimental Proof:

One of the main problems in economy was the problem of inflation in costs, a smart technique is proposed to normalize the cost. This is a proof to overcome the problem of inflation, as shown in the following proof.
Evaluating the cost and determining the range of length of Key, used in encryption.
Nomenclature:
max : maximum cost.
min: minimum cost.
S : Scale.
T: Trend.
L pub. :Length of public key.
L priv. :Length of private key.
Where Lpriv., denotes the length of key used in encryption as shown in reference.[12]

$$\min \le \mathrm{Lpriv.} \le \mathrm{S} + \max \quad (16)$$

Where S is the width of the scale of the length Kilo Line of Code.
N= max Length in Scale and S=N-min Length in scale.
In the same Steps in reference [12] the length of public key was counted as follow:

$$Lpub. = T\left(\frac{\max - \mathrm{cost}}{\max}\right) + \min \quad (17)$$

Where T denotes as:

$$\mathrm{T} = \max(\mathrm{Length\ pub.}) - \min(\mathrm{Length\ pub.}) \quad (18)$$

$$\therefore Length\ pub. = |Y| = \sqrt{\left(\frac{pk_{t2}^{(n)} - pk_{t1}^{(n)}}{t_2 - t_1}\right)^2 + \left(\frac{pk_{t1}^{(n)} - pk_{t2}^{(n)}}{t_1 - t_2}\right)^2} \quad (19)$$

Where *Y* denotes as *Pt.* , as shown in Equation (15).

This experiment demonstrated the equation that related to the length of the key with the cost of the data. In the previous search, the length of the key depended on the cost, but here two private and public keys have been made, and it was proved through experiment, that this method differs from the previous methods, as the encryption keys here are variable and not fixed, and this makes it difficult to guess and decipher the code, as well as by reading charts and graphs, the decoding time takes longer for the process of merging symmetric and asymmetric equations.

## 6. Evaluation of the experiment:

According to the mathematical experiment in section 5, the evaluation was measured based on the following:

## A-The Real Time of Encryption & Decryption:

This can be calculated based on the real time needed for encryption which included converting the plain text file into cipher text. The encryption process time used to find the throughput which indicated the computation cost and the encryption speed. The decryption process time was calculated by a time required for converting the cipher text back into plain text.

- Size of the keys used in this test started from the size of 128, 256, 512, 1024 and 2048 to encrypt text size 1KB, 100KB, 500KB, 1MB.
- A set of ciphering algorithms was used, in this experiment, RC5, AES, 3DES, MD5, RC5 + AES as symmetric algorithm and with RSA as asymmetric algorithm, combined between all these algorithms respectively, as an example to test the work activity of such a combination of Symmetric and Asymmetric algorithms.
- The results of the cost of encryption and decryption, using different kinds of symmetric asymmetric algorithms, and different sizes of texts and several sizes of keys, showed the trend line cost of encryption and decryption of the smallest key size with the largest key size that appeared in figure 5, to, 12, respectively.

The results appeared as follows:

Table 1.Using a 128-Bit key Length Encryption.

| Trend Line Cost | | | | |
|---|---|---|---|---|
| Key Length 2048 | 1KB | 100KB | 500KB | 1MB |
| RC5+RSA | 1.5924 | 1.404 | 1.512 | 0.22 |
| AES+RSA | 0.0896 | 0.1941 | 2.3172 | 1.1765 |
| 3DEA+RSA | 1.581 | 1.755 | 0.592 | 0.395 |
| MD5+RSA | 1.816 | 3.447 | 4.504 | 5.7 |
| RC5+AES+RSA | 1.581 | 1.755 | 2.992 | 0.395 |

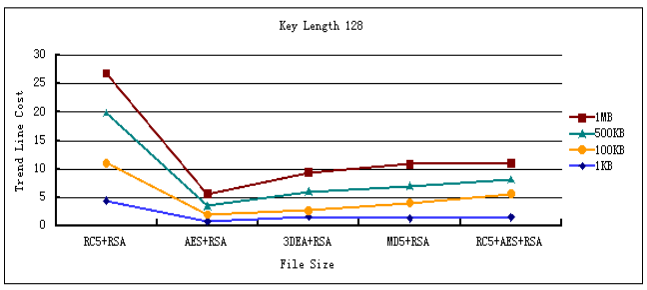


Figure 3. Trend Line Cost Using 128-Bit Key Length Encryption.

