VOL. 12, NO. 20, OCTOBER 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ADVANCED ENCRYPTION STANDARD ALGORITHM BASED DISTRIBUTED DATA STORAGE SECURITY MECHANISM (D2S2M) FOR PRIVATE CLOUD

A. Anusha Priya[1] and R. Gunasundari[2]
[1]Department of Computer Science, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, India
[2]Department of Information Technology, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, India
E-Mail: anupriyaazariah@gmail.com

ABSTRACT

Cloud computing is the buzz word in the today's information technology arena and thrust research area due to its wide range in offering services. Ensuring security is the ever demanding research problem in private cloud environment. This research work aims in proposing improved security mechanism which is based on advanced encryption standard algorithm. A decisive method is used in order to verify the security of data packets. Then by making use of distributed data storage mechanism the data is stored in the private cloud servers. Undemanding data retrieval is used for obtaining the data back for the user. Simulations are carried out using MATLAB. Performance metrics such as time taken for encryption, time taken for decryption, overall elapsed time and time taken for data retrieval are chosen. From the results it is evident that the proposed D2S2M outperforms the other existing methods.

Keywords: private cloud, information technology, security, authentication, AES algorithm, parallel processing, MATLAB.

1. INTRODUCTION

Cloud computing is a promising information technology structural design for both enterprises and individuals that instigates an pretty data storage and interactive idea with obvious advantages, including on-demand self-services, ubiquitous network access, and location independent resource pooling. Consequently, security and privacy issues are attractive key concerns with the growing fame of cloud services. Conformist usual security approaches mainly focus on the strong authentication to understand that a user can remotely access its own data in on-demand mode. Next with the variety of the application requirements, users probably will desire to access and share each other's authorized data fields to achieve fruitful remuneration, which brings new security and privacy challenges for the private cloud storage. Secured distributed data storage in the throng remote data storage by the use of Storage-as-a-Service (STaaS) service model is gaining major research interest for the past decade. Several cloud vendors have given striking storage service assistance that endow with enormous and scalable cloud-based storage spaces for users, such as Amazon, Drop box, Google Drive, and Microsoft's One Drive [7, 11, 14]. On the other hand, the security problem sourced by the operations on cloud side is yet an impediment of making use of STaaS for private cloud environment [1, 5, 6, 8, and 23]. A motivation example that details the key part of the proposed model is securing data packets with sensitive information. The process has splitting data packets and data packets retrievals. This state of affairs takes place in the monetary industry, health care etc in which users' sensitive information needs to be highly protected on the cloud environment. It is presumed that there are two remote cloud storage servers, A and B. There is an input data D that is 0100 1010 0101 1110. The proposed model aims to store data D in distributed fashion on to the cloud server A and B and ensure cloud operators at A and B are not supposed to directly access the data. The storage process also requires assuring both high security and low latency and overhead requirements.

2. RELATED WORKS

Security issues have penetrated into most layers of cloud computing, from networks to system managements [21]. Many security issues in networks and data storage are also applicable to cloud computing due to the interconnections between technical applications, such as using Virtual Machine (VM). Prior researches explored the security problems and solutions in multiple perspectives. First, the data management security is an aspect of securing data in cloud computing, which often focus on encryption preparations or data classifications for the purpose of the security [16, 18]. Some approaches have been developed to ensure the secure query processing for Resource Description Framework (RDF), such as using eXtensible Access Control Mark-up Language (XACML) management policy [4]. Moreover, a selective data encryption is considered a way of reducing computing cost while protecting data in clouds. For example, classifying data in diverse ranks using searchable encryption is an approach for users to alter whether the data need to be encrypted [3, 12]. However, most current data management methods assume that the cloud operators do not abuse the data or have limited access to the data. There is a possibility of retrieving information even though the data are encrypted on the cloud side, in some situations. Next, monitoring and protecting data storage is another dimension in securing cloud data, which considers the data processing or operations occurred in the clouds. It implies that the cloud operators' behaviours are examined or inspected. One of the approaches is using Attributed-Based Encryption (ABE) to secure the privacy information when the data are shared among multiple clouds [15, 20].

