Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REAL TIME ORDERED-UNORDERED SESSION KEY DISTRIBUTION SCHEME FOR IMPROVED DLP AND IRM IN CLOUD ENVIRONMENT

PAVITHRA P[1], HARIHARAN B[2],WILFRED BLESSING N.R[3]

[1]Assistant Profesor,Rmk College Of Engineering And Technology, Department of Computer Science and Engineering, Chennai.
[2]Assistant Profesor,SRM Institute of Science and Technology, Department of Computational Intelligence, Chennai.
[3]Assistant Profesor,University of Technology and Applied sciences-lbri, Department of Information Technology, Oman.
E-mail:[1]pavithracse@rmkcet.ac.in,[2]hariharb@srmist.edu.in,[3]wilfred.b@ibrict.edu.om

ABSTRACT:

The problem of Data Loss Prevention (DLP) and Information Right Management (IRM) has been well analyzed towards security development in cloud. The walls of cloud security enforcement hide the user's personal data from the service provider which challenges them in maintaining data secrecy as well as data leak.Such loosely coupled nature allows the cloud users in generating different threats against various Quality of Service parameters. Towards DLP and IRM, different approaches are furnished in literature but suffer in achieving expected QoS values. does not know much about There exist numerous techniques to handle the security problem, but suffer to achieve To handle this issue, an efficient real time Ordered-Unordered Session Key Distribution Scheme (ROUSKDS) is presented in this article. The article is focused on using different secret keys in various sessions to restrict malformed access as well as restricting information leakage. In the focus to improve the performance of data loss prevention and information right management, the proposed model generates keys for various services for the session according to the result of Ordered-Unordered Shuffling (OUS) scheme. The method maintains number of keys for various services and shuffle the session keys either in a ordered way or unordered way. Similarly, the model uses Dual Mode Information Right Management (DMIRM) to restrict the user from malicious access. The method measure the trust of user at key level trust and access level trust values. Based on these values, the method restricts the malformed access to improve the performance of IRM.By maintaining various secret keys towards different services in various time stamp, both IRM and DLP process can be enhanced. The proposed method improves the performance of DLP and IRM which in turn improves the performance of cloud.

Keywords: *Cloud Security, DLP, IRM, OUS, DMIRM, Access Restriction, Trust Measure.*

1. INTRODUCTION:

The organizations maintain variety of data in their data servers which would be belong to different users of the environment. However, the environment contains number of users, not all of them are allowed to access the entire data. The data server would maintain number of data which belongs to various categories like users, customers, and business and so on. So, the organization has the responsibility in maintaining the secrecy of user data and maintaining the integrity and security as well. Towards this, there are number of approaches available like key based approaches which restrict the user access based on the possession of exact key. Similarly, the access restriction is performed based on the profile of user, role of user, behavior of user and so on. However, the methods suffer with poor performance in achieving data security in cloud.

The presence of malicious user in the environment would generate number of threats and there will be data leakage which must be stopped. The Data Leakage Prevention (DLP) is the process of preventing the malformed access and preventing the leakage of data. The DLP can

be enforced by using various schemes of data encryption. The data encryption schemes can be adapted to prevent the data leakage. In this way, there exist numerous techniques like AES, DES and so on. In recent times, the ABE (Attribute based encryption) schemes are widely used and service based schemes also widely used. However, they suffer to achieve higher performance in DLP achievement. Because, the adversary are capable of identifying the key being used for data encryption and steal the data encoded. To handle this, this article recommend a real time Ordered-Unordered Session Key Distribution Scheme (ROUSKDS). The model would generate

different set of keys towards various services for various session. The user can use the concern key for data encryption and scheme.

On the other side, the performance of the cloud environment can be improved by adapting efficient Information Right Management (IRM). This has been approached with different techniques like profile based IRM, Role based IRM, Behavior Based IRM and so on. However, the use of such approaches does not make any difference on the performance. To handle this issue, the proposed model uses different trust values and computes the trust of user at key level trust and access level trust values. Based on these values, the method restricts the malformed access to improve the performance of IRM. By enforcing efficient IRM in cloud, the performance of cloud can be improved. This article concentrate on both information right management and data loss prevention. The section 1 details the introduction of IRM and DLP approaches in cloud. The section 2 details the survey of various approaches related to the problem. Section 3 presents the detailed sketch of proposed approach and section 4 details the experimental results. Finally, section 5 details the conclusion of the proposed approach.

