Asian Journal of Information Technology 15 (18): 3480-3486, 2016
ISSN: 1682-3915

Elliptic Curve Cryptography with Optimal Resource Allocation Schema for Security in Cloud Computing Environment

S. Rajalakshmi and R. Maguteeswaran
Jay Shriram Group of Institutions, Avinashipalayam, Tamil Nadu, India

Abstract: Cloud computing is a pristine methodology of computing in which dynamically scalable and often virtualized s are given as service over internet. Appropriation of cloud is a fascinating and yet unfamiliar province in cloud computing to imbrutes the miscellany of s for cloud purveyor becomes a challenging issue in recent years. This problem is solve by using three novel fashion for cloud purveyor with appropriation: Cloud-Dominant Strategy Incentive Compatible (C-DSIC), Cloud-Bayesian Incentive Compatible (C-BIC) and Cloud Optimal (C-OPT). In C-OPT modules where the administration is done based on host winner value, the major issue of the work is that corroboration is done for all cloud end user. To solve security issue problem in the cloud appropriation method in this effort introduce a novel Expectation Maximization (EM) algorithm for cloud optimal modules. The proposed EM methods are utilized for identifying maximum likelihood based on undiscovered dormant cloud artifice variables for virtual cost and quality of service curtailments. To corroborate the cloud end user data, cryptanalysis method is introduced in this proposed work. The proposed cryptanalysis method follows the procedure of Elliptic curve cryptography for corroborating end users and cloud purveyors. Key values between the cloud end user and cloud purveyors are exchanged. Each and every key is verified by both cloud end user and cloud purveyor. If the key value anyone becomes wrong the appropriation is not administrated to cloud end user, since these end users become uncorroborated end user, there are not allowed to perform appropriation process. A cloud negotiator with such an appropriation module enables end users to miscellany the miscellany of a cloud purveyor. Our demonstration indicates that the appropriation cost drops by calculation of the expectation maximization algorithm and more security than the existing C-OPT Methods by using the elliptic curve cryptography with multiplication in number of cloud purveyors irrespective of the fashions.

Key words: Cloud computing, fashion, cloud negotiator, appropriation, reverse demands, multi sign demands, Elliptic curve cryptography (ECC), Expectation maximization (EM)

INTRODUCTION

Cloud computing is a multiplicative accepted archetype of offering services over the internet (Mell and Grance, 2009). It is also an active province of research, and the popularity of this archetype is increasing rapidly. Many companies like Amazon, IBM, Google, sales force. com, Unisys and so on now offer cloud services. The main advantage of cloud computing is the ability to provision IT artifices on demand (thus avoiding the problems of over-provisioning and under-provisioning which are commonly seen with organizations that have widely variable requirements due to growth/shrinkage, seasonal peaks and valleys, etc). The artifices offered may include storage, CPU processing power, IT services and so on. These artifices are often geographically distant from end users.

Artifice appropriation of cloud artifices is a fascinating and yet unfamiliar province in cloud computing. Cloud purveyors follow a fixed pricing strategy for pricing their artifices and do not provide any incentive to their end users to adjust consumption patterns according to availability or other factors. The end user has to go through the specifications of each cloud purveyor to select the appropriate one, to obtain the service within budget and of the desired quality becomes also major challenge; security of the cloud computing during artifice appropriation process becomes also challenging issue.

Hence, economic models are more appropriate in the context of cloud services. An important feature of economic models is the distribution of incentives to bidders which are cloud purveyors in our domain. However, this means that cloud purveyors may not act

Corresponding Author: S. Rajalakshmi, Jay Shriram Group of Institutions, Avinashipalayam, Tamil Nadu, India

truthfully and may seek to maximize their incentives using improper behavior. Game-theoretic models cannot enforce the structure in games. Fashion design enables the social planner to design the game according to his wish. So, the social planner can implement strategies to motivate participants to act truthfully. The important contributions of this work are:

- Appropriation fashions for implementing dynamic pricing by proposing Expectation Maximization (EM) algorithm
- Novel appropriation module based on fashion design for a cloud negotiator (Grivas *et al*., 2010)
- Proposed ECC based security fashion between end user interface and corroboration manager

The appropriation module enables the cloud negotiator to imbrute artifice appropriation. In the appropriation module, the end user sends the specifications to the cloud negotiator and requests for artifice. The cloud negotiator sends the end user specification to all cloud purveyors. The cloud purveyors respond with cost and QoS parameters of their services. Do not consider implementation issues like caching, refresh and so on of cost and QoS by the negotiator. Expectation Maximization (EM) algorithm is an iterative method for finding maximum likelihood artifice appropriation results to estimates of cost and Quality of Service (QOS) parameters in statistical models where the model depends on unobserved cloud artifices.