However, restricting cloud operators' access scale can also result in other problems, such as data integration and data intactness [10, 17]. Risks of data damage or operation failure rate will be increased if the cloud service providers are fully blocked [5, 13, 22]. Therefore, from the perspective of data storage, the contradictions between the privacy protection and data processing are difficult to be solved. It is desired to protect data on cloud servers by using encryption-oriented approaches. Previous researches have also addressed this field, such as Fully Homomorphism Encryption (FHE) [19] and ABE. Despite this type of secure mechanisms can effectively protect data from the target attackers, such as external malicious actions and internal improper operations; nonetheless, the efficiency of the data processing can be negative impacted due to the additional computations [2, 9]. The next section addresses certain research scope dealt in the literatures.

3. PROPOSED WORK

The proposed research work consists of several stages namely decisive method (DM), encryption using AES algorithm, distributed data storage mechanism (DDSM) and data retrieval (DR). DM is used in this research work in order to verify if the input data packets are in need of security or not. The conceptual framework is portrayed in the Figure-1. At first, the DM identifies that the data packets are stored in a distributed manner in cloud environment. Setting up of input data is discoverable. It means that the input data can be identified by queries, keywords or search tag. Each input data will be given with name and known as Named Data Packets (NDP). The owner of the data and cloud service provider construct a pool of NDPs. If the NDPs are already present in Pre-Stored Name List (PSNL), the data storage method is invoked; else, XOR operation is carried out on the NDPs. The purpose of doing DM in the proposed framework is to lessen the costs of the computing resource and computation workloads that are in the cloud environment.

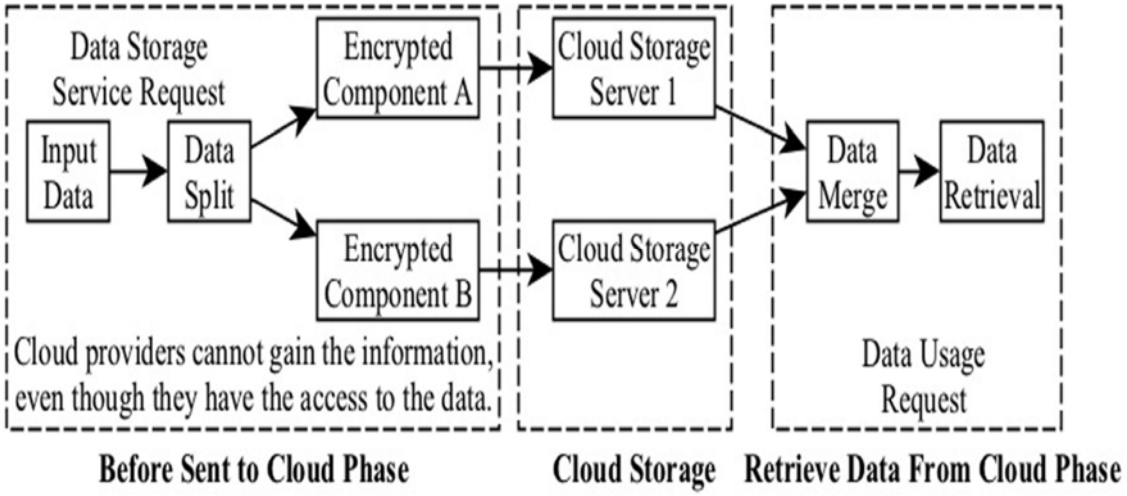

Figure-1. Conceptual framework.

3.1. Distributed data split and storage mechanism (D2S2M)

There are mainly two components in the proposed framework, which are associated with the central point and the left boxes in the Figure-1. At the time of data transmission, these two key components phases form two essential actions. Before sending the data to the cloud, the input data D is divided into two separate components. As portrayed in the Figure-1, there are two encrypted components, called A and B. The encryption is performed by using AES algorithm. AES is a block cipher technique by which the number of bytes that it encrypts is fixed. AES probably will encrypt blocks of 16 bytes at a time. When the bytes being encrypted are generously proportioned than the specified block then AES is executed in parallel manner. When the plain text is lesser than 16 bytes then it needs to be protected. The AES algorithm is portrayed in Figure-2.

