ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 9, SEPTEMBER 2015, PP 570-574

Performance and Cost Evaluation of Adaptive Architecture with dual Layer Encryption

[1]Barma Udayashanth Kumar,[2] N.Poorna Chandra Rao,[3]Dr.S.Prem Kumar
[1](M.Tech), CSE
[2]Assistant Professor, Department of Computer Science and Engineering
[3]Professor & HOD, Department of computer science and engineering,
G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract: Cloud Computing is a developing service situated space which performs Primitive services as IaaS,PaaS and SaaS alongside A Cloud database management system framework (CDBMS) is an appropriated database that conveys registering as an service rather than an item is called as DBaaS (Database as an Service) . Enhancing classification of data put away in cloud database it is a critical commitment to cloud database. Information encryption is the ideal answer for accomplishing classification. In some local technique, encode the entire database through some standard encryption calculation that not permits the any sql operation specifically on the cloud. This formal arrangement influenced by workload and expense would make the cloud database service badly designed. We propose a novel Adaptable architecture for encryption of open cloud database as autonomous encryption architecture which performs double layer encryption keeping in mind the end goal to secure Cloud database too client protection with information honesty. Versatile encryption permits any sql operation over encoded information. The novel cloud database architecture that uses versatile encryption strategy with no transitional servers. This plan gives cloud supplier the best level of secrecy for any database workload. We can focus the encryption and versatile encryption expense of information secrecy from the exploration perspective.

Keywords: Symmetric encryption, Adaptive Architecture, double layer encryption ,DBaaS.

1. INTRODUCTION

The cloud computing worldview is effectively joining as the fifth utility [1], yet this positive pattern is halfway constrained by worries about data classification [2] and indistinct costs over a medium-long term [3], [4]. We are occupied with the Database as a Service worldview (DBaaS) [5] that represents a few exploration challenges in terms of security and expense assessment from a rental service perspective. Most results concerning encryption for cloud-based services [6], [7] are unessential to the database worldview. Other encryption plans, which permit the execution of SQL operations over encoded information, either experience the ill effects of execution points of confinement (e.g., [8]) or they require the decision of which encryption plan must be embraced for every database segment and SQL operations (e.g., [9]). These last recommendations are fine when the arrangement of inquiries can be statically determined at configuration time, while in this paper we are intrigued to other regular situations where the workload may change after the database outline. In this paper, we propose a novel architecture for versatile encryption of open cloud databases that offers an intermediary free different option for the framework proposed in [10]. The proposed architecture ensures in a versatile way the best level of information secrecy for any database workload, notwithstanding when the arrangement of SQL questions powerfully changes. The versatile encryption plan, which was at first proposed for applications not alluding to the cloud, encodes every plain section into numerous scrambled segments, and every worth is embodied into diverse layers of encryption so that the external layers ensure higher privacy however bolster less calculation abilities as for the internal layers. The external layers are progressively it adjusted at runtime when new SQL operations are added to the workload. In spite of the fact that this versatile encryption architecture is appealing on the grounds that it doesn't oblige characterizing at outline time which database operations are permitted on every segment, it postures novel issues in terms of achievability in a cloud setting, and stockpiling and system costs estimation.

In this paper, we examine each of these issues and we achieve unique conclusions in terms of model usage, execution assessment, and expense assessment. We execute the first intermediary free architecture for versatile encryption of cloud databases. It doesn't restrict the accessibility, versatility and adaptability of a plain cloud database; on the grounds that simultaneous customers can issue parallel operations without going through some brought together part as in option architectures [10]. Additionally, we propose the first logical expense estimation model for assessing cloud database costs in plain and encoded examples from an inhabitant's perspective in a medium-term period. It considers likewise the variability of cloud costs and the likelihood that the database workload may change amid the assessment period. This model is instanced as for a few cloud suppliers offers and related genuine costs. Of course, versatile encryption impacts the costs identified with capacity size and system use of a database service. Be that as it may, it is critical that an inhabitant can suspect the last costs in its time of interest, and can pick the best trade off between information privacy and costs.