Table 2.Using a 2048-Bit key Length Encryption.

| Trend Line Cost | | | | |
|---|---|---|---|---|
| Key Length 2048 | 1KB | 100KB | 500KB | 1MB |
| RC5+RSA | 4.17 | 6.246 | 7.98 | 7.305 |
| AES+RSA | 0.745 | 1.0578 | 0.768 | 1.09 |
| 3DEA+RSA | 1.581 | 1.755 | 0.192 | 3.9545 |
| MD5+RSA | 1.816 | 2.247 | 2.104 | 3.825 |
| RC5+AES+RSA | 0.15 | 0.1755 | 0.0824 | 0.545 |

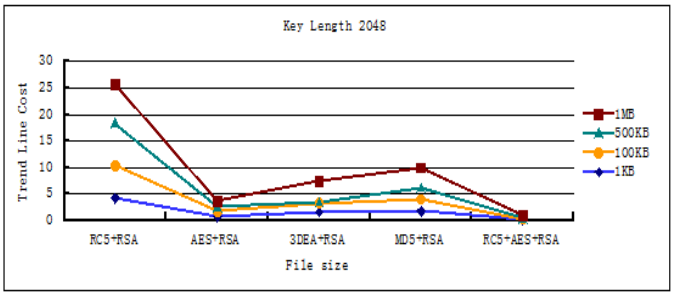


Figure 4. Trend Line Cost Using 2048-Bit Key Size Encryption process.

Table 3.Using 128-Bit key Length Decryption.

| Trend Line Cost | | | | |
|---|---|---|---|---|
| Key Length 128 | 1KB | 100KB | 500KB | 1MB |
| RC5+RSA | 4.4358 | 6.6435 | 8.7792 | 6.99 |
| AES+RSA | 0.8018 | 1.1925 | 1.5112 | 2.095 |
| 3DEA+RSA | 1.638 | 1.077 | 3.336 | 3.385 |
| MD5+RSA | 1.306 | 2.757 | 2.932 | 3.865 |
| RC5+AES+RSA | 1.532 | 4.077 | 2.536 | 2.885 |

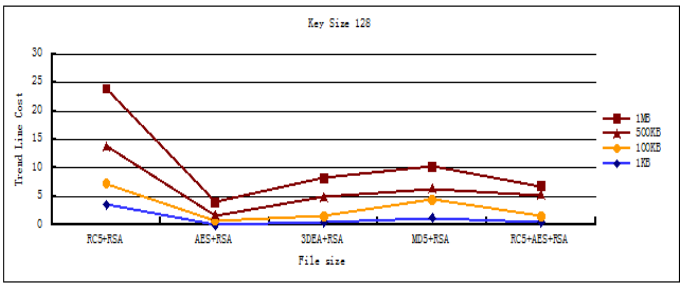


Figure 5.Trend cost Using 128-Bit Key Length Decryption.

Table 4.Using 2048-Bit key Length Decryption

| Trend Line Cost | | | | |
|---|---|---|---|---|
| Key Length 128 | 1KB | 100KB | 500KB | 1MB |
| RC5+RSA | 3.59 | 3.72 | 6.52 | 10.07 |
| AES+RSA | 0.0452 | 0.7761 | 0.8748 | 2.3135 |
| 3DEA+RSA | 0.468 | 1.077 | 3.336 | 3.385 |
| MD5+RSA | 1.31 | 3.1887 | 1.92 | 3.865 |
| RC5+AES+RSA | 0.468 | 1.077 | 3.7032 | 1.615 |

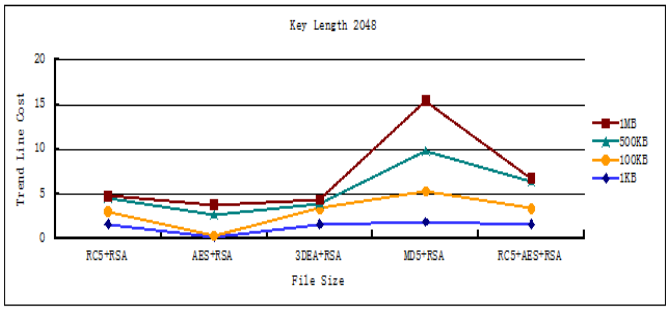


Figure 6. Trend Line cost Using 2048-Bit Key Length Decryption.

By reading and testing the results and figures, the encoding and decoding process for Symmetric Asymmetric algorithms trend line cost, the 128-bit key was easy but not fast. The encryption process took time between 1KB to 1MB key length, 4.4 ms, to 6.99 ms in RC5+RSA. In the case of operation process of symmetric Asymmetric algorithms, and the results above showed the encryption speed time for others combination algorithms and the differences between them. In the case of decryption, the process was changed in speed, and it took between 3.59 ms to 10.07 ms, for the same size of key length, which was expected.