2. RELATED WORKS:

Different approaches of data loss prevention and information right management has been discussed in literature. This section details various approaches around the problem.

A hybrid attribute based encryption (HABE) scheme with customizable authorization is presented in [1], which uses CPABE algorithm towards access control in cloud. In [2], the author analyzes like RSA, SHA1, and MD5 towards data sharing in banking model. The method merges both ABE and Byte Rotation Encryption Algorithm. Similarly, the proxy re-encryption and key aggregate schemes are merged towards improving data security in [4]. A blow fish based data retrieval model is presented in [5], which uses porter stemming and blowfish algorithm in data encryption. Finally, ECC has been used towards public key encryption in [5].

A distributed eraser code with proxy re-encryption scheme is presented in [6], which share the data in cloud with different encryption format. AEncryscation based approach is presented in [7], which performs client side authentication and performs data obfuscation in the server. A comparative study has been presented in [8], which analyzes various homomorphic encryption methods towards secure data access in cloud. A DiffieHelman based data encryption scheme with AES is presented in [9], to protect confidentiality of data stored in cloud. A multi level security scheme is presented in [10], which involves in encrypting and enforcing data security in multiple level. The concept of hybrid encryption approach is enforced in [11], towards providing security measures in cloud storage.

An fully homomorphic encryption (FHE) based approach is presented to support privacy in public clouds in [12], where a hybrid encryption scheme is presented in [13], which combines RSA and blowfish approaches. Similarly in [14], anhomomorphic encryption scheme is presented named cloud-Elgamal which allows specific type of computations to be performed on encrypted data without decrypting it. A sliced revocable solution towards security issues named RS-CPABE is presented in [15], which uses spitting algorithm and a comparative study on various approaches are presented in [16].

A policy update enforced lightweight ABE (PU-ABE) is presented in [17], which captures attributes and access policies to perform access restriction and privacy preservation.

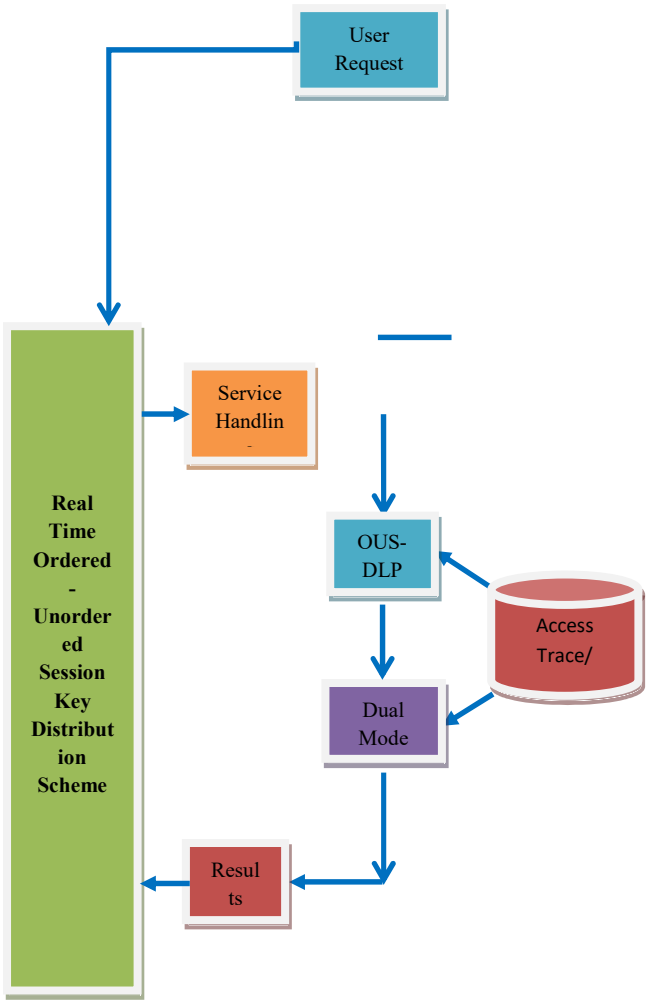

Figure 1: Architecture of Proposed ROUSKDS Scheme

In [18], an Enhanced Homomorphic Encryption Scheme with PSO is presented which selects the particle according to the PSO and uses homomorphic encryption.