2. LITERATURE REVIEW

Hong-Linh Truong and SchahramDustdar: have done experiment by taking few scientific applications and they are only talking about the cost of different components associated with computing environment and most important challenges are to discuss only costs associated with application executions. While cloud service providers give some basic tools for determining computation and data transfer costs, they are trivial. On their work they do not perform the performance prediction but provided a tool for scientists to define the dependency and estimated metrics for their applications based on that the cost is being estimated. Thus, the accuracy of the cost estimation is dependent on scientist knowledge, and this accuracy quality can be improved if our service can also be well integrated with existing performance prediction tools.

ZuzanaKristekova at.al [7] suggested to design and develop a simulation model which covers the system dynamic aspect and supports decision makers to analyze costbenefits over cloud computing versus own datacenter [7]. Basically one important thing is for service providers whether it is more economical to move the existing datacenter-hosted services to the cloud or to keep them in the datacenter [7]. This means, that one of the service provider´s primarycriterion for such a decision is costs.In practice, some models exists that support organizations in analyzing and comparing costs, such as “Amazon Simple Monthly Calculator”.Amazon Simply Monthly calculatoris a static and do not consider the dynamics of cost development by using cloud computing [8]. To overcome this problem they develop one simulation model, which covers the dynamics of cost development and assists decision makers by analyzing cost benefits associated with cloud computing and own data center. On the other hand the model is based on ‘System Dynamic’ approach [7] [8]. System dynamics is useful for identifying key decision factors and relationship between them and helps to perform decision making in a more efficient way. System Dynamics is a simulation methodology for modeling dynamic and complex system [7].

3. RELATED WORK:

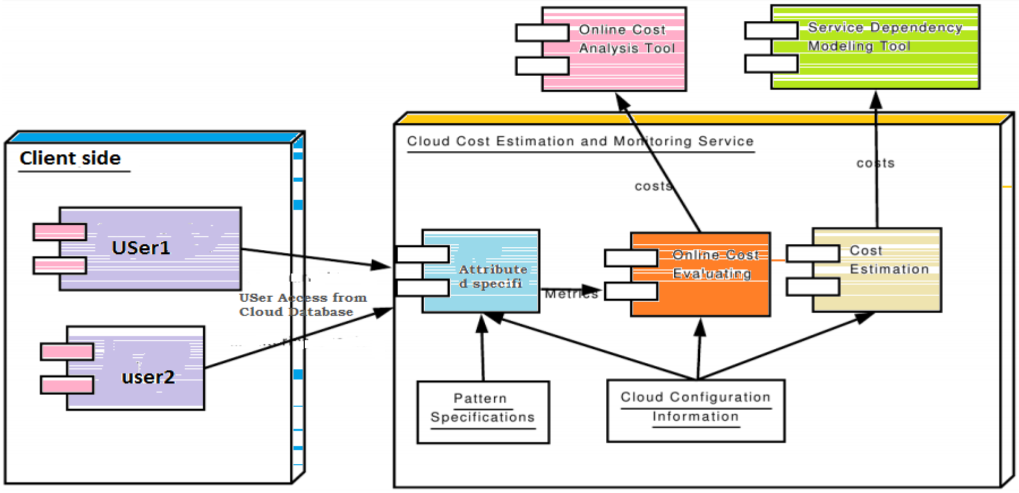


Fig 1.Cloud Cost estimation and Monitoring Service Model

Client Side: Where in the cloud estimation cloud database will be evaluated using cost estimation tools measurements where a client can invoke the cloud data based on some sort of specific attributes , here client need to match with the cloud data specific attributes. In the front end, cloud system acts as the source of information, it collects the information and sends to back end which is nothing but our CCEMSM. CCEMSM connected with online cost analysis tool and service dependency monitoring tool to get the approx cost of the resources used.

Application monitoring sensors:- These sensors collect the data from different PCs or server, relating to each machines performance as well as the performance of applications running on the machines.

Application trace extraction tool:- You can use this tool to verify the flow of logic or to identify bottlenecks within transaction programs. End to End Application Tracing can identify the source of an excessive workload, such as a high load SQL statement, by client identifier, service, module, action, session, an instance. This isolates the problem to a specific user, service, session, or application component.

Online cost analysis tool:- For monitoring and analyzing the cost, data we need to collect is execution time, machine name, data transfer size, data transfer source and destination. This work can be done by different instrumentation techniques, one of them are inserting probes in the beginning and end of the data transfer, application processes, MPI calls and workflows.