The cloud negotiator assigns weights for different QoS parameters using Analytic Hierarchy Process (AHP) which are scaled before computing a weighted QoS score. This step is called normalization. If normalization is not done, then it is not possible to compare different QoS specifications. The cloud negotiator implements one of Cloud-Dominant Strategy Incentive Compatible (C-DSIC), Cloud-Bayesian Incentive Compatible (C-BIC) or Cloud-Optimal (C-OPT) fashions. The winner is determined based on the fashion implemented. The cloud negotiator notifies both winner and end user. Finally, the cloud negotiator pays money to the cloud purveyors according to the payment function of the fashion. This is called the appropriation cost.

Literature review: Compute artifices are the collection of Physical Machines (PMs), each comprised of one or more processors, memory, network interface and local I/O which together provide the computational capacity of a cloud environment. Typically PMs have deployed on them virtualization software that allows them host a number of Virtual Machines (Vms) that are isolated from each other and that may run different operating systems, platforms and applications. In the literature, most researchers model VMs and PMs as being curtailment by their processing capacity and memory availability. However, recent work (Mithani *et al*., 2010; Govindan *et al*., 2011) highlights the impact of contention between VMs caused for shared processor caches and other micro architectural artifices, suggesting that artifice management process may benefit from more detailed models of compute artifices.

The first is network chorography, the design of which significantly impacts performance and fault tolerance. Current data center network choreographies are based on hierarchical, tree-like choreographies similar to those used in early telephony networks, although a number of alternative choreographies including proposals based on hyper cubes (Guo *et al*., 2009) and randomized small-world choreographies (Shin *et al*., 2011) have emerged. In all cases a key goal is cubes and randomized small-world choreographies have emerged. In all cases a key goal is engineering a scalable chorography in which increasing the number of ports in the network should linearly increase the delivered bisection bandwidth. The second key aspect is more directly tied to artifice management: it is how to provide predictable latency and bandwidth in a data center network in the face of varying traffic patterns. Traditionally, the solution has been network over-provisioning but this is prohibitively expensive in large scale data centers and is inherently difficult due to lack of detailed traffic models. Given this, there has been a move towards implementing service differentiation via Quality-of-Service (QoS) policies that segregate traffic for performance isolation, so permitting high-level traffic engineering. A natural extension of this approach towards technologies enabling the virtualization of data center networks is currently gaining attention. Hence, appropriating artifices from the end users' perspective is an important and interesting issue.

The main strength of economic models is distributing incentives to the participants. But there are cases where the participants may not act truthfully. Hence, assume that cloud purveyors are selfish and rational. Also, the cloud negotiator performs reverse demands on behalf of the cloud end user. Prasad and Rao (2012) propose a artifice appropriation module for a cloud negotiator based on fashion design. This appropriation module enables the cloud negotiator to imbrute artifice appropriation in the cloud. The winner provides all the required artifices.

The scaling algorithm deployed in our work is the well known Combinatorial Demands Branch on Bids (CABOB). CABOB over other algorithms as it runs very fast and is scalable. CABOB uses Depth First Search (DFS) internally. Branch on Bids (BOB) is superior compared to Branch on Items (BOI) (Sandholm *et al*., 2005). The concepts of BOB and the internal working of CABOB are explained in the following sections. Since, CABOB is built on an incremental basis, it is very easy to process new requests of the end user as and when it comes compared to the other standard algorithms.

Sandholm (2002) serves as the first significant work on winner determination in combinatorial demands. Demands with multiple distinguishable items to be administrated but the techniques could also be used in the special case where some of the items are indistinguishable. These demands are complex in the general case where the bidders have preferences over bundles that is a bidder's valuation for a bundle of items need not equal the sum of his valuations of the individual items in the bundle.