A Host-based Anomaly DEtection System for IoT (HADES-IoT) is presented in [19] which perform detection according to proactive data and generates tamper-proof resistance to the system. A combination of genetic algorithm and back propagation neural network is presented in [20], which applies genetic algorithm to perform feature selection and BPNN to perform attack detection.

All the above discussed approaches suffer to achive expected performance on DLP and IRM factors.

2.1 Problem Statement:

From the literature survey, it is well analyzed and list of issues are identified. The methods focused on improving the data security by enforcing various encryption schemes. But in reality, using keys for encryption is not just enough but it is necessary to restrict the user from malformed access. Also, the malicious user should not be allowed to getting the original data by applying fruit force attack or any other trial and error methods. According to this, it is necessary to design effective IRM and DLP scheme in one slot to support the achievement of higher QoS.

3. REAL TIME ORDERED-UNORDERED SESSION KEY DISTRIBUTION SCHEME:

The proposed model maintains the traces of various services access performed by different users. According to the traces maintained, the method enforces the Information Right Management in dual mode. Similarly, the model maintains different scheme and key sets. The method enforce the data leakage protection (DLP) using the Ordered-Unordered Shuffling (OUS) scheme towards various sessions regarding various services. By using both dual mode RIM and OUS data leakage protection, the method controls both access restriction and data security. The detailed approach is presented in this section.

The architecture of proposed real time ordered unordered session key distribution based IRM and DLP model has been presented in Figure 1. The detailed approach is presented in this section.

3.1 Service Handling:

The service request generated by user has been received here. From the service request, the method identifies the service being request by the user. Further, the method performs Ordered-Unordered Shuffling based Data leak protection, which selects the optimal key for the user according to the key and scheme set given for the user at the starting of session. Also, the method performs Information right management with Dual Mode IRM algorithm. If the user clears the trust evaluation with DMIRM algorithm, then the data has been encrypted according to the scheme and key being identified

for the user. The cipher data has been given to the user as result.

Service Handling Algorithm:

Given: Service Request Sreq, User Set Uset.

Obtain: Null

Start

Read Sreq, Uset.

Service S = Service$\in Sreq$

Trust weight Tw = Perform Dual Mode IRM.

If Tw>Th then

{scheme,Key}=

$$Uset(i).Scheme, keywhere Uset(i).User == U \&\& Uset(i).Service == S \quad \text{for } i = 1 \text{ to } size(Uset)$$

Cipher text CT = Perform Data Encryption (Service data, scheme, key)

Else

Drop request

End

If request is login then

Perform OUS-DLP.

End

Stop

The working of service handling algorithm is presented in the above pseudo code which receive the user request and applies both OUS-DLP and Dual mode IRM to improve the security performance.

3.2 Ordered Unordered Shuffle Data Leakage Protection:

Towards data leakage protection, the method generates scheme and key sets for various services at different time stamp and session. At each session, the method generates different scheme and key sets for each user who registered and given to them. The method maintains set of schemes and keys in the set and at the start of the session, the method shuffle the scheme set and key set in a ordered way or un ordered manner. The scheme set contains set of schemes using which the data belongs to the specific service is encrypted and decrypted. Similarly, the key set contains set of keys belongs to specific service using which the encryption and decryption should be performed. Here the shuffling is done not just on the key and scheme sets but also done on the list of services. So, everything will be shuffled before giving to the user. This will be used only for the specific session. Also, this will be iterated at all the sessions. In case of ordered shuffling, the set has been split into number of blocks and shuffling will be done within the unique tiny sets. In case of unordered shuffling, the method shuffle with entire set. By enforcing DLP according to the shuffled key and scheme sets, the security performance is improved.

Algorithm:

Given: Scheme set Ss, Key set Ks, Service set Ses.

Obtain: Scheme set, Key set Ks and Service Set Ses.

Start

Read Scheme set Ss, Key set Ks, Service set Ses.

At each session

Generate random number Rn = $\int Random(1,100)$

If Rn is odd then // do unordered shuffling

Perform unordered shuffling on Ss, Ks, Ses.

Else

Split Ss, ses, ks into K number of blocks.

For each set

For each block

Perform ordered shuffling within the block.

End

End

End

Send Ss, Ses, Ks to the user.