Service dependency modeling tool:- This tool keeps the information of dependency among part of applications, computational resources and storages. Mainly 3 types of dependencies are supported: data, control and resource dependency. After getting the data from the application, it keeps checking the dependency tree and generates the events to be sent back to the “cost estimation component”.

4. SYSTEM MODEL

PRESENTED SYSTEM:

With Our presented System, there is no adaptive encryption architecture in order to perform data integrity and improve system performance to wards to complete the computation in estimated cost. our presented system has lack of security it means no privacy for user data which are stored at cloud database, who can access the data from Cloud data base by performing SQL operations without decrypting the data they can invoke the cloud database service due to lack of fine grained access control In this connection our presented system fails in providing security, confidentiality, data integrity and improves the system performance in order to achieve adaptive encryption architecture.

PROPOSED SYSTEM

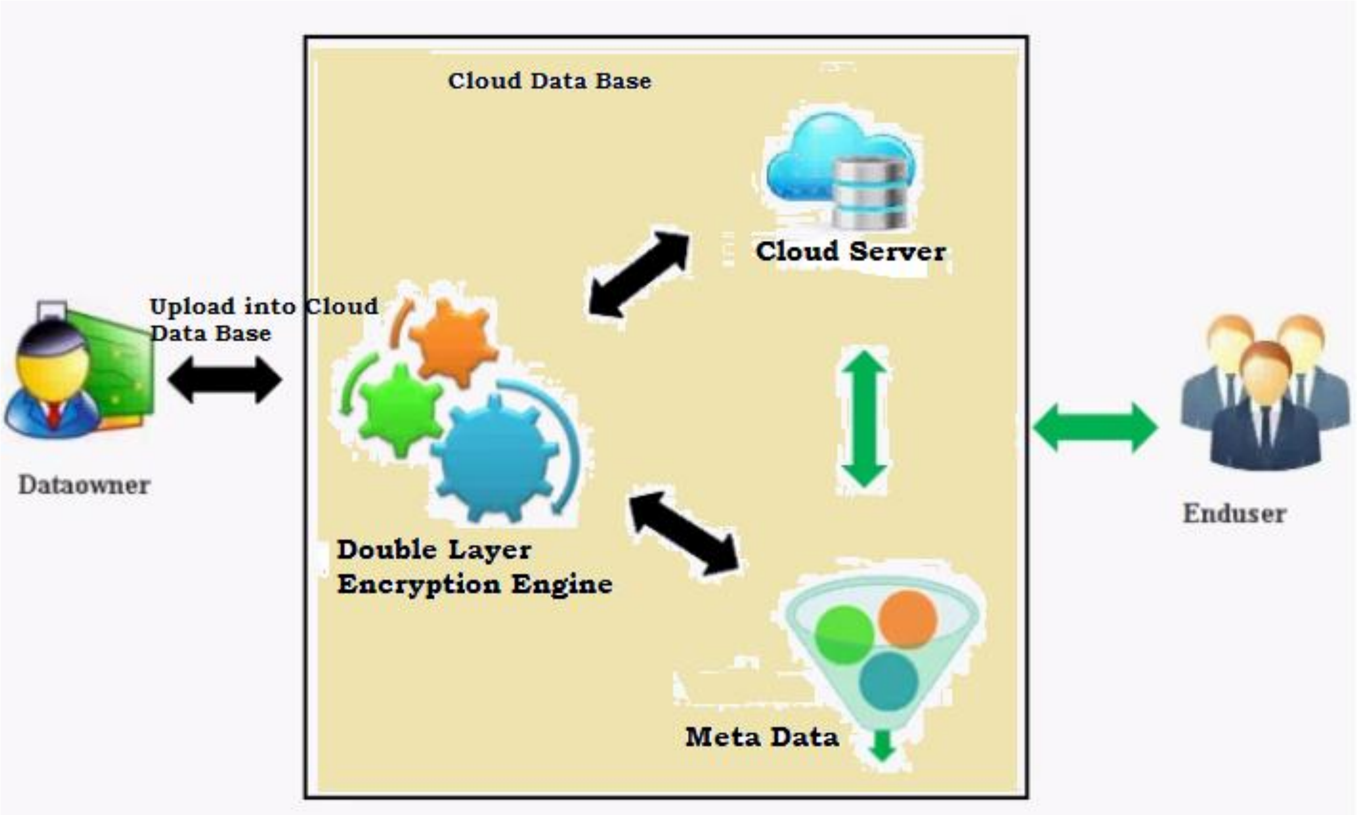
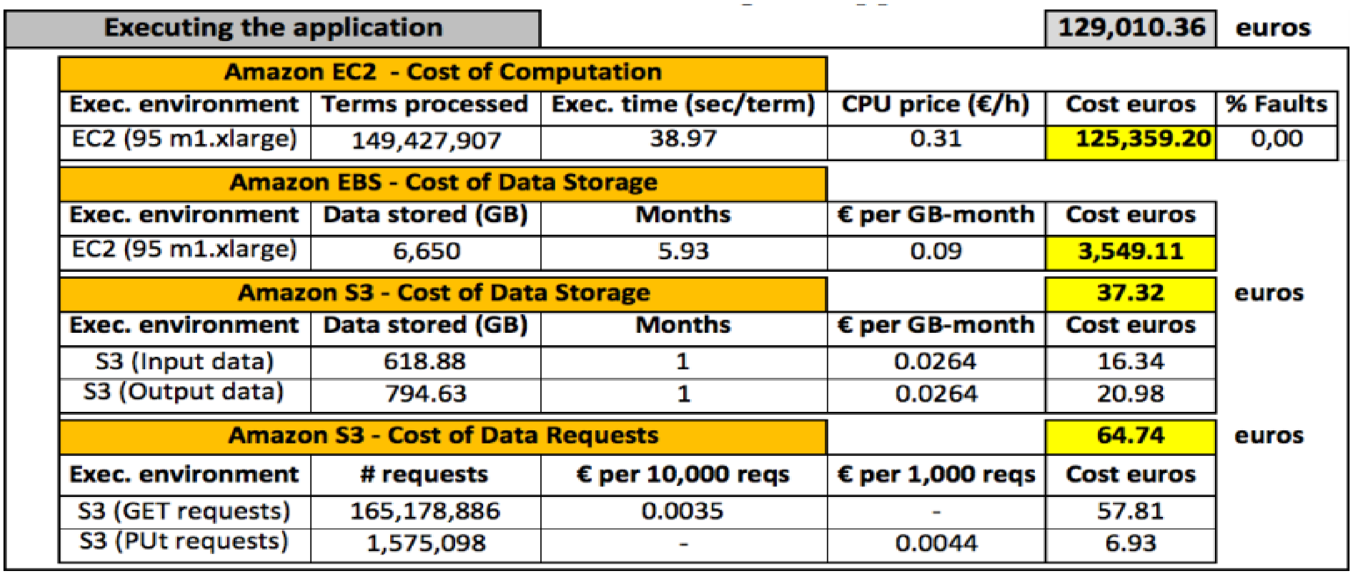