He presents a generic algorithm that allows combinatorial demands to scale up to significantly larger numbers of items and bids than prior approaches to optimal winner determination (Chang *et al*., 2010), by capitalizing on the fact that the space of bids is sparsely populated in practice. This also presents the fact that basic combinatorial demands only allow bidders to express complementariness of items. Formulate demand for computing power and other artifices as a artifice administration problem with multiplicity where computations that have to be done concurrently are represented as tasks and a later task can reuse artifices released by an earlier task. It shows that finding a minimized administration is NP complete. This study presents an approximation algorithm with a proof of its approximation bound that can yield close to optimum solutions in polynomial time. Enterprise end users can exploit the solution to reduce the leasing cost and amortize the administration overhead. Cloud providers may utilize the solution to share their artifices among a larger number of end users.

Ismail *et al*. (2008) propose a formal model for evaluating formal analysis of artifice administration algorithms in grid computing. Shu uses a "quantum chromosomes" genetic algorithm to solve the problem of artifice administration in Grid. Based on artifice administration in grid computing, develop an optimization model and a Quantum Chromosomes Genetic Algorithm (QCGA) to effectively solve it. Li and Qi (2008) present a grid artifice administration algorithm based on fuzzy clustering. This algorithm assigns artifices based on task need and also performs reservation of the artifices. By this way, our algorithm can effectively avoid assigning powerful artifices to simple and medium scale tasks or assigning poor artifices to complex large scale tasks for they may lead to misuse of artifices and failure scheduling of tasks (Narahari *et al*., 2009). The presented algorithm has high efficiency and good robustness and works better than other similar algorithms.

MATERIALS AND METHODS

In game theory, assume that players are rational and have common knowledge and private information. Rationality implies that goal is to maximize payoff. In our model, cloud purveyors are rational. Hence, cloud purveyors are risk neutral. The concepts of risk neutral and quasi linear are described in detail elsewhere.

Each cloud end user has artifice requirements. The end users perform reverse demands for appropriating artifices. Cloud purveyors offer artifices but with varying costs and quality metrics. The goal of the cloud end user is to minimize the total cost of appropriating artifices without compromising quality of service. To minimize the appropriation cost, it is necessary for the cloud end user to know the real costs of cloud purveyors. A end user announces its specifications for desired artifices and quality of service to all cloud purveyors with the negotiator acting as a middleman. The cloud purveyors decide whether to participate in the demand based on the end user information and submit their bids to the negotiator. The negotiator aggregates the bidding information and selects the appropriate cloud purveyor. Cloud purveyors are rational and intelligent. Hence, one of them might bid with a false valuation to maximize its utility. The goal of providing incentives is to encourage truthful bidding.

The study presents a novel cloud artifice appropriation approach in this proposed work the cloud optimal modules artifices administrated based on the Expectation Maximization (EM) algorithm is an iterative method for finding maximum likelihood for virtual host winner value the virtual host winner value payment rule where the model depends on unobserved dormant cloud artifice variables. Expectation Maximization (EM) algorithm is an iterative method for finding maximum likelihood artifice appropriation results to estimates of cost and Quality of Service (QOS) parameters in statistical models where the model depends on unobserved cloud artifices.

Elliptic Curve Cryptography (ECC) is responsible for corroborating end users and cloud purveyors. In ECC methods they exchange the key values between the cloud end user and cloud purveyors. Each and every key is verified by both cloud end user and cloud purveyor. If the key value anyone becomes wrong the artifice appropriation is not administrated to cloud end user, since

