VOL. 13, NO. 15, AUGUST 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

RESOURCEFUL INVESTIGATE ENCRYPTION METHOD USING DATA HUNT IN MOBILE CLOUD SERVICE

A. S. Syed Navaz[1], Asha. N[2], Vanmathi Chandrasekaran[2] and J. Jayashree[2]
[1]Computer Applications Muthayammal College of Arts & Science, Namakkal, Tamil Nadu, India
[2] Vellore Institute of Technology University, Vellore, Tamil Nadu, India
E-Mail: a.s.syednawaz@gmail.com

ABSTRACT

In this paper, we showcase demand elevated class applications, storage space of data distantly, the less protection burden of local data storage and shared pool of configurable computing resources are the services provided that can be enjoyed by the users by using cloud storage. Data integrity protection is an imposing task in cloud computing that is done as the outsourced data is no longer physically possessed, especially for users with constrained computing resources. Cloud storage is a model used by the users to store their files and the providers are responsible for keeping the data available and accessible. The mobile cloud environment has security issues as the cloud environment that cannot be applied in mobile devices. Low transmission rates, latency sensitivity, poor connectivity are the challenges required to be undertaken by wireless networks to avoid security issues. Conventional investigate schemes and ranked serial binary investigate (RSBI) algorithm leads to extra traffic costs and a long investigate time for the users. The resourceful investigate an able encryption scheme is proposed to address these issues as a mobile cloud service. The data communication process is optimized for traffic efficiency by reducing the access size by using lightweight access encrypted keyword compression method in this innovative scheme. The user registries in the cloud to upload their files and then the files are encrypted by using the index and compress, key generation and secure flow algorithm (SFA). The encrypted files are stored in the cloud server that can be downloaded by the user by entering the keyword and in the database investigate able encryption is used to investigate the files to speed up the investigate time. Two optimization methods have been proposed in document, investigate called to investigate able encryption and SFA algorithm. The result shows that investigate able encryption scheme which reduces the investigate time as well as network traffic.

Keywords: cloud storage, energy efficiency, mobile device, network traffic, investigate encryption.

1. INTRODUCTION

Cloud computing is a critical pattern for advanced data service, has become a necessary feasibility for data users to outsource data. Cloud computing services are used to store the data, such as photos, text files, videos, etc. In online instead of home computers or webmail. For example, an online invoicing service is a "cloud computing" service. The delivery of computing resources over the internet referred as cloud computing. The resource implies to use the cloud service over the internet at any location instead of storing the data or information in a hard drive or by updating applications for the needs. Cloud computing is a form of enabling relaxing, on-demand system connected to a shared pool of configurable computing resources that can be promptly provisioned and released with less management effort or service provider interaction. The cloud model develops availability by composing five essential characteristics, four deployment models and three service models. The characteristics of cloud computing include on-demand self service, rapid elasticity, resource pooling, broad network access and measured service.

The cloud computing service models are software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Deployment of cloud services is made available via a private cloud, community cloud, public cloud and hybrid cloud. Specifically, cloud computing may upgrade efforts to develop privacy protection into technology from the start and the use of improved security mechanisms. The security issues when considering a cloud provider and reviewing the terms of service with a cloud provider or when negotiating contracts the areas that organizations should keep in mind are to isolate data when dealing with providers that serve various customers and possible secondary uses of the data. Before outsourcing data onto cloud the user usually encrypts data to ensure privacy, which brings huge challenges for resourceful data utilization. However, even if the encrypted data utilization is available, the leakages of sensitive information are caused by communication of users with the cloud and allow the cloud to operate on the encrypted data. Furthermore, in cloud computing, the data files can be retrieved by the user they are interested in from the outsourced data shared by the data owner.

One of the most popular ways to retrieve the data from the cloud is through keyword-based retrieval. Keyword-based retrieval is a typical data service that is widely used in plain text scenarios, in which users retrieve similar files in a file set based on keywords. However, due to limited operations on encrypted data, it turns out to be a difficult task in the cipher text scenario. Besides, in order to develop useful and save on the consumption in the cloud paradigm, it is preferred to get the retrieval result that matches the user's interest from the most relevant files instead of all the files, which indicates that the files are ranked and from that with the highest relevance's are sent back to users.