Fig 2. Proposed System Architecture

Where in the Proposed System Data owner can upload data in to Cloud database, as a owner before to upload the data he need to register with policy as Small or Medium or Long And also provide specific attributes as access policy in order to restrict access from un authorized users , soon after getting registration with cloud server , owner can upload double layer encrypted files in to cloud database , as a cloud server can't read that file , data will be available as encrypted formatted as cipher text. So by providing double layer encryption it doesn't allow to read and write to the cloud service providers.When a user want to access cloud database data , he need to be match with access policy with data owner in terms of tenet policy in order to access the data. In this regards we used Blow fish encryption algorithms for layer-1 Encryption and SHA-1 (Secured Hashing Algorithm) is used for 2-layer encryption.



Executing the application				129,010.36	euros
Amazon EC2 - Cost of Computation					
Exec. environment	Terms processed	Exec. time (sec/term)	CPU price (€/h)	Cost euros	% Faults
EC2 (95 m1.xlarge)	149,427,907	38.97	0.31	125,359.20	0,00
Amazon EBS - Cost of Data Storage					
Exec. environment	Data stored (GB)	Months	€ per GB-month	Cost euros	
EC2 (95 m1.xlarge)	6,650	5.93	0.09	3,549.11	
Amazon S3 - Cost of Data Storage				37.32	euros
Exec. environment	Data stored (GB)	Months	€ per GB-month	Cost euros	
S3 (Input data)	618.88	1	0.0264	16.34	
S3 (Output data)	794.63	1	0.0264	20.98	
Amazon S3 - Cost of Data Requests				64.74	euros
Exec. environment	# requests	€ per 10,000 reqs	€ per 1,000 reqs	Cost euros	
S3 (GET requests)	165,178,886	0.0035	-	57.81	
S3 (PUt requests)	1,575,098	-	0.0044	6.93	