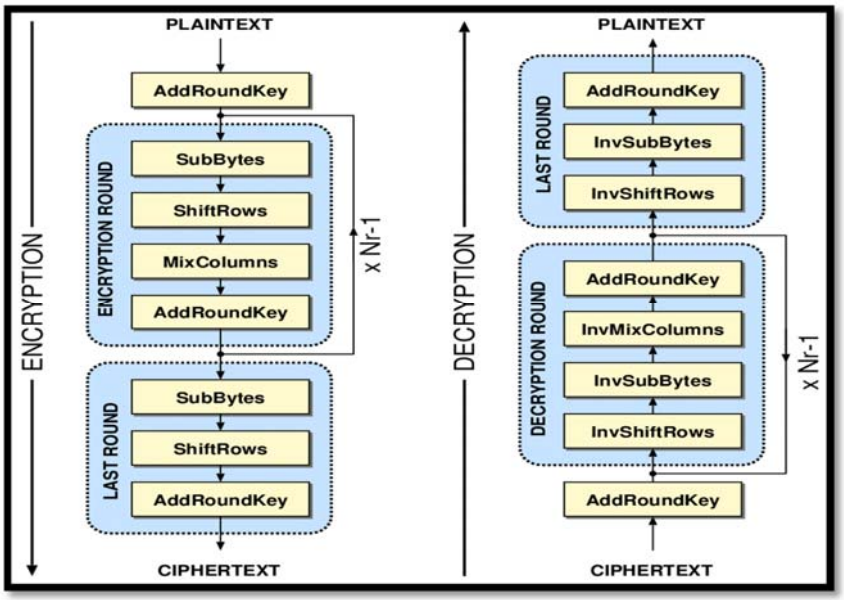

Figure-2. Block diagram of AES.

Initially a random parameter data C is generated and use it to fabricate new data packets. Next, a random key is used which will be held by users to operate XOR. This key is mandatorily to be saved in a special register at client / user side. As a final point, both encrypted data packets were uploaded to different cloud servers.

Algorithm -1: Data distribution algorithm

1. $Input\ D, C$
2. $Initialize\ R \leftarrow 0,\ \alpha \leftarrow 0, \beta \leftarrow 0$
3. $Randomly\ generate\ a\ key\ K$
4. $for\ \forall\ input\ data\ packets\ do$
5. $if\ D \neq C\ \&\&\ C \neq 0\ then$
6. $Do\ R \leftarrow D - C$
7. $\alpha \leftarrow C \oplus K$
8. $\beta \leftarrow R \oplus K$
9. $end\ if$
10. $end\ for$

a) Input data packet D and C. Data C will be a non-null set and also will be undersized than D. Also C need not to be as same as D. Certain dataset are generated namely R, α, and β; then the value 0 will be assigned to R, α, and β.

b) Key K is generated in random manner and will be stored at the user's unique register in order to perform the task of encryption and decryption for protecting privacy before the data are sent out.

c) The value of R is calculated by (D-C) after those two XOR operations are executed in order to acquire the data value stored in the clouds. The data in the remote storage are denoted to α and β.

d) Output α and β and disjointedly store up them in the diverse cloud servers.

3.2. Undemanding data retrieval

Moreover, during the data retrieval, data users need to obtain data packets from both cloud providers. Attaining the original data needs a series of operations after the data packets are received from cloud sides. In the beginning, the related data packets need to be added up to construct the new data string. After that, users will make use of the key to do two actions, XOR operation to the new data string and add the Key data value after. The original data will be obtained after this process gets completed.

$\alpha, \beta, \kappa - data\ components\ from\ cloud\ servers$

$D - actual\ data$

1. $input\ \alpha, \beta, \kappa$
2. $initialize\ \gamma \leftarrow 0, \gamma' \leftarrow 0, D \leftarrow 0$
3. $/*User\ obtains\ data\ from\ several\ cloud\ servers$
4. $\gamma \leftarrow \alpha \oplus \kappa$
5. $\gamma' \leftarrow \beta \oplus \kappa$
6. $D \leftarrow \gamma + \gamma'$

$Output\ D$

4. SECURITY MODEL

The following potential attacks which threaten the security of the cloud data are given in this section.

a) Unauthorized accessing: In this kind of threat for security, the adversaries intend at thieving the key to decrypt the cloud data without the data owner's access permission. The adversaries are probably the attackers outside.

b) Collusive attack: In this kind of threat the collusion between the untrusted cloud server and the malicious cloud user is deployed. It is presumed that the cloud server probably will collude with a user who has restricted access for helping him keep hold of the data access licence to menace the security of the private cloud data sharing system.

5. RESULTS AND DISCUSSIONS

The experimental machine is a HP with Intel Pentium CPU N3700, 8GB DDR3 memory and SATA2 500 GB hard disk. In this experiment, different file types with the sizes range from 10MB to 50 MB are used. Performance metrics such as time taken for encryption, time taken for decryption, overall elapsed time and time taken for data retrieval are chosen. The proposed D2S2M is compared with two existing mechanisms proposed by L. Wei *et al* (2014) and Q. Liu *et al* (2014). The results are shown below.