To enable investigate on cipher text a series of investigating able symmetric encryption schemes have been proposed. Traditional SSE schemes enable users to

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

securely The retrieval of the cipher text security is enabled in traditional SSE, but boolean keyword investigates only supports this scheme, whether in a file the keyword exists or not. To increase security without compromising efficiency, schemes presented in show under various scenarios that they support top-k single keyword retrieval. In the former, from the number of retrieved keywords the files are ranked, which reduces investigate accuracy. Then latter, security is implicitly sacrificed to trade off for efficiency, which is particularly undesirable in security-oriented applications. However, on the user side the high computational overhead and limited computational power preclude information security. The security issue of top-k retrieval over encrypted cloud data is to avoid information leakage during the process of retrieval.

This paper proposes the concepts of similarity relevance and scheme robustness to formulate the privacy issue by proposing investigate able encryption and secure flow algorithm. In the proposed scheme, the most of computing work is performed in the cloud while the user takes part in the ranking, which guarantees top k file retrieval over encrypted cloud data with more security.

2. RELATED WORK

The data privacy issue is primarily in the cloud storage system, so the owner encrypts the sensitive data before outsourcing onto the cloud, and by using encrypted investigate scheme data users retrieves the data they are interested. The modern mobile device confronts many security threats same as PCs, and various traditional data encryption methods are imported in mobile cloud storage. However, the mobile cloud storage system obtains new challenges over the traditional encrypted investigate schemes, in consideration of the limited battery capacity and computing of mobile device, as well as sharing of data and approaches for accessing through wireless communication. Therefore, a suitable and Resourceful encrypted investigate scheme is necessary for mobile cloud storage. The bandwidth and energy efficiency are needed maximum to perform data encrypted investigate a scheme in mobile cloud storage, because the mobile devices have limited battery life and payable traffic fee. Therefore, the design of a mobile cloud scheme is focused on both energy consumption and the network traffic in terms of efficiency, as well as security requirements.

For data protection, the previous encryption algorithms cannot directly apply to mobile cloud, because it is hard to achieve capable network traffic and the search time to address the main issues for mobile cloud. Agrawal *et al*. future a one-to-one mapping order preserving encryption method; however, it leads to information leaks. Wang *et al*. proposed a one-to-many mapping order preserving encryption method that requires a complex computation process, and therefore is not suitable for the mobile cloud. Wang *et al* and Swaminathan *et al*. employed an order-preserving encryption method to retrieve data from encrypted cloud data, which preserved security perfectly. However, this can only be applied in a single-keyword search that retrieves files in a coarse granularity. Some researchers solved this problem through fully homomorphism encryption to retain the security of the encrypted search scheme. In a word, these order preserving encryption algorithms and fully homomorphism encryption methods proved themselves secure and accurate enough for searching encrypted data purpose. However, they cost many computing resources. As network collision and search time effectiveness becoming important, a difficult algorithm is not suitable in mobile devices. So we choose a Resourceful encryption algorithm, fast accumulated hash to encrypt document's index.

2.1 TEES

In the TEES two categories are performed in the encrypted investigate scheme first is ranked keyword investigate and the second is Boolean keyword investigate. The rank keyword investigates use relevance scores and sends a top k relevant file to the user. Boolean keyword investigate sends all the relevant files to the client.

2.2 Conventional encrypted investigate system

The customary twisted track framework over the cloud is made out of three diverse standard participants, provider, cloud and user, which are characterized beneath. The provider has an arrangement of archives and their files. It means to outsource these to the cloud and let clients contact the cloud for the inquiry administration. The cloud is a business association that gives calculation and capacity assets as virtual machines, normally known as "cloud" administration. The user is somebody who submits catchphrases to hunt archives that contain these watchwords. In our situation, clients would utilize cell phone, for example, cell phones and tablets to submit look demands. The execution stream of a conventional encoded seek over the cloud, including three primary streams: records and files transferring process, trapdoor era process and report recovery process.

