Integrated Attribute Based Multi Level Encryption Framework for Improved Cloud Security using Hybrid Algorithms TOR-RCT-TREM

V.Poongodi[1]
[1]Research Scholar,
Manonmaniam Sundaranar University,
Tirunelveli,Tamil Nadu ,India
E-mail:vmpoongodi@yahoo.com

Dr.K.Thangadurai[2]
[2]Head, PG&Research Dept. of Computer Science,
Government Arts College, Karur.
Tamil Nadu ,India
E-mail:ktramprasad04@yahoo.com

***Abstract*-The growth of service orient architecture has great impact in different domain of applications. The cloud environment is such a SOA which provides different services at different levels to solve the problem of data management. In cloud environment, the user can access the services to store and retrieve the data whenever necessary. In such a loosely coupled environment, the security for the data is necessary and to provide such security, there are different encryption standards described earlier. The earlier methods suffers with the problem of securing data from unauthorized access and from various threats. To overcome the issues of various QoS parameters of cloud, we propose an integrated framework which enforces attribute based multi level encryption standard. The method classifies the data attributes into three different classes and for each class of attribute the method enforces different encryption standards. The proposed model improves the performance of security and reduces the overall time complexity in various factors.**

Keywords-Cloud Computing, Data Security, Encryption Standards, ABMLE, TOR, RCT, TREM

I. INTRODUCTION

The organizations stores many valuable information in the cloud storage which can be accessed by the users. In cloud there are number of services provided by the service provider in different levels. The service provider deploys different services like IaaS (Infrastructure as as Service), PaaS (Platform as a Service) and DaaS (Data as a Service). The user can access different resources through the services provided by the service providers. The user identity is not visible to the service provider and the trust management is performed by the third party. The third party maintains the user details and verifies the user identity before allowing the user to access the service.

The loosely coupled cloud environment has more chance of facing various network threats and there are malicious users who can perform various attacks over the cloud services provided. The data stored in the cloud can be accessed by the genuine users through the services provided and the malicious user can focus on producing malicious threats against the data stored. In general case the data stored in the cloud is in encrypted form which can be decrypted by the registered user at the time of access.

There are many encryption methods available for the data encryption from the RSA to Diffie Helman approaches. The methods can be classified as symmetric and asymmetric according to the method of encryption. Also there are methods which uses public and private key mechanisms. Each of the method has their own credit and disadvantages depending on various parameters. Some of the methods are fool proof but suffers with the large time complexity. In such a service orient architecture, the latency or the time complexity is more necessary which affects various other parameters of quality of service like throughput and service utilization.

This paper consider more number of quality of service parameters and to achieve that it incorporates three different methods like TOR, RCT and TREM. The TOR is a security service algorithm which combines TORDES and RSA and proposed a new hybrid security service algorithm called TOR. The proposed TOR algorithm consist of both symmetric and asymmetric cryptographic algorithm. In this TORDES is a symmetric key algorithm whereas RSA is an asymmetric key algorithm. The RCT algorithm is used to enhance the data storage in the cloud environment. The proposed algorithm is integrated with two symmetric cryptographic techniques namely, RC6 and TORDES. The TREM Security service algorithm combines two efficient cryptographic algorithms. In this service the original text is converted into cipher text using the message digest technique. If a cryptographic algorithm use the message digest technique it is very difficult to extract the information from the cipher text. The main advantage in this service the size of the cipher text is small. Hence it does not have difficulty in the cloud storage.

The ABMLE (Attribute Based Multi Level Encryption) , is the method which groups the different attributes into different level and for each level the method enforces different encryption standards. For example, the method splits the entire attributes into different security levels as generic, moderate and more sensitive. Based on the level of the data the method chooses the encryption standards. This paper discusses about such method in the next sections.

II. RELATED WORK

There are number of security methods discussed to improve the security of data in the cloud environment. This section discusses about some of the methods.