Table-1. Time taken for encryption.

Data size (in MB)	**Time taken for encryption** (in milliseconds)		
	D2S2M (Proposed)	**Q.Liu *et al*** (2014)	**L.Wei *et al*** (2014)
10	23065	38172	45821
20	42811	54834	67299
30	59488	73389	86244
40	71847	94893	104332
50	96847	125732	138748

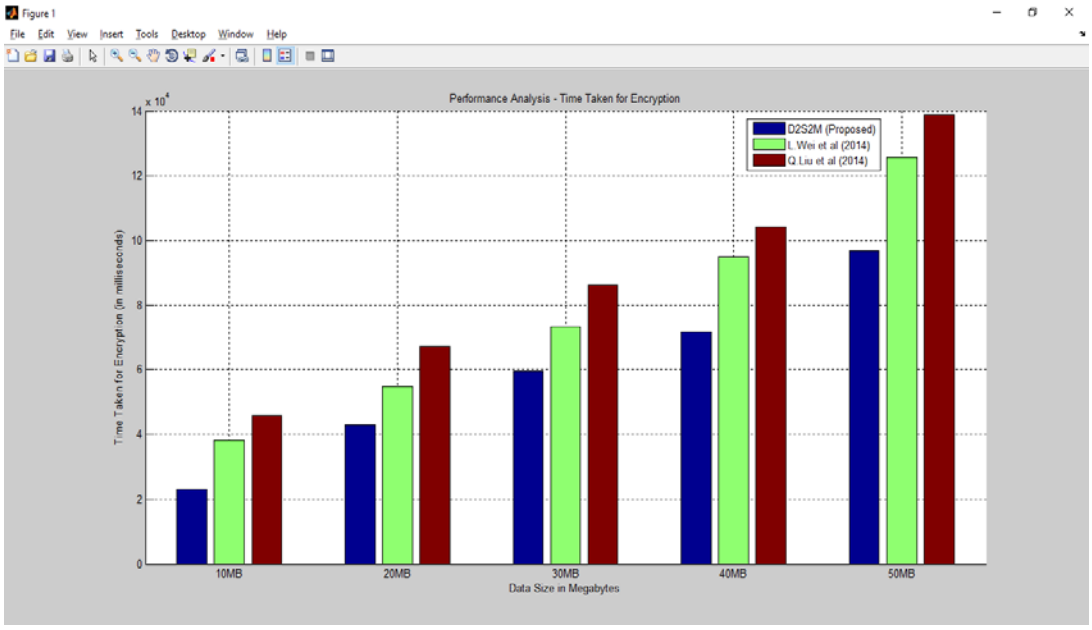

Figure-3. Performance analysis in terms of time taken for encryption.

Table-2. Time taken for decryption.

Data size (in MB)	**Time taken for decryption** (in milliseconds)		
	D2S2M (Proposed)	**Q.Liu *et al*** (2014)	**L.Wei *et al*** (2014)
10	22133	37384	46294
20	41942	53173	68013
30	58323	72094	86115
40	70119	93126	104274
50	96017	126743	137938