The heaviness of lines demonstrates the measure of information being exchanged. Reports and records transferring process: First, the supplier accountable for this stream stems all words in these archives to be put away in the cloud and holds these terms. The encryption calculation can employ the exemplary symmetric-key cryptography calculation, for example, the advanced encryption standard. The recurrence of every term in the archive set is numbered and after that composed into the comparing section of the record file. At long last, the supplier encodes this list and outsources it to the cloud with the scrambled records. Generally, this file is a word recurrence table scrambled by the calculable encryption calculation.

Some studies have used the fast accumulated hash (FAH) calculation to accomplish these reasons. Trapdoor era procedure: To perform a pursuit demand, the client first verifies with the supplier. Amid confirmation, the give would send its mystery key to the client to decode the records put away in cloud. Once confirmed, the client would send the inquiry catchphrases to the supplier. The supplier then processes trapdoors, regularly with FAH calculations and answers back. In such case, two round

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

outings are required (authentication and trapdoor era) for a client to get the trapdoor for the inquiry catchphrases. Report recovery process: In this procedure, the client sends the noised trapdoor to the cloud. The cloud then evacuates commotion in the trapdoor and hunts the records with a pursuit calculation. At the point when reports are found, the cloud positions them as per every archive's score. At that point the top-k important archives are picked and sent to the client. At long last, they are decoded and recuperated by the client. By and large, the ranked serial search (RSS) calculation is picked as the pursuit calculation.

2.3 Privacy-preserving multi keyword fuzzy investigate

The class of approaches under fuzzy investigate relies by the locality-sensitive flowing technique. Rather than expanding index file the fuzzy matching is achieved by algorithmic design. To exhibit high efficiency in terms of computation and storage, locality flowing technique and bloom filter is proposed. The LSH in Bloom filter constructs file index and finds the document by matching the keyword resourcefully.

2.4 Enabling protected and resourceful ranked keyword

Traditional investigate techniques used by the users to investigate the encrypted data through keyword, they only support Boolean investigate but still data utilization is not effective. Ranking investigate enhances the system usability instead of sending undifferentiated results it enables investigate result relevance ranking, and file retrieval accuracy is ensured. Statistical measure approach, i.e. relevance score is explored, a secure investigate able index is build from information retrieval and to properly protect those sensitive score information a one-to-many order-preserving mapping technique is developed.

2.5 Resourceful and protected ranked multi keyword investigation

The investigate terms are used to retrieve the documents and information investigate from the remote database. The documents that should be retrieved later by the user may contain sensitive information due to this privacy concerns are applied to the relevant documents. private information retrieval, a related protocol returns the most relevant document to the user by hiding the queried investigate terms and the data retrieved from the database. Based on PIR a practical privacy preserving ranked keyword investigate scheme that allows multi keyword queries with ranking capabilities is proposed.

3. SYSTEM DESIGN

In the proposed system architecture design figure data owner usually encrypt the data before outsourcing it onto cloud, which brings great challenges for resourceful data utilization. This new scheme uses a lightweight access encrypted keyword compression method, where the access key size is reduced for traffic efficiency which optimizes the data communication process.

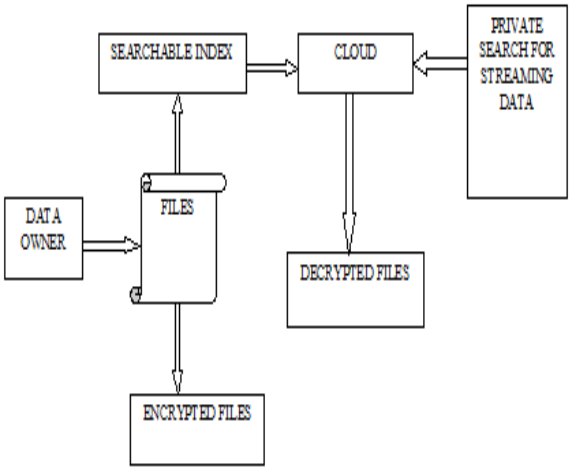

Figure-1. System architecture.