Enhanced data security in cloud computing with third party auditor [3], explained different existing paper techniques and their merits and demerits. We discussed their methods of data security and privacy etc. In all those papers some haven‟t described proper data security mechanisms, some were lack in supporting dynamic data operations, some were lack in ensuring data integrity, while some were lacking by high resource and computation cost. Hence this paper gives overall clue of all existing techniques for cloud data security and methods proposed for ensuring data authentication using TPA.

Robust Data Security for Cloud while using Third Party Auditor [4], the client or data owner send their data to data centre and utilize the service provided by the Cloud Service Provider (CSP). The CSP will manage the data of client at data centre. If there is large number of clients is there who using the services of cloud then the management of data at data centre will be difficult and even some time for their mutual benefit of CSP (limited space available at Data Centre) it can discard some data of client which is not used by the client for a long time. So we use Third Party Auditor (TPA) who not only manage the data but also tells the client that how much CSP is reliable and can keep the data safe. Even sometime client send false data or data is corrupted due to noise or some error, he claims that CSP change his data. Since there is no provisioning of accountability of data, so no one accounts for false data and also we can't trust fully on TPA, he can also transfer clients' data to his competitor.

Cloud Data Security using Authentication and Encryption Technique [5], brings about many new challenges, which have not been well understood. Security and privacy concerns, however, are among the top concerns standing in the way of wider adoption of cloud. In cloud computing the main concern is to provide the security to end user to protect files or data from unauthorized user. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. We have designed one proposed design and architecture that can help to encrypt and decrypt the file at the user side that provide security to data at rest as well as while moving. In this research paper, we have used the Rijndael Encryption Algorithm along with EAP-CHAP.

Enhancing security in cloud computing structure by hybrid encryption [7], addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of message Digest encryption (MD5), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability.

A proficient model for high end security in cloud computing [9], propose a new model to ensure the data correctness for assurance of stored data, distributed accountability for authentication and efficient access control of outsourced data for authorization. This model strengthens the correctness of data and helps to achieve the cloud data integrity, supports data owner to have control on their own data through tracking and improves the access control of outsourced data.

Enhancing Data Storage Security in Cloud Computing Through Steganography [10], investigated the problem of security in cloud computing, which is essentially a distributed storage system. To ensure the security of user’ data in cloud storage, we proposed an effective and efficient steganographic strategy for enhancing security on data-at-rest. So, when these images are stored in the cloud data centre, no one can view the original content of the data without any proper identification. Through detailed security and performance analysis, we have seen that our scheme almost guarantees the security of data when it is residing on the data center of any Cloud Service Provider (CSP).All the above discussed methods has the problem of identifying malicious request efficiently and produces large time complexity.

III. PROPOSED WORK

Attribute Based Multi Level Encryption (ABMLE)

The proposed method splits the attributes of data into three levels and for each level of attributes the method uses different encryption standards. The method incorporates TOR, RCT and TREM to improve the performance of the cloud security. This section details the implementation of ABMLE algorithm as follows:

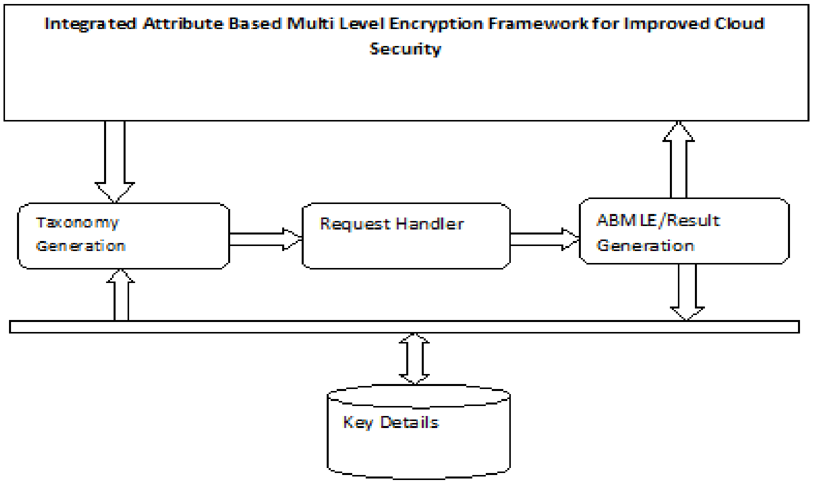
Integrated Attribute Based Multi Level Encryption Framework for Improved Cloud Security
Taxonomy Generation
Request Handler
ABMLE/Result Generation
Key Details