Fig 3. Policy Selection for Adaptive architecture

METADATA include all information that allows a legitimate client knowing the master key to execute SQL operations over an encrypted database. They are organized and stored at a table-level granularity to reduce communication overhead for retrieval, and to improve management of concurrent SQL operations. We define all metadata information associated to a table as table metadata. Let us describe the structure of a table metadata .Table metadata includes the correspondence between the plain table name and the encrypted table name because each encrypted table name is randomly generated. Moreover, for each column of the original plain table it also includes a column metadata parameter containing the name and the data type of the corresponding plain column (e.g., integer, string, timestamp). Each column metadata is associated to one or more onion metadata, as many as the number of onions related to the column.

COST ESTIMATION OF CLOUD DATABASE SERVICES:

A tenant that is interested in estimating the cost of porting its database to a cloud platform. This porting is a strategic decision that must evaluate confidentiality issues and the related costs over a medium-long term. For these reasons, we propose a model that includes the overhead of encryption schemes and variability of database workload and cloud prices. The proposed model is general enough to be applied to the most popular cloud database services, such as Amazon Relational Database Service.

COST MODEL:

The cost of a cloud database service can be estimated as a function of three main parameters:
Cost = f(T ime, Pricing,Usage) where:

- Time: identifies the time interval T for which the tenant requires the service.
- Pricing: refers to the prices of the cloud provider for subscription and resource usage; they typically tend to diminish during T .
- Usage: denotes the total amount of resources used by the tenant; it typically increases during T .In order to detail the pricing attribute, it is important to specify that cloud providers adopt two subscription

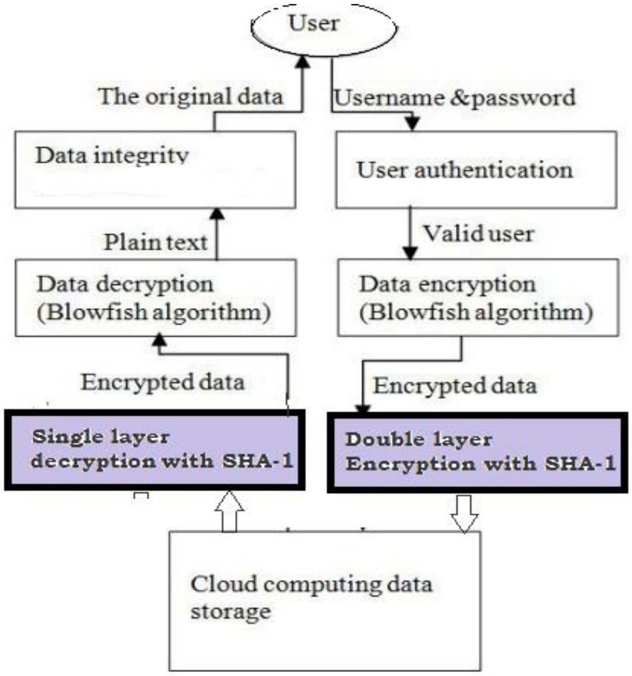

User
The original data
Username &password
Data integrity
User authentication
Plain text
Valid user
Data decryption (Blowfish algorithm)
Data encryption (Blowfish algorithm)
Encrypted data
Encrypted data
Single layer decryption with SHA-1
Double layer Encryption with SHA-1
Cloud computing data storage

Fig 4. Data encryption and Decryption using symmetric algorithms

Authentication method:

Username and password used for authentication process.

Encryption operation:

Blowfish encryption algorithm is used for exchanging information or data for its superiority in terms of the processing time, and no attack is known to be successful against this. Blowfish algorithm used for encryption and decryption operations. The file sent to the cloud computing data store and stored in fully encrypted form and nobody can decrypt it without having the key. And when the encrypted file is uploaded for storing to the cloud data store, the key and the path of the encrypted file along with the user account is kept and maintained in the database table on the cloud data store.