Based on the binary tree principle SFA algorithm is presented, which could reduce query time in the cloud. Furthermore, in cloud computing, data owners may share their outsourced data with a number of users, where the users can retrieve the data files they are interested.

In the Figure-1 shows user uses single keyword investigate scheme to make encrypted data investigate resourceful. From the keyword given by the user the top relevant file is retrieved from the encrypted files in the cloud database. After finding the file, decryption is processed and the original data from the cloud server to the users mobile device.

3.1 Proposed system investigation

The encrypted data utilization is possible in cloud computing, users still need to communicate with the cloud and allow the cloud to operate on the data which are encrypted, which might causes leakage of sensitive information. Data owners may share their outsourced data with a number of users in cloud computing, where the users can retrieve the data files they are interested in. To retrieve the files Keyword-based retrieval is one of the most popular ways for the users. The security issue of top-k retrieval over encrypted cloud data is to avoid information leakage during the process of retrieval.

The concepts of comparison relevance and scheme robustness to formulate the privacy issue introduces investigate able encryption scheme, and then solve the insecurity problem by proposing a single keyword investigate able encryption scheme.

Advantages

- The traditional encrypted investigate able scheme architecture in terms of network traffic and investigate time is examined. Results show that the typical approach is not applicable in mobile-cloud environments.
- A resourceful investigate able encryption scheme to address these challenges is developed. The architecture includes an access key compression

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

method to reduce traffic costs, as well as a access key SFA algorithm to reduce investigate time.

- The efficiency of a resourceful investigate able encryption scheme in network traffic and investigate time is evaluated.
- Data owner encrypts data before outsourcing onto the cloud, and users retrieve the interested data by encrypted investigate scheme it take less time of investigate
- Save computing and battery capacities of mobile device.
- Bandwidth and energy efficiency for data encrypted investigate scheme, due to the save battery life and payable traffic fee.

3.2 Network collision inadequacy difficulty

As noticed in the trapdoor making process, the trapdoor is by tradition generated by the provider to provide data security. However, in such case, the trapdoors would need to be transmitted twice per request among the provider and the user plus among the user and cloud. It depicts the search flow with two network communication round trips for established systems, including trapdoor generation process and document retrieval process. Here we do not care for the confirmation process as well as transmitting target documents from the cloud to the user. So the total network collision of the traditional system depends on network collision cost when generating trapdoors. Then we analyze the network collision cost of the established system with two network round trips.

3.3 Resourceful investigate algorithm

The resourceful search algorithm proposed by RIEMCS (resourceful investigate encryption method data hunt as a mobile cloud service) relies on a binary search tree structure to accelerate indexing. In the section, we will first introduce the conventional privacy-preserving index construction procedures, including index construction, index slicing as well as index encryption and then elaborate our binary search tree construction to accelerate index matching.

Finally we will present our encryption algorithm which leverages this data structure to perform privacy-preserving searches more resourceful document index construction. The cloud uses the indexes provided by the provider to quickly search documents. The provider is responsible for constructing document indexes and sends to the cloud. In general, two important matrices are commonly used to generate the index of documents. The term- regularity matrix denotes the frequency of each term in documents. The inverted document regularity matrix depicts the significance of rare terms that are used to distinguish documents. The multiplication of these two matrices, which produces the score matrix A. The matrix A will be encrypted and outsourced to the cloud, rather than traditional TR matrix and IDR matrix. This avoids multiplication operation when searching documents score in the cloud. Suppose we have N documents and T terms, matrix A is a N-by- T matrix. Each element RSt;c stands for the relevance score of term t in document c, for a particular document c, c 2 a1; : : :Ng and a term t, t 2 a1; : : : ; Tg. We use the column vectors Ic of matrix A as the index for a particular document.