Figure 1: Architecture of ABMLE Approach

The Figure 1, shows the architecture of attribute based multi level encryption algorithm for improved cloud security.

Taxonomy Generation:

Initially the method reads the meta data and for each data, the method identifies the level of security it requires. First the method identifies list of attributes present in the data and for each data attribute the method identifies the kind of security necessary from the meta data. Finally the method classifies the entire data into three categories and the classified data taxonomy will be used to perform encryption.

Algorithm:

```
Input: Data set Ds
Output: Taxonomy T
Start
    Read data set ds.
    Generate attribute set As = Identify distinct attribute Ai.
    For each attribute Ai
        Compute the security level Sl.
    End
    For each attribute Ai
        Assign a class according to security level.
    End
Stop.
```

The above discussed algorithm computes the security level required for each attribute and assigns a class according to the computed value.

Request Handler:

The request handler receives the user request from the cloud users. From the request being received the method identifies the data being requested. Based on the request being identified the method access the multi level attribute based encryption to encrypt data to produce result to the users. The user may request any type of data and from the request the method identifies the type of data being requested. The method uses the attribute taxonomy and identifies the security level of the attribute. Based on the security level identified the method uses a encryption method.

Algorithm:

```
Input: Request R, Taxonomy T
Output: Result Rs
Start
    Identify the data requested.
    Rd = Request.Data
    Identify the data type from the taxonomy.
    For each class C from T
        Identify the presence of Rd
            If Rd$\in C$ then
            Assign class to the data.
    end
    End
    If C==Type 1 then
        ABMLE( R,TREM)
    Else C==Type2 then
        ABMLE(R,RCT)
    Else
        ABMLE(R,TOR)
    End
Stop.
```

The above discussed algorithm selects the encryption method should be used to produce the cipher text according to the class of the data being requested.

At this stage the method reads the data request and identified data type. The method also reads the security level identified by the request handler and based on identified security level the method selects the method from available three methods of encryption to generate cipher text.

Algorithm:

```
Input: Request R, Method M.
Output: Cipher text T.
Start
    Read the data D.
    Use method M to produce cipher text T.
Stop.
```

The above discussed algorithm produces cipher text based on the algorithm being selected to produce the cipher text.

A.TORDES Algorithm

TORDES is a block cipher algorithm. It is a unique and independent approach which uses several computational steps along with string of randomized operators and delimiter selections by using some suitable mathematical logic with transformation and mirror image operation. It is specially designed to produce different cipher texts by applying same key on same plain text. It is one of the best performing partial symmetric key algorithms particularly for the text message in its class. It also safeguard against various attacks like Brute-force because it is not fully dependent on the key and code cannot be deciphered by applying all possible combinations of keys. The following information invariably used in TORDES for encryption techniques.

1) 32 bit key.
2) Code sequence string generated from a particular process (Multithread).
3) Transformation of String.
4) Mirror image of String.
5) Lookup Table
6) Randomized delimiter string

B.TOR Algorithm

In this security service algorithm TORDES and RSA were combined and proposed a new hybrid security service algorithm called TOR. The proposed TOR algorithm consists of both symmetric and asymmetric cryptographic algorithm. In this TORDES is a symmetric key algorithm whereas RSA is an asymmetric key algorithm. The proposed algorithm is implemented as a security service in the cloud environment. The working process of the proposed TOR algorithm is clearly explained in the following steps to know how the cloud users data are stored in a highly secured way over the cloud storage environment.