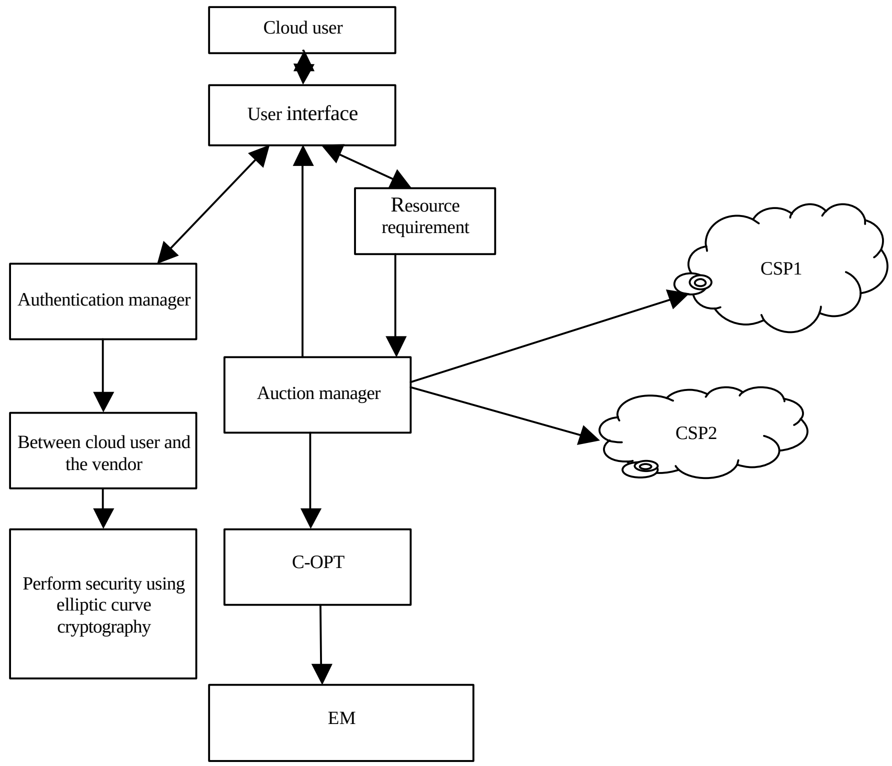

Fig. 1: Proposed architecture

these end users becomes uncorroborated end user, there are not allowed to done artifice appropriation process. A cloud negotiator with such a appropriation module enables end users to imbrute the choice of a cloud purvey or among many with diverse offerings and is also an essential first step toward implementing dynamic pricing in the cloud. The proposed architecture representation is shown in Fig. 1.

Appropriation demand using expectation maximization: Cloud purveyors are represented by $M = \{1, 2, ..\}$ in this appropriation demand, each cloud purveyor responds by bidding with total cost and promised QoS parameters. These parameters are converted into numbers using the technique presented in the previous section. Hence, the bid is an ordered pair (c_i, q_i). Each cloud purveyor $i \in M$ has execution cost where 0 and QoS where $0<q_i$. Let be the lowest cost valuation and the highest cost valuation. The cloud purveyor's cost is always in the interval $[\underline{c}, \overline{c}]$, i.e., $\underline{c} \leq c_i \leq \overline{c}$. Similarly, let be the lowest QoS value and the highest QoS value. The cloud purveyor's QoS is always in the interval $[\underline{q}, \overline{q}]$ i.e., $\underline{q} \leq q_i \leq \overline{q}$, this information is private to the cloud purveyor. Let be the set of all possible true types of the cloud purveyor and $\theta_i = [\underline{c}, \overline{c}] \times [\underline{q}, \overline{q}]$. Let $\theta = \theta_1 \times \theta_2 \times ... \times \theta_n$. Assume that cost and QoS are correlated. Hence, there is a joint distribution function of cost and QoS represented by. Then, assume that the joint distribution function is the same for all n cloud purveyors, i.e., $\Phi_1 = \Phi_2 =..= \Phi_n$. Hence, all cloud purveyors are symmetric.

Given a statistical model consisting of a set of observed cloud purveyor artifices in terms of cost and quality of service and a vector of unknown artifices appropriation results as along with a likelihood function $L(\theta, c, Q) = P(c, q|\theta)$, the Maximum Likelihood Estimate (MLE) of the unknown parameters is determined by the marginal likelihood of the Maximum Likelihood Estimate (MLE) of the unknown parameters is determined by the marginal likelihood of the observed data:

$$L(\theta, c) = P(c|\theta) \tag{1}$$

The EM algorithm seeks to find the MLE of the marginal likelihood by iteratively applying the following two steps. Expectation step (E step): calculate the expected value artifice appropriation value for cloud purveyors of the log likelihood function with respect to the conditional distribution of QOS under the current estimate of the artifice appropriation results:

$$Q\left(c\,|\theta^{((t))}\right) = E_{Q|c,\,\theta^{((t))}}\left[\log L\left(\theta, c, q\right)\right] \quad (2)$$

Maximization step (M step): find the parameter that maximizes this quantity:

$$\theta^{(t+1)} = \underset{\theta}{\operatorname{argmax}}\; Q\left(\theta|\theta^{(t)}\right) \quad (3)$$