3.4 Experimental environment

To evaluate the RIEMCS system, we implemented our system on the private cloud with Open stack Essex from our lab. We rented a virtual machine with 8G memory for the cloud. We also implemented the ENCRYPTION algorithm, written as a python program, to search and return the retrieved documents to the user. Here, the user utilized a mobile device utilized an Android tablet with a Cortex-A9 Quad 3.2 GHz CPU, and 4GB memory. The tablet is connected to a mobile network with 112 Mbps rate. The trapdoor mapping table is pre-computed on a PC and uploaded to the mobile device before experiments, which consumes 0.31MB of device storage.

The encrypted document set used here is the corpus of 2,386 VOA news extracted from the web site covering subjects such as politics, education, economy, military, etc. The number of terms in each news item is fewer than 211. For simplicity, we choose r = 216 bits. In order to facilitate construction of the final long hash code, we let d = 13. That is, the number of terms to be accumulated is not more than 213. We can achieve the final l = r_d = 851; 968, which means that each term will generate a 851,968-bit hash code. The optimized hash code is 65,536-bit by extracting the characteristic bits. The 851,968-bit hash code is generated by using MD5, SHA1 and SHA2 algorithms, recursively. We also generated 50 noise keywords randomly. We will compare the search performance of RIEMCS, the traditional encrypted search systems and the plain-text search systems with no encryption.

3.5 Investigate point evaluation

To reduce the search time and improve the calculation efficiency, we utilized the TMT module and the encryption algorithm in the RIEMCS system. In this part, we first evaluate the overall search time and its breakdown. Then we present the performance or the encryption algorithm in terms of the search time.

3.6 Network traffic evaluation

In the RIEMCS system, which benefits from the trapdoor compression method and the TMT module, we reduced network traffic significantly. Next we evaluate and analyze the overall system network traffic reduction and the performance of the trapdoor compression method. assisted by the trapdoor compression method and the TMT module, RIEMCS costs less network traffic than the traditional system. We evaluate this in the subsection. The throughput comparison of plain text, RIEMCS and the traditional system. We see that the transmission speed for the 1KB-size document is most effective, and the speed increases from 32 KB/s to 65 KB/s. Even if the document is 10 KB in size, the transmission speed is also effective (a 21% improvement). In addition, the throughput of RIEMCS is almost similar as that of plain text. In a word,

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

the RIEMCS system outperforms the traditional system in terms of network traffic costs.

4. IMPLEMENTATION

The proposed system flow of steps that involve how the data are uploaded by the owner the encryption process to protect from security issues. The process of download of data from cloud database is explained. In the proposed system flow data owner uploads the file to cloud server by encrypting for security purpose. The encryption is done by compress and index to reduce the file size and for encryption of raw file. Then private key and public key is generated to access the file by the users. SFA algorithm is applied to generate the flow function to produce unique identity for the each file. The encrypted file stored in the cloud server can be downloaded by the user by entering the keyword and then in the database investigate able encryption is used to investigate the file from the encrypted files. After investigating the user retrieves the original data from the cloud database.

5. PERFORMANCE ESTIMATION

The system security analysis and evaluation, now evaluate investigate able encryption scheme performance in terms of energy, traffic and file access. In the experiment, we use a data set of 1000 files with different sizes and a VM in the cloud with dual v CPUs at 2.27GHz. The user sends single keyword to investigate the file from the encrypted file in the cloud server.

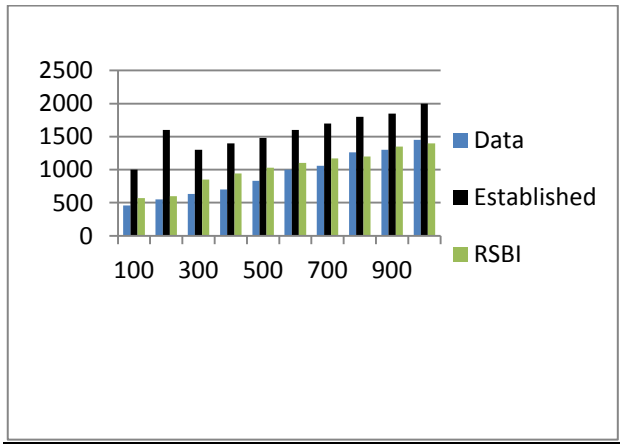

Figure-2. Performance evaluation.