STEP 1: Researcher proposed security service algorithms using different hybrid cryptographic techniques.

STEP 2: The Proposed TOR algorithm is deployed in the cloud environment as security services.

STEP 3: The cloud users want to store their data in the cloud storge environment. For this user request any one of the cloud security services in the cloud environment.

STEP 4: The requested cloud security service is offered to the cloud user to encrypt or to decrypt their data.

STEP 5: Finally, the cloud users encrypt / decrypt or their data to store or to retrieve from the cloud storage environment.

C.RCT

In the previous proposed TOR security algorithm we used symmetric and asymmetric key cryptographic techniques. In this algorithm the computational speed is little complex and the size of the cipher text is also high to reduce the computational complexity and the size of the cipher text we used two symmetric key algorithm techniques in a hybrid form. The proposed RCT algorithm is used to enhance the data storage in the cloud environment. The proposed algorithm is integrated with two symmetric cryptographic techniques namely, RC6 and TORDES.

The working process of the proposed RCT algorithm is clearly explained in the following steps to know how the cloud users' data are stored in a highly secured way over the cloud storage environment.

STEP 1: *Researcher proposed security service algorithms using different hybrid cryptographic techniques.*

STEP 2: *The Proposed **RCT** algorithm is deployed in the cloud environment as security services.*

STEP 3: *The cloud users want to store their data in the cloud storge environment. For this user request any one of the cloud security services in the cloud environment.*

STEP 4: *The requested cloud security service is offered to the cloud user to encrypt or to decrypt their data.*

STEP 5: *Finally, the cloud users encrypt / decrypt or their data to store or to reterieve form the cloud storage environment.*

D.TREM

The proposed TREM Security service algorithm combines two efficient cryptographic algorithms. In this service the original text is converted into cipher text using the message digest technique. If a cryptographic algorithm use the message digest technique, it is very difficult to extract the information from the cipher text. The main advantage in this service, the size of the cipher text is small. Hence it does not have difficult in the cloud storage. The proposed algorithm is analyzed in the cloud environment as a service.

The working process of the proposed TREM algorithm is clearly explained in the following steps to know how the cloud users' data are stored in a highly secured way over the cloud storage environment.

STEP 1: *Researcher proposed security service algorithms using different hybrid cryptographic techniques.*

STEP 2: *The Proposed **TREM** algorithm is deployed in the cloud environment as security services.*

STEP 3: *The cloud users want to store their data in the cloud storge environment. For this user request any one of the cloud security services in the cloud environment.*

STEP 4: *The requested cloud security service is offered to the cloud user to encrypt or to decrypt their data.*

STEP 5: *Finally, the cloud users encrypt / decrypt or their data to store or to retrieve form the cloud storage environment.*

IV. RESULTS AND DISCUSSION

The proposed algorithm is implemented using .NET. The simulation analysis is performed in the cloud environment(Microsoft Azure) with different data input. The time taken to Encrypt and Decrypt the given input data is calculated for the proposed ABMLE and Existing RSA,AES and BlowFish Algorithms. The results are compared and tabulated in table 1 and it is graphically represented in figure 4.

Size	**Algorithms**						
	RSA	**AES**	**Blowfish**	**TOR**	**RCT**	**TREM**	**ABMLE**
	Encryption Time (Minutes)						
1 MB	14.6754	13.9436	10.8872	5.7856	8.9769	4.7983	4.2983
5 MB	19.7381	17.8764	13.7968	9.8798	10.8976	7.8257	7.321
10 MB	24.6786	21.7548	17.9647	14.6888	15.7963	12.9327	11.327
15 MB	27.8654	24.6979	21.6548	18.9799	19.6875	14.8753	13.753

Table 1.Comparative Analysis based on Encryption Time

The Table 1, shows the comparative details on encryption time produced by different methods and the result shows that the proposed method produces less time complexity than the existing algorithm methods.