End

Stop

The ordered unordered shuffling data leakage protection algorithm generates different scheme and key sets for unique user of the environment at each session considered. It has been done by shuffling the scheme and key sets according to the condition obtained with random number. Generated sets are given to the user with which the user and system perform data encryption and decryption.

3.3 DUAL MODE IRM:

The information right management is performed in dual mode in the proposed model. The system maintains set of access trace belong to each user which is generated by the access performed by the user. According to this, the method fetch the traces of user and computes the trust measures as key level trust (KLT) and Access level trust (ALT). The key level trust is measured based on the number of times the user has possessed with the correct key and number of times the user accessed the service. The access level trust (ALT) is measured based on the number of times the user accessed the service and number of times the user has been grant access and completed successfully. Using these two measures, the method computes the value of Trust weight (TW). Based on the value of IRM the service handler either allows the request or denies.

Algorithm:

Given: Access Trace Act, User U, Service S

Obtain: Trust weight Tw.

Start

Read AcT, U, S.

User Trace Ut = $\sum_{i=1}^{Size(Act)} Act(i).User == U \&\& ACT(i).Service == S$

Compute Key level Trust KLT = $\frac{\sum_{i=1}^{Size(UT)} UT(i).KeyState==Safe}{Size(UT)}$

Compute Access Level Trust AlT = $\frac{\sum_{i=1}^{Size(UT)} UT(i).GrantState=}{Size(UT)} \times \frac{\sum_{i=1}^{Size(UT)} UT(i).State==Complete}{Size(UT)}$

Compute Trust weight Tw = KLT×ALT

Stop

The above discussed algorithm estimates key level trust and access level trust for the user. Based on these values, the method computes the value of Trust weight based on which the method enforces information right management.

4. RESULTS AND DISCUSSION:

The proposed real time Ordered Unordered Shuffling session key distribution based DLP and IRM has been implemented using Microsoft Azure. Further, the performance of the method has been evaluated using several conditions like services, session, data and so on. The results obtained have been compared with the results of other methods.

Table 1: Evaluation Details

Parameter	Value
Tool Used	Microsoft Azure
No of Services	50
No of Features	200
Number of Users	10000

The evaluation features towards performance measurement is given in Table 1. According to the environment conditions, the performance of the proposed approach is evaluated and presented in this section.

Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Analysis of security performance vs users

Performance Analysis on Data Security Vs Number of Features			
	50 Features	100 Features	200 Features
PU_ABE	65	68	72
PSO	69	73	77
HADES_IoT	72	76	83
BPNN	85	89	94
ROUSKDS	89	92	97

The analysis on data security performance produced by various approaches are presented in Table 2, where the ROUSKDS approach achieved higher performance up to 97 %, which is higher than other PU_ABE, PSO, HADES_IoT and BPNN schemes.

Figure 2: Performance in Security vs No of Users

The security performance produced by various approaches are measured and presented in Figure 2. The ROUSKDS scheme achieved security performance up to 97% which is higher than the existing PU_ABE, PSO, HADES_IoT and BPNN schemes.

Table 3: Analysis on throughput performance vs number of Features

Analysis of Throughput Performance vs No of Features in %			
	50 Features	100 Features	200 Features
PU_ABE	67	69	73
PSO	71	73	75
HADES_IoT	74	77	79
BPNN	84	87	95
ROUSKDS	87	91	98

The throughput performance achieved by the different schemes in varying conditions ofnumber of features or attributes in the environment and presented in Table 3.

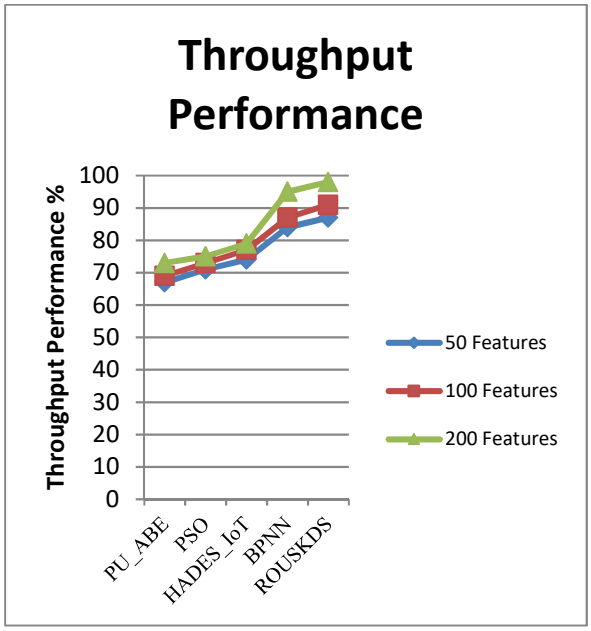

Figure 3: Performance on throughput achievement vs No of Users

At each conditions the ratio of throughput produced by the methods are measured and presented. However, the proposed ROUSKDS scheme has achieved higher throughput performance up to 95% which is higher than other PU_ABE, PSO, HADES_IoT and BPNN algorithms.