Investigate able encryption Resourceful ly investigates the file from the database with less traffic and the energy consumed by android mobile will be less. The file access and the retrieval time form the cloud server will take less time consumption which automatically reduces the energy consumption. Moreover the proposed scheme decrypts the file to original text before retrieving to the user within short time which evaluates high performance.

From the algorithm established encryption produces more traffic and time consumption. The ranked serial binary investigate was proposed by in the existing scheme. The investigate time was reduced accordingly to the file size compared to the traditional encrypted investigate system by the RSBI algorithm. Investigate able Encryption is proposed to reduce the network traffic and the investigate time to retrieve the file from the cloud database. The time is consumed according to the file size the user wants to retrieve. The energy consumption is also reduced as the file is downloaded faster by using investigate able encryption algorithm.

6. CONCLUSIONS

The traditional investigate scheme is an initial attempt to create a less traffic and energy Resourceful encrypted keyword investigate tool over mobile cloud storages. An encrypted investigate is achieved in a mobile cloud an Resourceful implementation Investigate able encryption developed. The security study of investigate able encryption showed that it is secure enough for mobile cloud computing, to retrieve the data with less traffic and energy consumption resourcefully. Investigate able encryption over plain-text slightly consumes more time and energy than keyword investigate, but at the same time it saves significant energy compared to traditional strategies featuring a similar security level. Single keyword investigate scheme is proposed to make encrypted data investigate Resourceful.

REFERENCES

[1] C. Wang, N. Cao, K. Ren and W. Lou. 2012. Enabling secure and Resourceful ranked keyword investigate over outsourced cloud data. IEEE Trans. Parallel Distributed Systems. 23(8): 1467-1479.

[2] D. Stehl´e and R. Steinfeld. 2010. Faster fully homomorphic encryption. in Advances in Cryptology-ASIACRYPT. pp. 377-394.

[3] P. Wang, H. Wang and J. Pieprzyk. 2009. An Resourceful scheme of common secure indices for conjunctive keyword-based retrieval on encrypted data. pp. 145-159.

[4] A. Boldyreva, N. Chenette, Y. Lee and A. Oneill. 2009. Order preserving symmetric encryption. in Advances in Cryptology EUROCRYPT. pp. 224-241.

[5] K.D. Bowers, A. Juels and A. Oprea. 2009. Hail: A high-availability and integrity layer for cloud storage. in Proc. ACM Conf. Computing. Communication Security (CCS). pp. 187-198.

[6] J.S. Culpepper, G. Navarro, S.J. Puglisi and A. Turpin. 2010. Top-k ranked document investigate in general text databases. in Proc. Annual Euro. Conf. Algorithms (ESA). pp. 194-205.

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

[7] C. Gentry and S. Halevi. 2011. Implementing gentry's fully homomorphic encryption scheme. in Advances in Cryptology - EUROCRYPT. pp. 129-148.

[8] J. Li, R. Ma and H.Guan. 2015. Tees: An Resourceful investigate scheme over encrypted data on mobile cloud. IEEE Trans. Cloud Computing. pp. 1-4.

[9] C.Orencik and E.Savas. 2012. Resourceful and secure ranked multikeyword investigates on encrypted cloud data. in Proc. Joint EDBT/ICDT Workshops. pp. 186-195.

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

[11] AA.Swaminathan, Y. Mao, G.M. Su, H. Gou, A.L. Varna, S.He, M.Wu and D.W. Oard. 2007. Confidentiality-preserving rank-ordered investigate. in Proc. ACM Workshop Storage Security. Survivability (Storage SS). pp. 7-12.

[12] MM.Van Dijk, C.Gentry, S.Halevi and V. Vaikuntanathan. 2010. Fully homomorphic encryption over the integers. in Advances in Cryptology-EUROCRYPT. pp. 24-43.