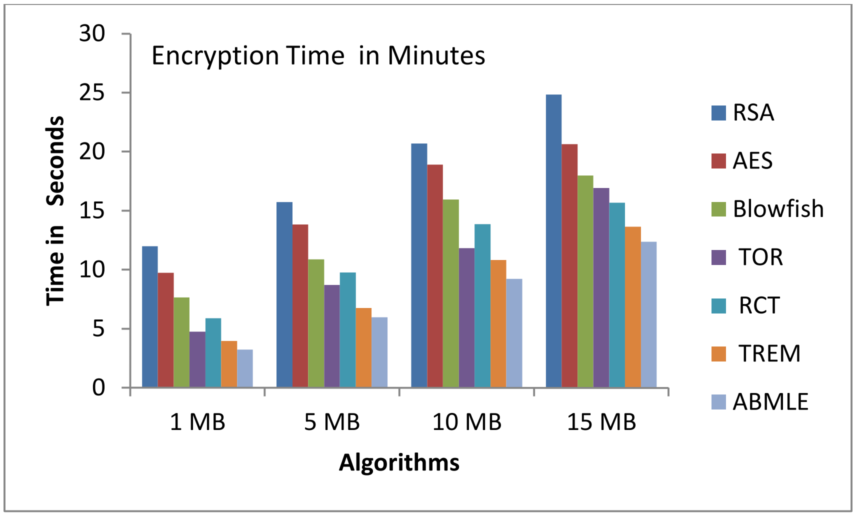

Figure 2. Comparative Analysis based on Encryption Time

Figure 2, shows the comparative results on encryption time produced by different methods and the results shows that the proposed methods produces less time complexity on varying size of data retrieval.

Size	Algorithms						
	RSA	AES	Blowfish	TOR	RCT	TREM	ABMLE
	Decryption Time(Minutes)						
1 MB	11.9738	9.7382	7.6347	4.7454	5.8945	3.9627	3.227
5 MB	15.7357	13.8172	10.8796	8.6940	9.7654	6.7635	5.9635
10 MB	20.6937	18.9073	15.9363	11.8132	13.8673	10.8214	9.214
15 MB	24.8392	20.6382	17.9826	16.9173	15.6759	13.6376	12.376

Table 2.Comparative Analysis based on Decryption Time

Table 2 presents the performance comparison of decryption with existing techniques. The time taken by the existing and proposed decryption algorithms is calculated for different sizes of data.

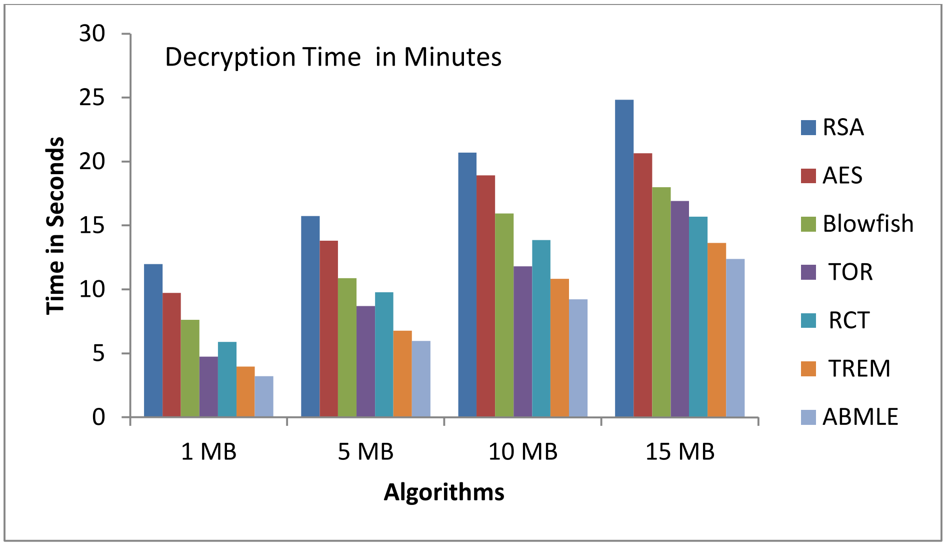

Figure 3. Comparative Analysis based on Decryption Time

The Figure 3, shows the comparative results on decryption time produced by different methods and the results shows that the proposed method has produced less time complexity than other methods.