The throughput performances produced by various approaches are displayed in Figure 3. The proposed ROUSKDS algorithms have

achieved higher throughput performance compare to other methods.

Table 4: Performance analysis on encryption / decryption vs no of Features

Performance on Encryption / Decryption in % vs No of Features			
	50 Features	100 Features	200 Features
PU_ABE	64	67	71
PSO	68	72	76
HADES_IoT	71	75	81
BPNN	86	91	95
ROUSKDS	89	93	98

The performance in data encryption and decryption are measured and presented in Table 4, which is measured in different conditions of different number of features in the environment. At each number of user condition, the performance on encryption and decryption are analyzed. The ROUSKDS approach produced higher performance.

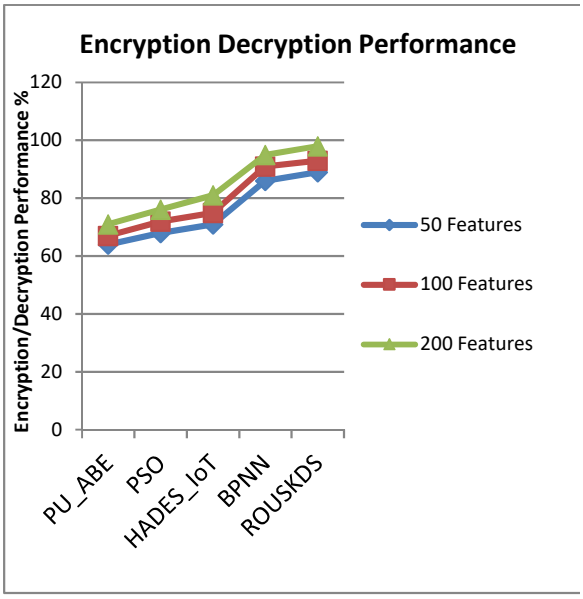

Figure 4: Performance in Encryption / Decryption vs No of Features

The performance in encryption and decryption is measured for different approaches and the ROUSKDS algorithm produced higher results.

Table 5: Analysis on Time Complexity vs No of Features

Time Complexity vs No of Features			
	50 Features	100 Features	200 Features
PU_ABE	85	89	95
PSO	81	85	88
HADES_IoT	70	74	81
BPNN	32	35	43
ROUSKDS	24	29	35

The value of time complexity is measured for various approaches and ROUSKDS approach produced least time complexity than others.

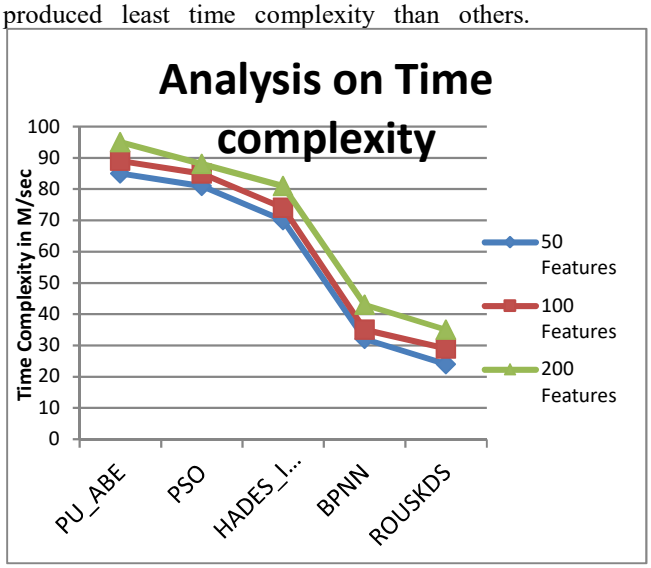

Figure 5: Performance in time complexity vs No of Features

The performance in time complexity has been measured at varying number of users and presented in Figure 5. The proposed ROUSKDS algorithms have produced less time complexity than other methods. The time complexities generated by different algorithms are measured at different conditions of features present in the environment. However, the proposed ROUSKDS scheme has produced less time complexity in all the feature conditions compare to other PU_ABE, PSO, HADES_IoTand BPNN methods.