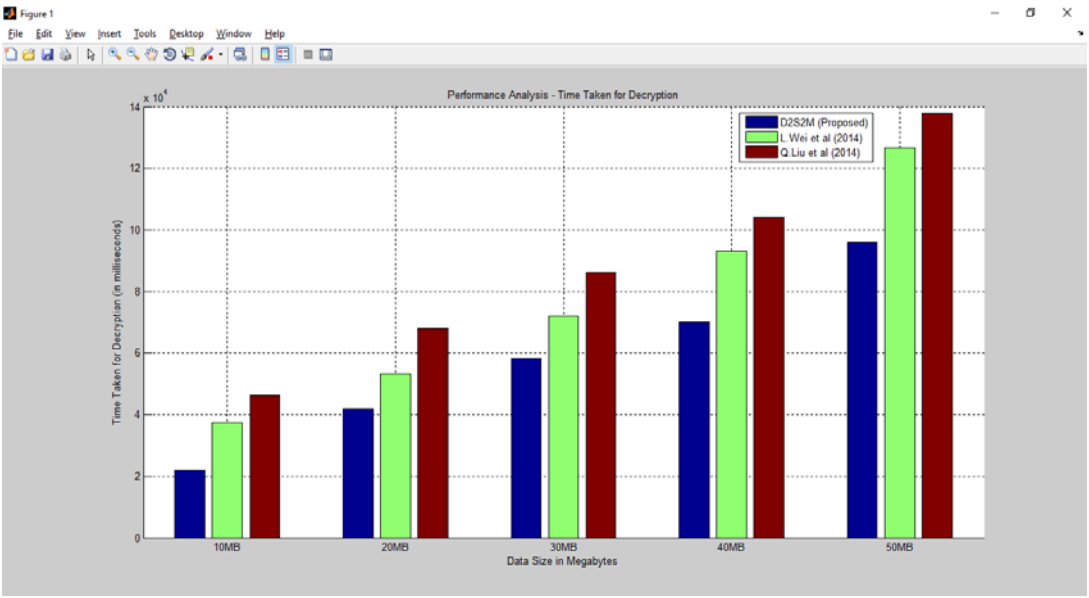

Figure-4. Performance analysis in terms of time taken for decryption.

Table-3. Overall elapsed time.

Data size (in MB)	**Overall elapsed time** (in milliseconds)		
	D2S2M (Proposed)	**Q.Liu *et al*** (2014)	**L.Wei *et al*** (2014)
10	46192	76550	93109
20	86037	109291	136596
30	119178	146850	173726
40	143712	189765	210352
50	194810	254421	278632

Table-4. Time taken for data retrieval.

Data Size (in MB)	**Time taken for encryption** (in seconds)		
	D2S2M (Proposed)	**Q.Liu *et al*** (2014)	**L.Wei *et al*** (2014)
10	3.6429	6.3845	9.6538
20	4.0148	7.1264	8.0265
30	3.9238	5.9475	8.9472
40	3.7412	6.8164	9.0472
50	4.1739	7.0372	8.5839

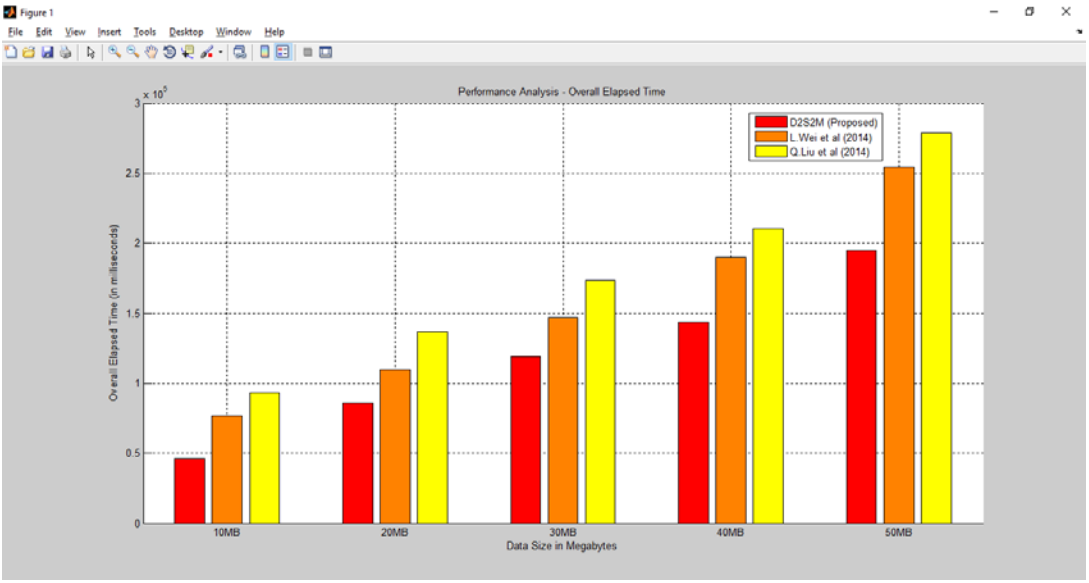

Figure-5. Performance analysis in terms of overall elapsed time.