Table 3. Comparison of Security Levels of Existing and Proposed Algorithms

Algorithms	Security Level(%)
BlowFish	74
AES	79
RSA	82
TOR	84
RCT	85
TREM	87
ABMLE	97

Table 3. Comparison of Security Levels of Existing and Proposed Algorithms

Table 3 and Figure 4 represent the comparison of security levels. The result shows that compared to the existing algorithms, TREM hybrid Security algorithm produces maximum security for cloud data. Security level of ABMLE is 97%, RSA is82%, AES is 79% and Blowfish is 74%.

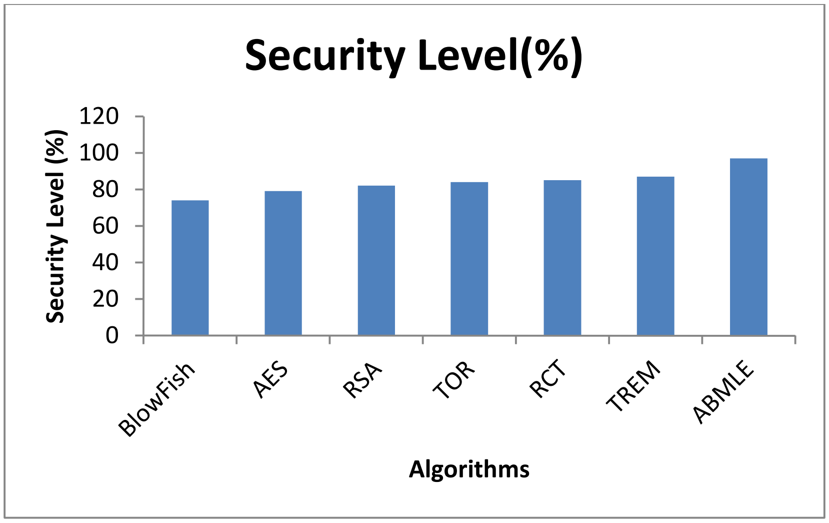

Figure 4. Comparison of Security Levels of Existing and Proposed Algorithms

The Figure 4 shows the comparative results on security level produced by different methods and it shows clearly that the proposed method has produced higher security levels than others.

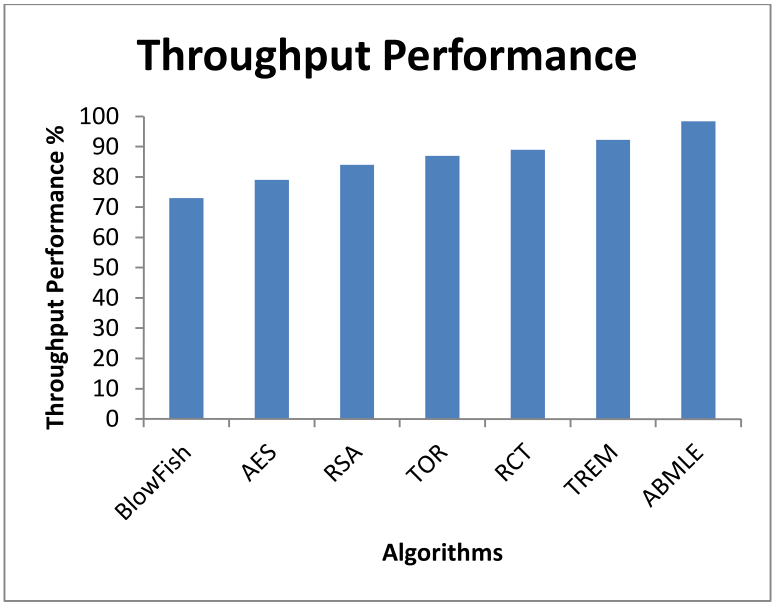

Figure 5 Comparison of throughput performance

The Figure 5, shows the comparison of throughput performance and the results shows that the proposed ABMLE algorithm has produced higher throughput than other methods.