[13] CC.Wang, N.Cao, J.Li,,K.Ren and W.Lou. 2010. Secure ranked keyword investigates over encrypted cloud data. in Proc. IEEE Int. Conf. Distributed Computing System (ICDCS). pp. 253-262.

[14] BB.Wang, S.Yu, W.Lou and Y.T.Hou. 2014. Privacy-preserving multi keyword fuzzy investigates over encrypted data in the cloud. in Proc. Int. Conf. Computing Communication (INFOCOM). pp. 2112-2120.

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

[16] 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. International Journal of Engineering and Technology. 8(3): 1506-1512.

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

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

[19] *A.* Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M. Wu and D.W. Oard. 2007. Confidentiality-preserving rank-ordered search. in Proc. ACM Workshop Storage Secur. Survivability (StorageSS). pp. 7-12.

[20] Boldyreva, N. Chenette, Y. Lee and A. Oneill. 2009. Order preserving symmetric encryption. in Advances in Cryptology- EUROCRYPT 2009, pp. 224-241.

[21] Gentry. 2009. A fully homomorphic encryption scheme. Ph.D. dissertation, Stanford University.

[22] M. Van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan. 2010. Fully homomorphic encryption over the integers. in Advances in Cryptology-EUROCRYPT 2010. pp. 24-43.

[23] Stehl´e and R. Steinfeld. 2010. Faster fully homomorphic encryption. in Advances in Cryptology-ASIACRYPT 2010, pp. 377-394.

[24] R. Chen, A. Reznichenko, P. Francis, and J. Gehrke. 2012. Towards statistical queries over distributed private user data. in USENIX Symp. Netw. Syst. Des. Implementation (NSDI). 12: 13-13.

[25] V. Rijmen and J. Daemen. 2001. Advanced encryption standard. Federal Information Processing Standard. pp. 19-22.

[26] X. Lai. 1992. On the design and security of block ciphers. Ph.D. dissertation, Diss. Techn. Wiss ETH Z urich, Nr. 9752, 1992. Ref.: JL Massey; Korref.: H. B uhlmann.

[27] K. Nyberg. 1996. Fast accumulated hashing. in Proc. Int. Workshop Fast Softw. Encryption (FSE). pp. 83-87.

[28] Nyberg and Kaisa. 1995. Commutativity in cryptography. in Proc. Int. Workshop Funct. Anal.

©2006-2018 Asian Research Publishing Network (ARPN). All rights reserved.

[29] J. Benaloh and M. De Mare. 1993, 1994. One-way accumulators: A decentralized alternative to digital signatures. in Advances in Cryptology-EUROCRYPT. pp. 274-285.

[30] O¨ rencik and E. Savas. 2014. An efficient privacy-preserving multikeyword search over encrypted cloud data with ranking. Distrib. Parallel Databases. 32(1): 119-160.

[31] J. Li, R. Ma, and H. Guan. 2015. Tees: An efficient search scheme over encrypted data on mobile cloud. IEEE Trans. Cloud Comput.

[32] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou. 2014. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans. Parallel Distrib. Systems. 25(1): 222-233.

[33] N. Asha & Prasanna Mani, Customized Services to Generate Test Suits for Testing Custom Software Application System based on Knowledge Reuse, Journal of Advanced Research in Dynamical & Control Systems, 01-Special Issue, April 2017, pp 14-20.

[34] A.S. Syed Fiaz, M. Usha and J. Akilandeswari. 2013. A Brokerage Service Model for QoS support in Inter-Cloud Environment. International Journal of Information and Computation Technology. 3(3): 257-260.

[35] M. Usha, J. Akilandeswari and A.S.Syed Fiaz. 2012. An efficient QoS framework for Cloud Brokerage Services. International Symposium on Cloud and Service Computing, pp. 76-79, 17-18, IEEE Xplore.

[36] A.S. Syed Fiaz, K.S.Guruprakash & A.S. Syed Navaz. 2018. Prediction of Best Cloud Service Provider using the QoS Ranking Framework. International Journal of Engineering & Technology. 7(1.1): 486-488.