Decryption operation:

In the proposed model Blowfish algorithm is used for the decryption operation, whenever the user requests for a file the file moves from the cloud to the user in encrypted form and after receiving an encrypted file from the cloud, the file decrypted with Blowfish algorithm using the same key that used in the encryption operation. Data integrity operation: In the proposed model SHA-1 cryptographic hash algorithm is used for the integrity operation, SHA-1 is that this method is a one way system and unbreakable.

Challenges of data encryption

Despite the benefits and applications of encryption method in safe guarding cloud database, various reasons have hindered the deployment and sending data to the cloud. These factors include, performance impacts, difficulty in performing query over the encrypted data, key management issue, requirements of changes in data application, and data availability. [11].

Solutions to the challenges of data encryption:

Solutions to these challenges are provided based on the priority to the cloud data.

Query performance:

Execution of query over an encrypted data have been provided with various proposed techniques such as Aggregation queries-partial and fully Homomorphic encryption, Range queries, trusted computing, cipher base and secure server [12], [1] and [4]. A profound flexible and reliable security solution to an encrypted data in the cloud according to [16] is the database should be worked in its encrypted form in the cloud without decrypting in the cloud. This approach would disallow the service provider to know the contents and query processing.

Key management:

According to (RSA Security) key management issue in database encryption can be solved using external Hardware Security Module or Wallet. The function of Wallet is to store, manage and protect the

5. CONCLUSION:

In this paper we reveal how secure a proposed novel Adaptable architecture for encryption of open cloud database as autonomous encryption architecture which performs double layer encryption keeping in mind the end goal to ensure Cloud database also client protection with information uprightness. Versatile encryption permits any sql operation over encoded information. The novel cloud database architecture that uses versatile encryption system with no intermediate servers. This plan furnishes cloud supplier with the best level of classification for any database workload. We can determine the encryption and versatile encryption expense of information privacy from the examination perspective. Further we saw to actualize upgraded procedure to perform double layer encryption strategy to enhance the framework execution.

6. REFRENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.

[2] T. Mather, S. Kumaraswamy, and S. Latif, Cloud security and privacy: an enterprise perspective on risks and compliance. O’ReillyMedia, Incorporated, 2009.

[3] H.-L. Truong and S. Dustdar, “Composable cost estimation and monitoring for computational applications in cloud computing environments,” Procedia Computer Science, vol. 1, no. 1, pp. 2175 – 2184, 2010, iCCS 2010.

[4] E. Deelman, G. Singh, M. Livny, B. Berriman, and J. Good, “The cost of doing science on the cloud: the montage example,” in Proc.2008 ACM/IEEE Conf. Supercomputing, ser. SC ’08. Piscataway, NJ,USA: IEEE Press, 2008, pp. 50:1–50:12.

[5] H. Hacig¨um¨us¸, B. Iyer, and S. Mehrotra, “Providing database as a service,” in Proc. 18th IEEE Int’l Conf. Data Engineering, Feb. 2002.

[6] G. Wang, Q. Liu, and J. Wu, “Hierarchical attributebased encryption for fine-grained access control in cloud storage services,” inProc. 17th ACM Conf. Computer and communications security. ACM,2010, pp. 735–737.

[7] H. Hacig¨um¨us¸, B. Iyer, C. Li, and S. Mehrotra, “Executing sql over encrypted data in the databaseservice-provider model,” in Proc.ACM SIGMOD Int’l Conf. Management of data, June 2002.

[8] L. Ferretti, M. Colajanni, and M. Marchetti, “Distributed, concurrent, and independent access to encrypted cloud databases,” IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, Feb. 2014.

[9] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, “CryptDB: protecting confidentiality with encrypted query processing,” in Proc. 23rd ACM Symp. Operating Systems Principles,Oct. 2011.

[10] C. Gentry, “Fully homomorphic encryption using ideal lattices,”in Proc. 41st ACM Symp. Theory of computing, May 2009.

[11] Boldyreva, N. Chenette, and A. O’Neill, “Orderpreserving encryption revisited: Improved security analysis and alternative solutions,” in Proc. Advances in Cryptology – CRYPTO 2011.Springer, Aug. 2011.

[12]K. Sravani , D. Praveen Kumar,"Performance And Cost Evaluation Of Flexible Architecture With Double Layer Encryption" International Journal Of Computer Engineering In Research Trends Volume 2, Issue 6, June 2015, Pp 395-399.

[13] P. Paillier, “Public-key cryptosystems based on composite degreeresiduosity classes,” in Proc.