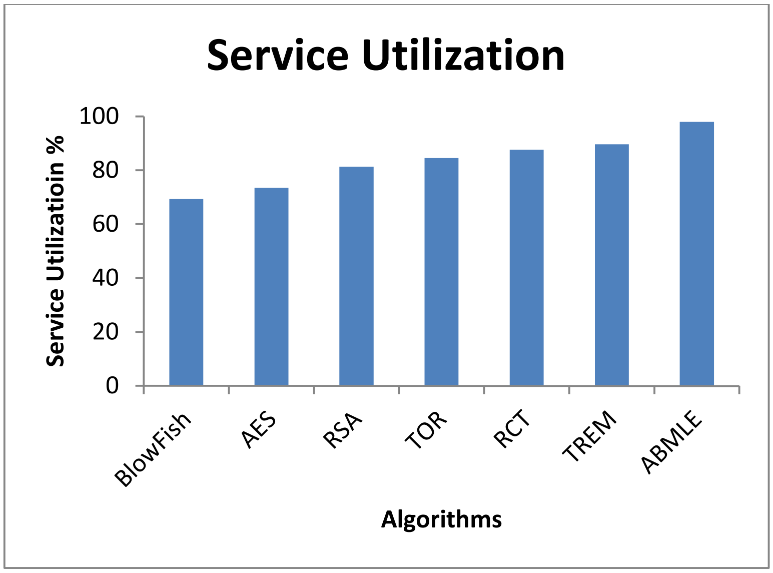

Figure 6: Comparison of service utilization

The Figure 6, shows the comparative results on service utilization and the result shows clearly that the proposed method has produced higher service utilization than other methods.

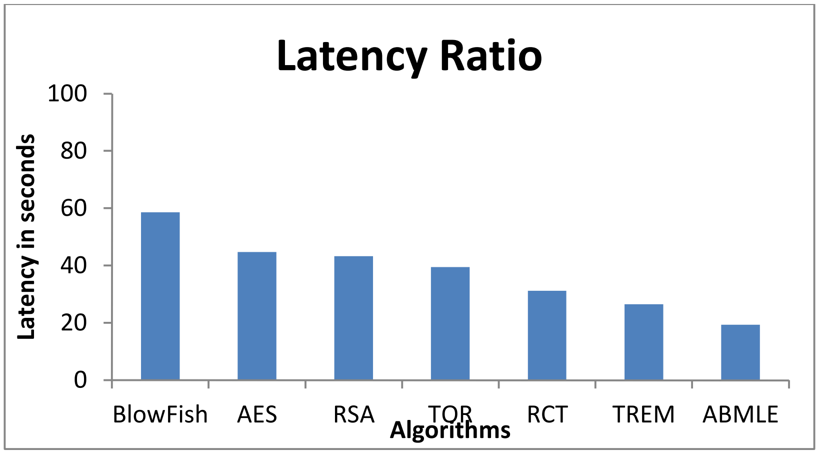

Figure 7: Comparison of latency ratio

The Figure 7, shows the comparison of latency ratio produced by different methods and the result shows clearly that the propose method has produced less value than other methods.

V. CONCLUSION

To improve the performance of cloud environment and improve the security performance, the author proposed an integrated attribute based multi level encryption framework in this paper. The method generates the taxonomy of data attributes from the input meta data of data's. The taxonomy generation approach classifies the data attributes into different class. Whenever a data request received, the method identifies the type of data or class of data being requested. Based on the type of data being requested the method selects the encryption approach. By assigning different methods for encrypting the different data types, the overall time complexity is reduced. Also the method selects the encryption method according to the data type being requested which improves various parameters of quality of service.

REFERENCES

[1] Security and privacy in cloud computing by Zhifeng Xiao and Yang Xiao in IEEE Communications Surveys and tutorials, 15.