If know the value of the artifice appropriations results can usually find the artifice appropriation value for cloud purveyors QOS Q by maximizing the log-likelihood over all possible values of quality of service q, either simply by iterating over. Conversely, if know the values of quality of service q, can find the estimate artifice appropriation value for cloud purveyors of the parameters fairly easily, typically by simply grouping the observed data points according to the value of the associated dormant variable. This suggests an iterative algorithm in the case where both and are unknown:

- First, initialize the artifice appropriation results parameters to some random selected cloud purveyors
- Compute the best QOS artifice appropriation value for given artifice appropriation results parameters
- Then, use the just-computed values of q to compute a better estimate for the parameters. Parameters associated with a particular quality of the service requirement QOS value
- Iterate steps 2 and 3 until convergence

Elliptic curve cryptography based enabled security: To an arbitrary pair of elliptic curve points specified by their affine coordinates $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, the group operation assigns a third point $R = P\times Q$ with the coordinates (x_3, y_3). Given such a curve E, the cryptographic group of the cloud end user and cloud purveyor that is employed in protocols is a large prime-order subgroup of the group $E(F_p)$ of rational points on E. The group of cloud end user and cloud purveyor rational points consists of all solutions $(x; y)\in F_p^2$ to the curve equation together with a point at infinity, the neutral element. The number of rational points is denoted by $\#E(F_p)$ and the prime order of the subgroup by a fixed generator of the cyclic subgroup is usually called the base point and denoted by $G\in E(F_p)$.

Elliptic curve public-key pairs: Given a set of cloud end user and cloud purveyor domain parameters that include a choice of base field prime, an elliptic curve and a base point of order on an elliptic curve key pair consists of a private key for each cloud end user and cloud purveyor which is a randomly selected non-zero integer modulo the group order and a public key for cloud end user and cloud purveyor is defined as the d-multiple of the base point. Thus, the point is a randomly selected point in the group generated by F.

Elliptic curve key exchange: Diffie-Hellman protocol is used here to exchange the key values between one cloud end user to another cloud purveyor based on the following key pairs (d_a, Q_a) and (d_b, Q_b). They then exchange the public keys Q_a and Q_b such that each can compute the point $P = d_aQ_B = d_BQ_a)$ using their respective private key. The shared secret key is derived from by a key derivation function, generally being applied to its x-coordinate. In this phase the signer generates a key pair (d, Q) consisting of a private signing key and a public verification key Q = dF. To sign a message m, the signer first chooses a per-message random integer i such that $1\leq i\leq n-1$, computes the point $(x_1; y_1) = k_G$, transforms to an integer and computes $r = x_1 \bmod n$. The message is hashed to a bit string of length no more than the bit length of n which is then transformed to an integer.

The signature of m is the pair (r; s) of integers modulo n where $= k^{-1}(e+dr) \bmod n$. Note that r and s need to be different from 0 and k must not be revealed and must be a per-message secret which means that it must not be used for more than one message. It is important that the per-message secret k is not revealed, since otherwise the secret signing key j can be computed by $j = r^{-1}(ks-e) \pmod n$ because r and s are given in the signature and e can be computed from the signed message. Even if only several consecutive bits of the per-message secrets for a certain number of signatures are known, it is possible to compute the private key. Also, if the same value for k is used to sign two different messages and using the same signing key d and producing signatures (r, s_1) and (r, s_2) then k can be easily computed as $k \equiv (s_2-s_1)^{-1}(e_1-e_2) \pmod n$ which then allows recovery of the secret key.

RESULTS AND DISCUSSION

Currently, the miscellany of a cloud purveyor is manual. The miscellany of a cloud purveyor with low cost is also acceptably called the first price demand. Similarly, a end user can perform a Vickrey demand and pay the second-lowest cost to the winner.

In the real world, cloud purveyors follow different price distributions. In this kind of scenario, the winner determination and appropriation cost computation using first-price and Vickrey demands is not optimal. Hence, this approach should not be followed in the real world. It may be noted that if we do not use fashion design, would need to use standard demands like first bid, second bid and so