In the decoding process, unusual status was noticed, during the use of decryption key at the size of 128 and 2048, where the trend line went downhill during the cost test converged only for one point for RC5+AES+RSA algorithms used in this test.

In figure3 and 4, using 128-2048 key length encryption, showed the activity of RC5+AES which started rising first and started down hall in RC5+AES+RSA in figure6, for all sizes in trend line cost calculation.

In figure5 and 6, using 128-2048 key length decryption, showed the activity of RC5+RSA and MD5+RSA started rising in many file sizes in trend line cost calculation.

**B-Machine operation:** this showed the CPU real time to process Kilo Line of Code, which includes the CPU size load and Battery power, the CPU Clock Cycle, was used during the encryption-decryption process.

**C-The size of plain text to be process:** It described the real file size, which was used during the test.

## 7. Conclusions:

This paper proposed a new way of calculating the variable in the key length in terms of time, based on the theory of market price movement in cloud computing where the computation cost of data encryption was calculated. The proposed system depended on the view that "the valuable things needed to be more secure and must be protected and maintained." Through the calculation, the dynamic arithmetic cost model was constructed using ambiguous rules based on the trend line rules cost of data. The computational cost of encryption and decryption was computed through the application and testing of a set of concurrent symmetric asymmetric encryption algorithms.

## Reference:

[1]Chandrakant D. Patel, Amip J.,Cost Model for Planning, Development and Operation of a Data Center Shah1 Internet Systems and Storage Laboratory HP Laboratories Palo Alto HPL-2005-107 (R.1) June 9,2005.

[2]M. Al-Roomi, Sh. Al-Ebrahim, S. Buqrais and I. Ahmad, Cloud Computing Pricing Models: A Survey, Inter. Journal of Grid and Distributed Computing Vol.6, No.5, pp.93-106, 2013.

[3]B. Sharma, R. K. Thulasiram, P. Thulasiraman, S. K. Garg and R. Buyya, Pricing Cloud Compute Commodities: A Novel Financial Economic Model, Proc. of IEEE/ACM Int. Symp. on Cluster, Cloud and Grid Computing, 2012.

[4]C. D. Patel and A. J. Shah, Cost model for planning, development and operation of a data center, hp technical report- hpl-2005-107(r.1), 2005.

[5]Pal, R. and Hui, P., Economic models for cloud service markets: Pricing and Capacity planning. Theoretical Computer Science 496, 113-124, July. 2013.

[6]W. Wang, P. Zhang, T. Lan and V. Aggarwal, Datacenter Net Profit Optimization with Individual Job Deadlines, Proc. Conference on Inform. Sciences and Systems 2012.

[7]C. S. Yeoa, S. Venugopalb, X. Chua and R. Buyyaa, Autonomic Metered Pricing for a Utility Computing Service, Future Generation Computer Syst., vol. 26, no. 8, 2010.

[8]M. Macias and J. Guitart, A Genetic Model for Pricing in Cloud Computing Markets, Proc. 26th Symp. of Applied Computing, 2011.

[9]H. Li, J. Liu and G. Tang, A Pricing Algorithm for Cloud Computing Resources, Proc. Int. Conference on Network Computing and Inform. Security, 2011.

[10]J. Jäätmaa, Financial aspects of cloud computing business models, Aalto University, master's thesis, 2010.

[11]ArtanM.,Isak S.,Besmir S., Prising Schemes in Cloud Computing:An Overview, International Journal of Advanced Computer Science and Applications, (IJACSA),Vol.7, No.2, 2016.

[12]Nazar.K.Khorsheed,Mohammad.A.El-Dosuky,Taher.T.Hamza,Mgdi. Z.Rashad, Management of data security based on Data cost Evaluation, Journal of Computational and Theoretical Nanoscience Vol. 14, 1–6, 2017.

[13]Li-Xin Wang, Dynamical Models of Stock Prices Based on Technical Trading Rules, IEEE Trans.on Fuzzy Systems 23(4):1127-1141,2015.

[14] Jan-Wouter Zwart, Asymmetric Merge, Michigan, Ann Arbor, July 6 2004.

[15]Serdar Dalkira, John W. Loganb, Robert T. Massonc, Mergers in symmetric and asymmetric noncooperative auction markets: the effects on prices and efficiency, International Journal of Industrial Organization,18 (2000) 383–413.

[16]David Pointcheval, Asymmetric Cryptography and Practical Security, journal of Telecommunications and Information Technology, 4/2002.