[2] Data security in the world of cloud computing by Lori M. Kaufman John Harauz in IEEE Computer and Reliability society.

[3] Enhanced data security in cloud computing with third party auditor by Indrajit Rajput in International Journal of Advanced Research in Computer Science and Software Engineering, 3.

[4] Robust Data Security for Cloud while using Third Party Auditor by AbhishekMohta,Ravi Kant Sahu and LK Awasthi, in International Journal of Advanced Research in Computer Science and Software Engineering, Vol No. 2, Issue 2,Feb 2012.

[5] Cloud Data Security using Authentication and Encryption Technique by SanjoliSingla and Jasmeet Singh in IJARCET Vol 2, Issue 7, July 2013.

[6] Survey on triple system security in cloud computing by ParulMukhi and Bhawna Chauhan in IJCSMC, Vol. 3, Issue. 4, April 2014.

[7] Enhancing security in cloud computing structure by hybrid encryption by Aparjita Sidhu and Rajiv Mahajan in International Journal of Recent Scientific Research Vol. 5, Issue, 1, pp.128-132, January, 2014.

[8] Data Security in Cloud Computing by K. S. Wagh, SwapnilChaudhari, Anita Deshmukh and PrajaktaKhandave in International Journal of Current Engineering and Technology.

[9] A proficient model for high end security in cloud computing by R. BalaChandar, M. S. Kavitha and K. Seenivasan in ICTACT journal on soft computing ,january 2014, volume: 04, issue: 02.

[10] Enhancing Data Storage Security in Cloud Computing Through Steganography by MrinalKanti Sarkar and Trijit Chatterjee in ACEEE Int. J. on Network Security , Vol. 5, No. 1, January 2014.

[11] Enhancing Security in Cloud computing using Public Key Cryptography with Matrices by BirendraGoswami and Dr.S.N.Singh in Vol. 2, Issue 4, July-August 2012, pp.339-344.

[12] Fingerprinting Based Recursive Information Hiding Strategy in Cloud Computing Environment by VarshaYadav and Preeti Aggarwal in IJCSMC, Vol. 3, Issue. 5, May 2014.

V.Poongodiwas born in Perambalur, Tamil Nadu (TN), India, in 1976. She received the Bachelor of Physics (B.Sc.) degree from the Bharathidasan University, Tiruchirapally, TN, India in 1996, the Master of Computer Applications (M.C.A.) degree from the Bharathidasan University, Tiruchirapally, TN, India, in 1999 and Master of Philospophy (M.Phil.)degree in Computer Science from the Bharathidasan University, Tiruchirapally, TN, India, in 2006. She is currently pursuing the Ph.D. degree with the Department of Computer Science, in Manonmaniam Sundaranar Univeriety, Tirunelveli, TN. Currently she is working as Assistant Professor in Department of Computer Applications in Thanthai Hans Roever College, Perambalur.TN, India. Her research interests include Cloud Computing, Cryptography and Network Security.

Dr.K.Thangaduraiwas born in Karur, Tamil Nadu (TN), India, in 1974. He received the Bachelor of Physics (B.Sc.) degree from the Madras University, TN, India, in 1994, Master of Physics (M.Sc.) degree from the Bharathidasan University, Tiruchirapalli, TN, India, in 1996, Master of Computer Applications (M.C.A.) degree from the Bharathidasan University, Tiruchirapally, TN, India,in 1999, Master of Philospophy in Computer Science (M.Phil.) degree from the Manonmaniam Sundaranar Univeristy, Tirunelveli, TN in 2002, Doctor of Philospophy in Computer Science (Ph.D.) degree from the Vinayaka Mission's Univeristy, Salem, TN in 2009. He is currently working as Assistant Professor and Head in P.G and Research Department of Computer Science, Government Arts College, Karur, TN, India. His total teaching expericnce is about 17 years. He published more than 40 research articles in various National and International Journals. His research interests include Data Mining, Software Engineering and Network Security.