5. CONCLUSION:

This article presented a novel real time Ordered Unordered Shuffle Session key distribution based model for efficient data leakage protection and Information recognition management. Unlike other methods, the proposed model shuffle the key set with ordered and un ordered manner which challenges the adversary in predicting the exact key being used for any service at specific session. This safeguards the service data towards higher QoS achievement. The model performs key distribution at each session according to ordered unordered shuffle scheme to enforce data leakage protection which support the data encryption and decryption. Further, the method uses dual mode information recognition management by computing both key level trust and access level trust to compute the trust weight. The system uses the trust weight as the key to decide on the grant or denying the access request. The proposed approach improves the performance in data leakage protection and information recognition management.

REFERENCES:

[1]. Y. S. Gunjal, M. S. Gunjal and A. R. Tambe, "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing," IEEE (ICACCT), 2018, pp. 187-190.

[2]. V. Sreenivas, "Performance evaluation of encryption techniques and uploading of encrypted data in cloud," IEEE (ICCCNT), 2013, pp. 1-6.

[3]. P. More, S. "Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud," IEEE (ICACCT), 2018, pp. 93-96.

[4]. W. Chen, "Efficient Key-Aggregate Proxy Re-Encryption for Secure Data Sharing in Clouds," IEEE (DSC), 2018, pp. 1-4.

[5]. S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," IEEE (ICICCS), 2017, pp. 267-271.

[6]. R. Nivedhaa and J. J. Justus, "A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption," IEEE (ICCSP), 2018, pp. 0755-0759.

[7]. K. Suthar and J. Patel, "EncryScation: A novel framework for cloud IaaS, DaaS security using encryption and Obfuscation techniques," IEEE (NUiCONE), 2015, pp. 1-5.

[8]. K. Rangasami and S. Vagdevi, "Comparative study of homomorphic encryption methods for secured data operations in cloud computing," IEEE (ICEECCOT), 2017, pp. 1-6.

[9]. P. Rewagad and Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," IEEE (ICCSNT), 2013, pp. 437-439.

[10]. B. Jana, "A multilevel encryption technique in cloud security," IEEE (CSNT), 2017, pp. 220-224.

[11]. S. Kaushik and C. Gandhi, "Cloud data security with hybrid symmetric encryption," IEEE (ICCTICT), 2016, pp. 636-640.

[12]. O. Kocabas and T. Soyata, "Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing," IEEE (ICCC), 2015, pp. 540-547.

[13]. V. P. Bansal and S. Singh, "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs," IEEE (RAECS), 2015, pp. 1-5.

[14]. K. El Makkaoui, "Cloud-ElGamal: An efficient homomorphic encryption scheme," IEEE (WINCOM), 2016, pp. 63-66.

[15]. M. Bouchaala, C. Ghazel and L. A. Saidane, "Revocable Sliced CipherText Policy Attribute Based Encryption Scheme in Cloud Computing," IEEE (IWCMC), 2019, pp. 1860-1865.

[16]. K. K. Chennam, "Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud," IEEE (RTEICT), 2017, pp. 2030-2033.

[17]. S. Belguith, "PU-ABE: Lightweight Attribute-Based Encryption Supporting Access Policy Update for Cloud Assisted IoT," IEEE (CLOUD), 2018, pp. 924-927.

[18]. S. A. Khan, R. K. Aggarwal and S. Kulkarni, "Enhanced Homomorphic Encryption Scheme with PSO for Encryption of Cloud Data," IEEE (ICACCS), 2019, pp. 395-400.

[19]. Breitenbacher D, Homoliak I, Aung YL, Tippenhauer NO, Elovici Y (2019) Hades-

iot: A practical host-based anomaly detection system for iot devices (extended version). CoRR abs/1905.01027.http://arxiv.org/abs/1905.01027.

[20]. Manimurugan S, Manimegalai P, PrajoonaValsalan, Krishnadas J, Narmatha C, Intrusion detection in cloud environment using hybrid genetic algorithm and back propagation neural network, International Journal of Communication System, 2020