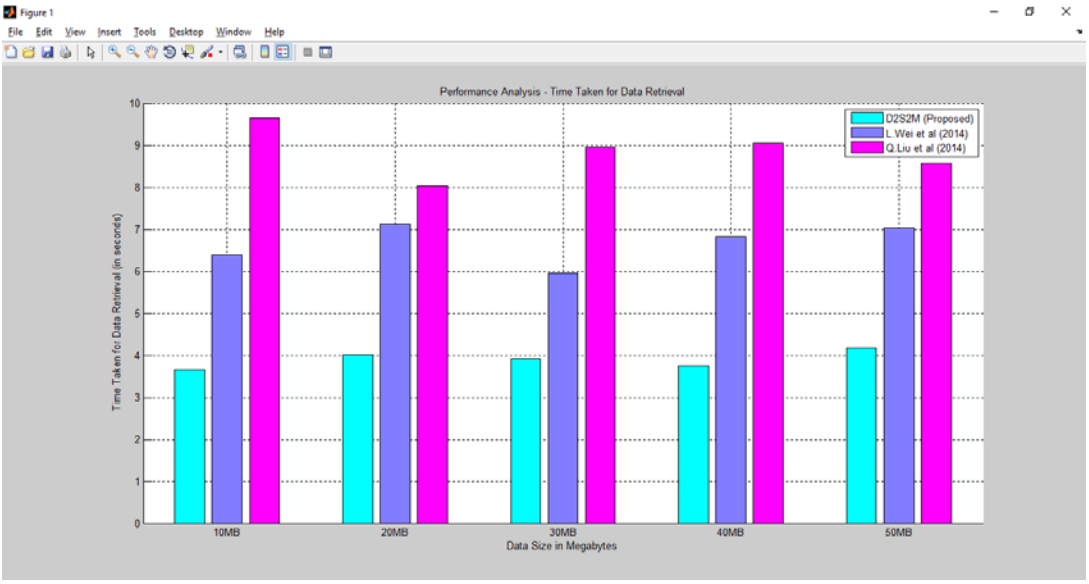

Figure-6. Performance analysis in terms of time taken for data retrieval.

6. CONCLUSIONS

The aim of this research work aims to develop an improved security mechanism based on standard advanced encryption standard algorithm. A decisive method is made use in this research for bearing out the security of data packets. After that a distributed data storage mechanism is employed for splitting the data and to store it in cloud server. An undemanding data retrieval mechanism is employed for getting back the data for the user. MATLAB simulations are carried out with chosen performance metrics such as time taken for encryption; time taken for decryption, overall elapsed time and time taken for data retrieval are chosen. From the results it is proved that the proposed D2S2M performs better than that of the other existing methods.

REFERENCES

[1] M. Ali, S. Khan, A. Vasilakos. 2015. Security in cloud computing: Opportunities and challenges, Inf. Sci. 305: 357-383.

[2] R. Aliev, W. Pedrycz, B. Fazlollahi, O. Huseynov, A. Alizadeh, B. Guirimov. 2012. Fuzzy logic-based generalized decision theory with imperfect information, Inf. Sci. 189: 18-42.

[3] N. Cao, C. Wang, M. Li, K. Ren, W. Lou. 2014. Privacy-preserving multi-keyword ranked search over

encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. 25(1): 222-233.

[4] D. Chadwick, K. Fatema. 2012. A privacy preserving authorisation system for the cloud, J. Comput. Syst. Sci. 78(5): 1359-1373.

[5] C. Chen, C. Zhang. 2014. Data-intensive applications, challenges, techniques and technologies: A survey on big data, Inf. Sci. 275: 314-347.

[6] K. Costa, L. Pereira, R. Nakamura, C. Pereira, J. Papa, A. Falcão. 2015. A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks, Inf. Sci. 294: 95-108.

[7] L. Darrell. Unlimited cloud storage at amazon.com, inc on black friday, Url = http://www.bidnessetc.com/58232-unlimited-cloud-storage-at-amazoncomincon-black-friday.

[8] Y. Ding, Y. Hu, K. Hao, L. Cheng. 2015. MPSICA: An intelligent routing recovery scheme for heterogeneous wireless sensor networks, Inf. Sci. 308: 49-60.

[9] K. Gai, Z. Du, M. Qiu, H. Zhao. 2015. Efficiency-aware workload optimizations of heterogenous cloud computing for capacity planning in financial industry, in: The 2nd IEEE International Conference on Cyber Security and Cloud Computing, IEEE, New York, USA. pp. 1-6.

[10] K. Gai, L. Qiu, M. Chen, H. Zhao, M. Qiu. 2016. SA-EAST: Security-aware efficient data transmission for ITS in mobile heterogeneous cloud computing, ACM Trans. Embedded Comput. Syst. 1: 99.