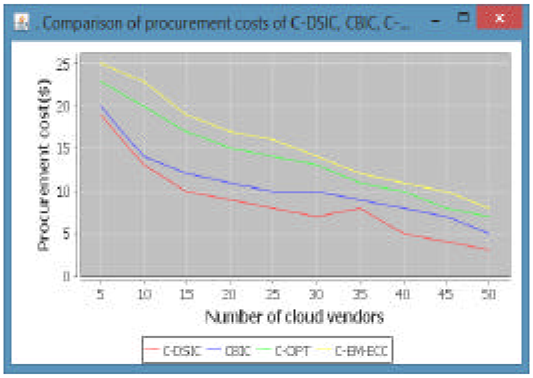

Fig. 2: Comparison of appropriation costs of C-DSIC, CBIC, C-OPT and C-EM-ECC in Scenario 1

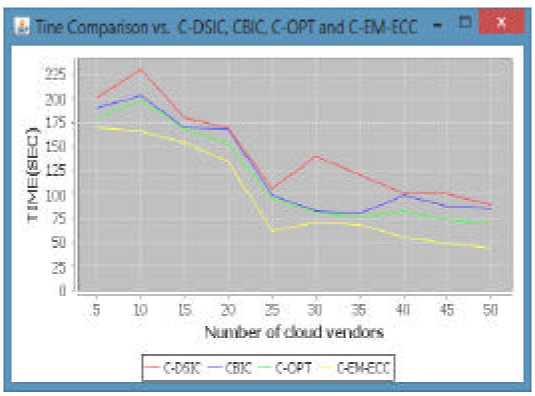

Fig. 3: Comparison of appropriation costs of C-DSIC, CBIC, C-OPT and C-EM-ECC in Scenario 2

on. However, cannot enforce truthfulness simply using demands. Truthfulness cannot be measured. Hence, there is no other baseline to compare our models.

Currently, the miscellany of a cloud purveyor is manual. The miscellany of a cloud purveyor with low cost is also acceptably called the first price demand. Costs and tasks are uniformly distributed. The average appropriation cost is calculated in every fashion and compared.

In Fig. 2, the x-axis scale is with one unit length representing 100 cloud purveyors in scenario 1. The performance comparison results of the proposed EM based cloud appropriation artifices administration performs best than existing appropriation cost to the end user in C-DSIC, C-BIC and C-OPT for different number of cloud purveyors. Since, proposed work calculates the cloud artifice appropriation based on the probability values and more secure by proposing ECC cryptography methods in corroboration manager phase.

The minimum number of cloud purveyors is taken to be 10 similarly, also is the case with Fig. 3 shows the

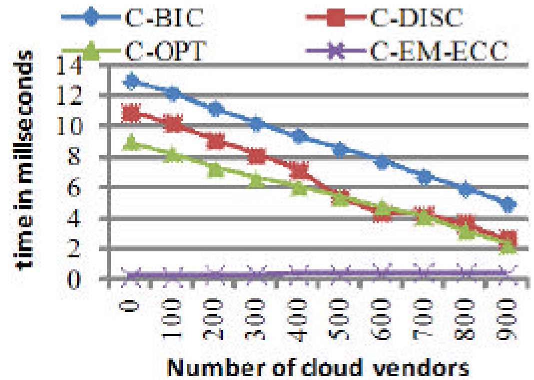

Fig. 4: Time Comparison vs. C-DSIC, CBIC, C-OPT and C-EM-ECC

graph of appropriation costs in C-DSIC, C-BIC, C-OPT and C-EM-ECC for different number of cloud purveyors in Scenario 2.

Time comparison results of the existing methods and proposed methods results are shown in Fig. 3. It shows that the proposed C-EM-ECC shows have less time for different number of cloud purveyors and it is compared with existing C-DSIC, CBIC and C-OPT methods.

CONCLUSION

Currently, the cloud end user pays a fixed price for artifices or services. This type of pricing is called fixed pricing. Fixed pricing is very accepted with telecom providers. On the flip side, there is no provision for incentives for end users in the fixed strategy. Artifice Appropriation is not only an important problem in cloud computing but is also an unfamiliar province. Currently, artifice appropriation is done manually and there is a pressing need to imbrute it. To imbrute appropriation, three fashions are used: C-DSIC, C-BIC and C-OPT. C-DSIC are a low bid Vickrey demand. It is allocate efficient and individual rational but not budget balanced. If the fashion is not budget balanced, then an external agency has to provide money to perform appropriation. In cloud artifice appropriation module still the miscellany of the optimal cloud artifices becomes difficult and security based fashion is not done in this research. In order to overcome these problem in our work proposed a artifice appropriation module based on the expectation maximization algorithm between the cost and QOS in the cloud purveyor for cloud computing environment. The proposed EM algorithm finding maximum likelihood for cost and QOS where the model depends on unobserved dormant cloud artifice variables. To perform QOS where the model depends on unobserved dormant cloud artifice variables. To perform the security process in efficient manner proposed Elliptic Curve Cryptography (ECC) is responsible for corroborating end users and cloud purveyors. In ECC methods they exchange the key values between the cloud end user and cloud purveyors without loss of the cloud data in the cloud computing environment. The experiments reveal an interesting pattern. The artifice appropriation cost reduces as the number of cloud purveyors increase, irrespective of the fashion implemented. The cost in CEM reduces more significantly, compared to the other two fashions.

The major issue of the present ECC methods it doesn't not stem from a weakness in the underlying hardness assumption but rather from implementation issues such as side-channel attacks, software bugs or design flaws In the current work artifice appropriation modules doesn't consider the following features such as caching and the refresh. After determining optimal integration of artifices appropriation based on mathematical models, these methods is applied to any type of real cloud related artifice appropriation application along with efficient secure fashion identified based on calculated optimal integration.

REFERENCES

Chang, F., J. Ren and R. Viswanathan, 2010. Optimal resource allocation in clouds. Proceedings of the IEEE 3rd International Conference on Cloud Computing, July 5-10, 2010, Miami, FL., USA., pp: 418-425.

Govindan, S., J. Liu, A. Kansal and A. Sivasubramaniam, 2011. Cuanta: Quantifying effects of shared on-chip resource interference for consolidated virtual machines. Proceedings of the 2nd ACM Symposium on Cloud Computing, October 26-28, 2011, ACM, Cascais, Portugal, ISBN:978-1-4503-0976-9, pp: 1-22.

Grivas, S.G., T.U. Kumar and H. Wache, 2010. Cloud broker: Bringing intelligence into the cloud. Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, July 5-10, 2010, IEEE, New York, USA., ISBN:978-1-4244-8207-8, pp: 544-545.

Guo, C., G. Lu, D. Li, X. Zhang and Y. Shi *et al*., 2009. BCube: A high performance, server-centric network architecture for modular data centers. Proceedings of the ACM SIGCOMM Computer Communication Review, August 17-21, 2009, Barcelona, Spain, pp: 63-74.

Ismail, L., B. Mills and A. Hennebelle, 2008. A formal model of dynamic resource allocation in grid computing environment. Proceedings of the Ninth ACIS International Conference on Software Engineering Artificial Intelligence Networking and Parallel-Distributed Computing (SNPD'08), August 6-8, 2008, IEEE, New York, USA., ISBN:978-0-7695-3263-9, pp: 685-693.

Li, F. and D. Qi, 2008. Research on grid resource allocation algorithm based on fuzzy clustering. Proceedings of the 2008 Second International Conference on Future Generation Communication and Networking, Vol. 2, December 13-15, 2008, IEEE, Guangzhou, China, ISBN:978-0-7695-3431-2, pp: 162-166.

Mell, P. and T. Grance, 2009. The NIST definition of cloud computing NIST special publication 800-145. Nat Inst. Standards Technol. US. Dept. Commerce, 53: 1-50.

Mithani, M.F., M. Salsburg and S. Rao, 2010. A decision support system for moving workloads to public clouds. GSTF Intl. J. Comput., 1: 150-157.

Narahari, Y. D. Garg, R. Narayanam and H. Prakash, 2009. Game Theoretic Problems in Network Economics and Mechanism Design Solutions. Springer, Bangalore, India, ISBN:978-1-84800-937-0, Pages: 274.

Prasad, A.S. and S. Rao, 2012. A mechanism design approach to resource procurement in cloud computing. IEEE. Trans. Comput., 63: 17-30.

Sandholm, T., 2002. Algorithm for optimal winner determination in combinatorial auctions. Artificial Intell., 135: 1-54.

Sandholm, T., S. Suri, A. Gilpin and D. Levine, 2005. CABOB: A fast optimal algorithm for winner determination in combinatorial auctions. Manage. Sci., 51: 374-390.

Shin, J.Y., B. Wong and E.G. Sirer, 2011. Small-world datacenters. Proceedings of the 2nd ACM Symposium on Cloud Computing, October 26-28, 2011, ACM, Cascais, Portugalp, ISBN: 978-1-4503-0976-9, pp: 1-2.