[11] K. Gai, L. Qiu, H. Zhao, M. Qiu. 2016. Cost-aware multimedia data allocation for heterogeneous memory using genetic algorithm in cloud computing. IEEE Trans. Cloud Comput. 1: 99.

[12] K. Gai, M. Qiu, B. Thuraisingham, L. Tao. 2015. Proactive attribute-based secure data schema for mobile cloud in financial industry, in: The IEEE International Symposium on Big Data Security on Cloud, IEEE 17th International Conference on High Performance Computing and Communications, New York, USA. pp. 1332-1337.

[13] K. Gai, M. Qiu, H. Zhao, W. Dai. 2015. Anti-counterfeit schema using monte carlo simulation for e-commerce in cloud systems, in: The 2nd IEEE International Conference on Cyber Security and Cloud Computing, IEEE, New York, USA. pp. 74-79.

[14] D. Howley. Is microsoft's onedrive the best cloud storage service? Url = https://www.yahoo.com/tech/microsoft- kills-unlimited- onedrive- accounts- 1759 27221.html.

[15] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou. 2013. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst. 24(1): 131-143.

[16] Q. Liu, G. Wang, J. Wu. 2014. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inf. Sci. 258: 355-370.

[17] A. Parakh, S. Kak. 2009. Online data storage using implicit security, Inf. Sci. 179(19): 3323-3331.

[18] W. Pedrycz. 2014. Allocation of information granularity in optimization and decision-making models: Towards building the foundations of granular computing, Eur. J. Oper. Res. 232(1): 137-145.

[19] T. Plantard, W. Susilo, Z. Zhang. 2013. Fully homomorphic encryption using hidden ideal lattice, IEEE Trans. Inf. Forensics Secur. 8(12): 2127-2137.

[20] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, H. Zhao. 2016. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry, Future Gener. Comput. Syst.

[21] C. Wang, S. Chow, Q. Wang, K. Ren, W. Lou. 2013. Privacy-preserving public auditing for secure cloud storage. IEEE Trans. Comput. 62(2): 362-375.

[22] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A. Vasilakos. 2014. Security and privacy for storage and computation in cloud computing, Inf. Sci. 258: 371-386.

[23] S. Yoon, K. Kim, J. Hong, S. Kim, S. Park. 2015. A community-based sampling method using DPL for online social networks, Inf. Sci. 306: 53-69.

[24] A.S. Syed Navaz, P. Jayalakshmi, N. Asha. Optimization of Real-Time Video Over 3G Wireless Networks. September – 2015, International Journal of Applied Engineering Research. 10(18): 39724-39730.

[25] A.S. Syed Fiaz, N.Asha, D. Sumathi & A.S. Syed Navaz. 2016. Data Visualization: Enhancing Big Data More Adaptable and Valuable. February - 2016, International Journal of Applied Engineering Research. 11(4): 2801-2804.

[26] A.S. Syed Navaz & Dr. G. M. Kadhar Nawaz. 2016. Flow Based Layer Selection Algorithm for Data Collection in Tree Structure Wireless Sensor Networks. March - 2016, International Journal of Applied Engineering Research. 11(5): 3359-3363.

[27] A.S. Syed Navaz & Dr. G.M. Kadhar Nawaz. 2016. Layer Orient Time Domain Density Estimation Technique Based Channel Assignment in Tree Structure Wireless Sensor Networks for Fast Data Collection. June - 2016, International Journal of Engineering and Technology. 8(3): 1506-1512.

[28] A. S. Syed Navaz, N. Asha & D. Sumathi. 2017. Energy Efficient Consumption for Quality Based Sleep Scheduling in Wireless Sensor Networks. March - 2017, ARPN Journal of Engineering and Applied Sciences. 12(5): 1494-1498.

[29] A Anusha Priya, R Gunasundari. 2017. Securing Data on the Cloud Server by the User Authentication and Data Security Techniques, 2017, International Journal of Computer Applications. 165(4).

[30] A. Anusha Priya, Lavanya. C. Enhanced Focus on User Revocation in Secure Dynamic Auditing For Data Storage in Cloud, 2016/8. International Journal of Emerging Technology in Computer Science & Electronics. 23(4): 51-55.

[31] S. Yasmin, A. Anusha Priya. Decentralized Entrance power with Secret Endorsement of data Stored in Clouds, 2015/8. International Journal of Innovative research in Computer and Communication Engineering. 3(8): 7279-7284.